Table of Contents

This document brings together the following three OECD reports on Radio-Frequency Identification (RFID)

OECD Policy Guidance on Radio Frequency Identification

Preface

The use of Radio Frequency IDentification (RFID) technologies[1] is growing. Many different RFID applications are implemented in various sectors, and used for very different purposes. RFID is now at a stage where there are potentially large benefits from wider application but barriers remain, warranting a policy framework to enhance business and consumer benefits while effectively addressing security and privacy issues. From a public policy perspective, such a framework should be supportive, technology neutral encompassing all RFID technologies and provide the basis to protect citizens from current and future negative impacts of the technologies. These policy principles address barriers to wider application of RFID. They draw on policy discussions and analytical studies on RFID carried out by the OECD from 2005 to 2007.[2]

RFID enables wireless data collection by readers from electronic tags attached to or embedded in objects, for identification and other purposes. RFID systems involve software, network and database components that enable information to flow from ° Š £ ¯ ˙ ° « ˙ ° ¤ ¡ ˙ « ® £ š ª ¥ ¯ š ° ¥ « ª ¯ ˙ ¥ ª ¢ « ® © š ° ¥ « ª ˙ ¥ ª ¢ ® š stored. Systems are application-specific. Some use passive, low cost tags with short read ranges, most data on the network, and only small amounts of information on tags. Others use sophisticated, high performance tags with high data capacity or read ranges that can have considerable data on tags without network connection. At present, the higher capacity tags remain less commercially viable but their cost is decreasing and they are becoming part of wider, often sensor-based, systems.

RFID applications have been in use for many years in transport (public transport entry), access control cards (building and highway entry), event ticketing and management, and, more recently, in government identity cards and passports, and extensively in manufacturing supply chains and in logistics for goods distribution. Industry sectors differ widely in RFID deployment, with many automotive

---

1. RFID may be considered as one of a group of automatic identification and data capturing technologies which also includes bar codes, biometrics, magnetic stripes, optical character recognition, smart cards, voice recognition and similar technologies.

2. See _Radio-∕ ® ¡ – ± ¡ ª œµ ˙ Ł Ÿ ¡ ª ° ¥ ¢ ¥ œš ° ¥ « ª ˙ ˙ š ˙ ∕ « œ± ¯ ˙ « ª ˙ ' ¡ œ ˙ ˙ ' (Ł Ł ˛ ˛ $ & ı fi ˙ ∕ Ł " ° ž ˙ & š Ÿ ¥ « ˙ ∕ ® ¡ – ± ¡ ª œµ ˙ Ł fi ¡ ® © š µ ˙ ¤ š ¨ ¡ ª £ ¡ ¯ š ª Ÿ ˙ $ ª Ł ı¢ ¥ ° Radio∕ Ł " ° ž ˙ (Ł ∕ ® ¡ – ± ¡ ª œµ ˙ Ł Ÿ ¡ ª ° ¥ ¢ ¥ œš ° ¥ « ª ® ¥ ² ¡ ® ˙ (2006) ¡ £ ¡ ¯ š ˙ ' (Ł Ł ˛ ˛ $ ∕ Ł " ° ž ˙ $ ® « œµµ¤ Yn¥ Radio « ¢ ˙ ° ¤ ¡ ˙ ∕ ® ¡ – ± ¡ ª œµ ˙ Ł Ÿ ¡ ª ° ¥ ¢ ¥ œš ° ¥ « ª ˙ ° ¬ ¬ ¨ ¥ œš ° ¥ « ¯) š ª Ÿ $ ± › [DSTI/ICCP(2006)7].

© OECD.2008

companies and hospitals relying on RFID systems. Wholesale and retail businesses are rapidly adopting such systems, with a shift towards more comprehensive application strategies along sector value chains. Most tagging still occurs at the pallet and packing carton level, but there is a trend toward item-level tagging, beginning with high-value goods or components, as tag prices decline.

Business benefits are sector-specific and commonly include process optimisation, more efficient supply chain inventory management, and increased process quality and security including recycling and anti-counterfeiting applications. Most implementation projects are in their early stages and many businesses need to change the processes or their work organisation to better capture benefits. Broad societal benefits are expected from RFID in various areas ranging from food safety, product recall, drug identification, public health and medical applications, better warranty management, better, more detailed product information and improved stocking.

Technological developments are focusing on increasing real-time information of business processes, improved business performance and improved security and privacy. Combination with other technologies is important in the longer-term, and communications and sensor technologies will enable distance monitoring of ambient conditions (*e.g.* temperature, pressure) in applications such as healthcare and environment. Many of the technical challenges are imposed by the laws of physics, such as interference, power management, reflection, and signal attenuation.

Many of the potential societal challenges raised by RFID relate to its core characteristic: invisible electromagnetic communications that make the collection of information by RFID devices not obvious to the person carrying the tagged product « ® ˙ « › ¦ ¡ œ° ˙ ˙ (š £ ¯ ˙ Ÿ š ° š ˙ Ÿ ¡ ¬ ¡ ª Ÿ ¯ ˙ « ª ˙ ° ¤ ¡ ¥ ® ˙ ± ¯ ¡ chain/retail context, tags attached to products usually contain product-identifying information and privacy concerns arise after the point of sale; in credentials, tags sometimes contain personal information. The extent to which tags are traceable is determined by the read range of the combined tag and reader. Specific concerns include the controls of the tag reading, the protection of personal data, the ability to join trace information with other information to profile individuals and the use to which the information may be put. Longer-term concerns are related to the potential pervasiveness of tags and readers.

Like any other information technology, RFID systems are subject to security risks[3] affecting their integrity, availability and confidentiality such as denial of service, jamming, cloning, interception/eavesdropping, and unauthorised access to Ÿ š ° š ˙ ¯ § ¥ © © ¥ ª £ ˙ + ¤ ¥ ¨ ¡ ˙ ª « ° ˙ š ¨ ˙ ± ¯ ¡ ¯ ˙ « ¢ ˙ & ⁄ ł systems which collect or process information relating to identified or identifiable individuals are subject to privacy risks (*e.g.* unauthorised access to information stored in tags). The use of RFID in identity credentials, for example, poses heightened privacy concerns, and it is necessary to ensure privacy is appropriately protected. These risks, if not taken into account at an early stage, are likely to increase the costs of RFID applications and, more generally, impede the adoption of the technology and delay potential benefits.

---

3. *E.g.* cloning of speed-pass payment RFID cards and automobile ignition keys.

The OECD *Security Guidelines*[4] and *Privacy Guidelines*[5] provide a comprehensive framework for the security of information systems and network and the protection of privacy and personal data. This framework applies to RFID.

The policy principles that follow provide policy and practical guidance to enhance business and consumer benefits from the use of RFID while proactively taking into account security and privacy concerns. Principles 1 to 6 cover government and business policies and practices to increase the use of, and economic benefits from, wider applications of RFID and emerging related sensor applications. Government policy roles are directed at: incentives for R&D and generic technologies and applications; developing public sector applications and being model users; information, awareness and education activities, including in privacy and security areas and for small businesses; harmonisation of standards; and spectrum allocation issues. Principles 7 to 12 provide all stakeholders with guidance to support the implementation of the *Security and Privacy Guidelines* when they deploy RFID systems. Specific issues are addressed in relation to RFID systems or RFID components in broader systems, including the need for: a comprehensive approach to security and privacy management; security risk and privacy impact assessments; tec¤ ª ¥ œš ¨ ' © ¡ š ¯ ± ® ¡ ¯ ' ° « ' ¬ ® « ° ¡ œ° ' ¯ ¡ œ± ® ¥ ° µ information; and a general policy of transparency. Principle 13 calls for a continued dialogue among all stakeholders. Finally, the need for monitoring developments related to RFID is highlighted in Principle 14.

Principles

1. Support for R&D and new applications

Government support and incentives should focus on R&D for generic RFID-related technologies and applications.

Many of the technological areas underlying RFID are still being developed and there are wide economic benefits to be gained from continued research in areas critical to RFID development, including new materials, and new reading technologies that can be used at greater distances and that can overcome interference and operate in hostile environments. There are social benefits from continued research on issues related to RFID use in the healthcare or environmental areas *e.g.* interference with other medical devices, impact of electromagnetic fields on individuals, or the effect tags will have on recycling practices. Further efforts to research and develop cost-effective technical measures embedding security and privacy protections in RFID systems should also be encouraged (see Principle 9).

---

4.   *OECD Guidelines for the Security of Information Systems and Networks : Towards a Culture of Security* (2002).

5.   *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

2.   Technological neutrality

Government policies to encourage the use and expand the benefits of RFID should be technology-neutral.

RFID technologies and applications are highly diverse and evolving rapidly. RFID technologies vary in terms of capabilities (*e.g.* frequency range, battery and memory capacity, size). Individual RFID applications involve a wide range of different operations and industry sectors. Attempts to focus support efforts on particular technologies or applications may diminish resources for other promising avenues and distort markets for components and equipments. Government policies to foster the use and expand the benefits of RFID should not favour one technology or application over another.

3.   Governments as model users

As developers and users of RFID for public purposes, governments should share their experience and good practices as widely as possible.

Governments are developing innovative RFID applications in areas ranging from tracking art works and library and museum stocks to improved airport management and defence applications. Their experience and good practices in developing such applications can benefit other actors and should be shared as widely as possible to maximise the benefits from government investments and help diffusion of the technology.

4.   Awareness and inform   ation

Governments should encourage initiatives to help raise awareness of the benefits and challenges of RFID and encourage sharing of information on large-scale pilots and demonstration projects.

Governments, in conjunction with business associations, the technical community and increasingly with consumer and other citizen groups, have experience in raising awareness of the benefits and challenges of emerging technology applications and their economic and social impacts. Clear and neutral information on RFID technologies, their characteristics and related security and privacy aspects can help small business and the general public appreciate the benefits and risks of these technologies and make informed choices in relation to their use. Governments should promote provision of such information at the earliest possible stage, particularly where applications have cross-sector implications and broad social impacts.

5. Standards

The development of consensus-based global standards for RFID should be encouraged. Issues such as standards convergence should be addressed through market mechanisms to the extent possible.

The development and use of RFID technical and management standards, within and across sectors, enables interoperability, encourages new market entry and allows for economies of scale in applications particularly at the international level. The development of open global RFID standards and standards harmonisation within and across sectors should involve all stakeholders. Standards can play an equally important role in facilitating security and privacy by design and good practices for RFID systems.

6. Spectrum

Governments should encourage and facilitate RFID applications when considering spectrum licensing and allocation.

Governments, manufacturers, standardisation bodies and other stakeholders should co-operate at international level to ensure interoperability, to consider harmonisation of frequency bands as appropriate, to limit harmful interference with other radio devices and users, and to ensure that devices operating within the specified frequency bands comply with the electrical power, radio standards and policy set for those systems, and encourage the development of internationally compatible applications. The exemption of licenses for frequency usage in RFID applications is a recognised licensing option, and is known to be a driver for RFID technology adoption.

7. Security and privacy management

Participants should adopt a comprehensive approach to developing a security and, where appropriate, a privacy management strategy which should be tailored to each RFID system and take into account the interests of all parties involved, including individuals.

All RFID systems require the development of a security management strategy which considers each st š £ ¡ ¨ « ¢ ¨ ˚ ¤ ¡ ¨ ¯ µ ¯ ˚ ¡ © ¯ ¨ ¨ ¥ ¢ ¡ ¨ ¬ ¨ š ª ª ¥ ª £ data processing and end of life) and each component of the system (tags and readers, middleware, databases, network and back-end components).

Not all RFID systems require a privacy management strategy. Such strategy is required when an RFID system collects or processes information relating to an identified or identifiable individual. An organisation which implements an RFID system should conduct a careful analysis of whether the RFID information is personal data (*e.g.* name or personal identifier), or if the RFID information, while not personal data (*e.g.* object identifier), can be linked to an identified or identifiable individual (*e.g.* at the point of sale). In both cases, the RFID system requires a privacy management strategy which considers each step of the RFID data lifecycle, ¡ š œ ¤ ¨ ¯ ˚ š £ ¡ ¨ « ¢ ¨ ˚ ¤ ¡ ¨ ¯ µ ¯ ˚ ¡ © ¯ ¨ ¨ ¥ ¢ ¡ ¨ š ª Ÿ ¨ ¡ š œ ¤ ¨ œ « ©

8.   Security risk and privacy impact assessments

Participants should conduct and periodically review a security risk assessment and, where appropriate, a privacy impact assessment.

Security risk assessment and, where applicable, privacy impact assessment are essential tools for managing security and privacy in relation to RFID systems. Such assessments are necessary to determine the appropriate preventative and mitigation measures to manage the risk of potential harm to RFID systems, to the organisation, and to individuals in light of the nature and sensitivity of the information to be protected. Security risk assessments and privacy impact assessments should take into consideration the technology, the application and operational scenarios, and consider the entire life cycle of the actual RFID tags including those that remain functional even when no longer under the control of the organisation.

The privacy impact assessment of an RFID system should consider whether it is necessary to collect and process information relating to an identified or identifiable individual. It should also take into account the possibility of linking data collected or transmitted using RFID with other data and the potential impact those linkages could have on individuals. This becomes even more important in the case of sensitive personal data (*e.g.* biometric, health, or identity credential data), as does the issue of protecting the data. Finally, organisations could consider making their privacy impact assessments public, as appropriate.

9.   Technical measures to protect security and privacy

Participants who develop or operate RFID technologies and systems should adopt technical security and privacy protection measures in the design and operation of their systems.

A combination of technical and non-technical safeguards is required to ensure security and protect privacy in relation to RFID technologies and systems. Cost-effective technical measures embedding security and privacy protections can play a significant role in reducing risks related to, and fostering trust in, RFID technologies and systems. A number of measures are either available or under development (*e.g.* deactivation, authentication mechanisms, cryptography, data minimisation and anonymisation). Further efforts towards their adoption should be encouraged.

10.   Knowledge and consent

Participants who collect or process information relating to identified or identifiable individuals using RFID should do so with the knowledge and, where appropriate, the consent of the individuals concerned.

Individuals should be informed about, or, where appropriate, have the possibility to consent to, the collection, processing, storage and dissemination of RFID data relating to them. Their knowledge or consent should be based on an understanding of the entire RFID data life cycle not just the initial transmission. Governments should encourage all participants to work towards a consensus on the circumstances under which consent should or should not be required.

11. Privacy notices

Participants who collect or process information relating to identified or identifiable individuals using RFID could include more information in RFID privacy notices than in usual privacy notices, given the invisibility of the data collection.

In addition to information about the data collected, the purpose of the collection and the right of access, privacy notices could include all or part of the following: *i)* the existence of tags, *ii)* their content, use and control, *iii)* the presence of active readers, *iv)* the ability to disable tags and *v)* where to obtain assistance. Such explanatory information would also help educate the public about the new technology. Research towards innovative notification practices, standardised notices and technical means to improve user notification should be encouraged.

12. Transparency

Participants who provide functional tags to individuals   whether or not they collect personal data   should inform individuals about the existence of the tags, any associated privacy risks, and any measures to mitigate these risks.

Participants who provide individuals with RFID tags that remain functional and could be read at a later stage, including by third parties, should have a general policy of transparency about the existence of such tags, their content, any potential privacy risks in presence of active readers, any measures to prevent or mitigate risks such as information on how to deactivate the tags, information on where to obtain assistance, and any further relevant information. Furthermore, there should be a possibility for individuals to disable RFID tags transparently, easily and without extra cost. It is however recognised that there may be specific circumstances in which it would be impossible or involve disproportionate efforts to provide such ¥ ª ¢ « ® © š ° ¥ « ª ˙ « ® ˙ ¥ ª ˙ ³ ¤ ¥ œ¤ ˙ ¥ ° ˙ ³ « ± ¨ Ÿ ˙ ª « ° ˙ › ¡ ˙ ¥ ª ˙ the RFID devices.

13. Continued dialogue

Governments should encourage all participants to continue to work towards better policies to enhance the economic and social benefits from wider applications of RFID and effectively address outstanding security and privacy issues.

A continued dialogue between all participants will enhance the economic and social benefits from wider applications of RFID, and foster increased security and privacy in RFID systems. The usefulness of such dialogue has already been mentioned in areas such as awareness and information, standards, spectrum, ¥ ª Ÿ ¥ ² ¥ Ÿ ± š ¨ ¯ ˙ § ª « ³ ¨ ¡ Ÿ £ ¡ ˙ š ª Ÿ ˙ œ« ª ¯ ¡ ª ° ˙ š ª Ÿ ˙ ° ® š ª the development, publication and adoption of good practices more widely, including security and privacy practices, would facilitate wider diffusion of RFID technologies and help address concerns raised by their potential widespread adoption.

14. Looking forward: monitoring evolution

Governments should encourage research and analysis on the economic and social impacts of the use of RFID in conjunction with other technologies and systems.

Because of continuous technical innovation and its impact on the economy and society, monitoring developments and detecting trends early is essential to identify new opportunities to be seized, new challenges to be addressed, and to adjust policies. Potential developments of RFID to be monitored include their combination with sensor-based systems, their cross-border use, the convergence of these technologies on the Internet, and their potential pervasiveness.

RADIO FREQUENCY IDENTIFICATION (RFID):
A FOCUS ON INFORMATION SECURITY AND PRIVACY

FOREWORD

This report was prepared by the Laurent Bernat of the OECD Secretariat with the assistance of Nick Mansfield, consultant to the OECD, under the supervision of Anne Carblanc. The first draft benefitted from initial input from Francis Aldhouse, consultant to the OECD. It includes comments and suggestions from OECD member countries, business and civil society.

The report was discussed by the Working Party on Information Security and Privacy in October 2007 and declassified by the Committee for Information, Computer and Communications Policy on 17 December 2007. It is published under the responsibility of the Secretary-General of the OECD.

Table of contents

Executive Summary

The deployment of Radio Frequency Identification (RFID) in a large number of application areas is promising. This paper introduces the main characteristics of RFID technologies and focuses on the information security and privacy aspects of RFID in the short term. It will be complemented by an overview of RFID applications and an analysis of economic aspects of RFID carried out by the OECD Working Party on the Information Economy (WPIE).[6] Later on, and based on both sets of work, a common set of policy principles related to RFID will be developed.[7]

This report represents the first step of OECD work related to sensor-based environments. Follow-up work will address security and privacy issues raised by a number of possible longer-term trends such as the generalisation of object tagging (pervasive RFID), of open loop RFID and of other sensors and sensor networks that can monitor the environment.

A varied and complex technology

RFID is a convenient and popular term for a technology with **vague boundaries** and **many facets**. Radio-frequency identification is not always based on radio-frequency communications and identification is only one among the many functions RFID technology can perform. Rather, RFID enables data collection with contactless electronic tags and wireless transmitters (readers) for identification and other purposes. It can be seen as a first step towards sensor-based environments.

Understanding the capabilities and limitations of RFID technology is essential because the likelihood of several potential security and privacy risks varies according to the type of RFID technology used as much as according to the context in which RFID is implemented. The paper therefore provides **basic information** on RFID technology, including elements regarding standards, hardware and software components, frequency ranges, modes of operation (electromagnetic induction or radio-waves) and operation ranges.

Information security aspects

There are a **large number of potential risks** to RFID tags, readers and tag-reader communication that implicate each of the three classical dimensions of security: availability, integrity and confidentiality. Examples include denial of service, jamming, cloning, eavesdropping and skimming. Malware using tags as a

---

6. See OECD (2007b, c).

7. DSTI/ICCP/IE/REG(2007)1.

vector for dissemination has also been identified as a potential risk. Tags and readers are not the only components of RFID systems that require security protection. Software (middleware), network and database components are also subject to information security risks. RFID security risks are not theoretical: a number of vulnerable security products and systems, sometimes deployed at very large scale, have been discovered by researchers or reported in the press. However, many of these potential risks are more or less likely to occur depending on the type of RFID technology used (*e.g.* eavesdropping is less likely when magnetic induction is used because the operation range is very short).

Ensuring RFID security requires a mix of technical and non-technical controls to prevent and mitigate risk. A number of **technical controls** are available. However, their degree of sophistication, robustness, complexity and cost varies. As a result, there is no one-size-fits-all RFID security measure that would efficiently address a given class of risks in all possible situations and at low cost. The development of well tailored and innovative technical security safeguards for RFID may therefore be a critical success factor for large scale deployment of RFID in many areas.

As mentioned above, not only do risks to RFID systems vary considerably according to the technology used, they also vary depending on the application contexts and scenarios. Consistent with the OECD *Security Guidelines*, risk assessment and risk management can help address the security of RFID systems. A **holistic approach** to risk (*e.g.* œš ®¡ ¢ ± ¨ ¨ µ ˙ œ« ª ¯ ¥ Ÿ ¡ ®¥ ª £ ˙ ¡ š œ¤ ˙ ¯ ° š £ ¡ planning, deployment, operation, data processing and end of life and each component of the system tags and readers, middleware, databases, back-end and network components) is required to develop an overall security strategy. The risk evaluation and management strategy help identify the necessity to strengthen specific parts of the system in order to compensate for some weaknesses that cannot be addressed directly.

Like any technology, adjusting RFID security to the appropriate level requires striking the right balance between the **value of the assets to protect,** the possible damages an attack could generate, and the risks. Key factors to consider include the potential impact on privacy when information related to individuals is used. Strategies to enhance the level of security include investing in more secure RFID, associating RFID with non-RFID security controls or using other technologies than RFID.

As RFID technology is still young and evolving, innovative and unpredicted cracking techniques are likely to emerge. **Review and reassessment** of RFID systems is key for deciding where security investments should be made to deal with evolving risks.

Privacy aspects

Potential risks to privacy are generally **important concerns** for individuals and organisations. Key characteristics and functionalities of RFID technologies have the potential to offer benefits (*e.g.* convenience, expediting processes) as well as to foster misperceptions and to impact privacy. RFID systems that collect data related to identified or identifiable individuals raise specific privacy issues that should be considered as a priority challenge to the adoption of the technology in a large

number of areas. In most cases, the potential invasion of privacy through the use of RFID depends on both the technology used and the context.

Invisibility of the data collection may be the primary characteristic of RFID that raises concerns. It is also a risk multiplier for the potential privacy challenges associated with the use of the technology. RFID might reveal to third parties information about objects carried by individuals without their knowledge. It might allow inferences enabling links to more information on the individual and more precise **profiling**: for example inferences made from multiple tags carried by an individual or from sensitive data, such as biometrics in an unsecure RFID passport, or from tagged medicines. Such a scenario would require the presence of readers in
° ¤ ¡ ˙ ° Š £ ¯ ˙ ¡ ª ² ¥ ® « ª © ¡ ª ° ˙ Š ¯ ˙ ³ ¡ ¨ ˙ ˙ Š ¯ ˙ ° ¤ ¡ ˙ œš ¬ š œ¥ °
« › ¦ ¡ œ° ¯ ˙ ° Š £ ˙ ¥ ª ¢ « ® © š ° ¥ « ª ˙ ¥ ª ° « ˙ © ¡ š ª ¥ ª £ ¢ ± ¨ ˙ Ÿ š ° Š

Likewise, **tracking** in real time or after the fact may be the primary functionality of RFID that raises concerns. In particular, because of the invisibility of the technology, tracking of individuals could happen without their knowledge, if they are provided with hidden tags or tags that are not sufficiently secured. In other cases, tracking people could also be the objective of the RFID application (*e.g.* tracking children in an amusement park).

° ª « ° ¤ ¡ ® ˙ œ« ª œ¡ ® ª ˙ ¥ ¯ ˙ ° ¤ š ° ˙ ¥ ª ° ¡ ® « ¬ ¡ ® š › ¨ ¡ ˙ « ¬ ¡ ª
and therefore multiply the collection and processing of personal information. Pervasive RFID taking advantage of **interoperability** and ubiquitous Internet connectivity is often described as an inevitable future, though there are currently few examples of open loop systems.

In cases where RFID systems collect data which is associated with an identified or identifiable individual, the **OECD** *Privacy Guidelines* provide a useful framework.

When an RFID system processes personal data, **transparency** of the purpose of the processing and **consent** of individuals are essential. Beyond basic data protection information, privacy notices may usefully include further information such as *i)* the existence of the tags, *ii)* their content, use and control, *iii)* the presence of readers; *iv)* the reading activity, *v)* the ability to disable tags and *vi)* where to obtain assistance. Innovative means of informing individuals efficiently could be explored. Continued stakeholder dialogue between stakeholders, across sectors and in each of the specific application areas, would help clarify or reach a consensus on what information to provide to individuals, the best means to communicate it to achieve efficient transparency, as well as the cases where consent should be or not be required.

Naturally, **security safeguards** are essential for the protection of privacy in RFID systems.

The wide variety of technical configurations and use scenarios make **privacy impact assessments** a good practice for identifying and understanding privacy risks and best strategies to mitigate them in a given system. As for security, because RFID systems are often components of broader information systems, it cannot be expected that all privacy challenges can be solved at the RFID level. A holistic approach to privacy management may be highlighted as a good practice. Such an approach would consider all the components of the information systems involved,

besides the core RFID components as well as the whole life cycle of the tag when it remains functional beyond the reach of the data controller.

The choice of the RFID technology to be used in a system influences the protection of privacy just as it impacts the security of the system. **Privacy by design** or embedding privacy in the design of the technology and of the systems can significantly facilitate the protection of privacy and foster trust in RFID systems. Efforts to develop **RFID privacy enhancing technologies** are ongoing and could be encouraged. Techniques such as data minimisation and anonymisation can be applied to RFID. Strategies to provide incentives to industry and business for designing and using RFID technologies that include sufficient privacy protections could be pursued. Nevertheless, as for security, privacy protection should not solely rely on technical measures but rather on a mix of technical and non-technical safeguards.

Some parties do not associate tag data with individuals yet provide them with consumer goods tagged with functional RFID tags that they or third parties could later read. It could be suggested that such parties take responsibility for either deactivating the tag or providing information to individuals regarding the presence of the tags, the privacy risks associated to them and the means to prevent or mitigate such risks.

Finally, and more generally, RFID is not well understood by individuals. Increasing the level of **awareness and understanding** about RFID, its possibilities and limitations as well as benefits and risks, can contribute to reducing this perception issue. It may also help individuals make appropriate choices and support efforts by organisations to deploy privacy friendly systems.

Conclusion

Security and privacy issues in relation to RFID infrastructures and related software should be addressed by all stakeholders before widespread deployment of the technology.

The OECD *Security Guidelines* provide a framework for developing a culture of security for RFID systems whether they process or not personal data. The OECD *Privacy Guidelines* also provide a useful framework for guiding the implementation of RFID systems that collect or process personal data.

However, dialogue is still necessary to clarify or to reach a consensus on a number of points, such as *i)* how to apply the concepts of personal data and data controller, *ii)* the nature of the information to provide to individuals and the best means to communicate it to achieve efficient transparency and *iii)* the cases where consent is needed.

Several concepts and approaches reflected in the 2002 *Security Guidelines* could be adapted to support the implementation of the OECD privacy principles, reinforce their effectiveness and help develop a culture of privacy for RFID systems. They include awareness raising initiatives, risk reduction methodologies (*e.g.* privacy impact assessments) and initiatives to integrate security and privacy protections in the design of RFID technologies and systems.

© OECD.2008

Introduction

Background

The OECD Information, Computer and Communications Policy (ICCP) Foresight ⁄ « ® ± © ˙ « ª ˙   & š Ÿ ¥ « ˙ ⁄ ®¡ − ± ¡ ª œµ ˙ Ł Ÿ ¡ ª ° ¥ ¢ ¥ œš ° ¥ « ª ˙   & ⁄ Considerati« ª ¯ ˙ ¥ ª ˙ # œ° « › ¡ ®˙   ˙ ¤ ¥ £ ¤ ¨ ¥ £ ¤ ° ¡ Ÿ ˙ ˙ ° ¤ ¡ ˙ technologies as well as new privacy and information security challenges associated with these technologies. It also signalled that RFID could be seen as the first illustration of intelligent ª ¡ ° ³ « ® § ¡ Ÿ ˙ ¯ ¡ ª ¯ « ® ˙ ° ¡ œ¤ ª « ˙ « £ ¥ ¡ ¯ ˙ ° ¤ š ° ³ « ± ¨ Ÿ ˙ ¡ « ¢ ˙ ° ¤ ¥ ª £ ¯ ˙   (¤ ¡ ˙ ± ¯ ¡ ˙ « ¢ ˙ & ⁄ Ł ˘ ˙ ¥ ¯ ˙ ¡ ´ ¬ ¡ œ° ¡ Ÿ ˙ ° « ˙ ¢ « ° ¡ œ¤ ª « ˙ « £ ¥ ¡ ¯ ˙ š ª Ÿ ˙ ± ° ° ° ¥ © š ° ¡ ¨ µ ˙ œ« ª ° ®¥ › ± ° ¡ ˙ ° « ˙ ®¡ ˙ through whic¤ ˙ š ¨ © « ¯ ° ˙ ¡ ² ¡ ®µ ˙ š ¯ ¬ ¡ œ° ˙ « ¢ ˙ š ª ˙ ¥ ª Ÿ ¥ ² ¥ Ÿ ± š ¨ ˙ ¯ be linked to an omnipresent, 24/7 global network.

Building on the interest generated in the ICCP Forum, further research on RFID was included in the OECD 2007-2008 programme of work:

‹ The Working Party on Information Security and Privacy (WPISP) undertook work on RFID and sensor-based computing within the broader context of pervasive sensors and networks with a view to exploring whether OECD Security and Privacy Guidelines would be challenged by these new technology trends, and

‹ The Working Party on Information Economy (WPIE) undertook work on the economic aspects of RFID.8

In October 2006, the WPISP discussed a preliminary report by the Secretariat exploring information security and privacy issues raised by RFID, sensors and pervasive networks technologies. It recognized that RFID and sensors are at two different stages of development and deployment. Though RFID technologies are evolving and progressing at a fast pace, they have already reached a certain level of maturity and are being deployed at small, medium and large scales in many countries, in several sectors and for various applications. They already raise security and privacy issues. Other sensor and sensor network technologies that monitor environmental parameters and communicate sensed data to other connected devices are less mature and generally deployed on a much smaller scale for applications that rarely affect individuals. Their widespread adoption is still to come, the applications and sectors that will drive that adoption are unknown, and the specific privacy and security issues they could raise are speculative. Specific privacy and security issues raised by pervasive RFID are also yet to come. Therefore, the WPISP agreed that work in 2007 would address issues raised by the use of RFID in the short term. Issues raised by pervasive RFID and other sensor-based technologies in the longer term would be addressed at a later stage.

---

8. OECD, 2007b and 2007c.

This report on RFID, Information Security and Privacy underscores the important cross-cutting nature of the security and privacy work of the WPISP. Identity management, authentication and malware all have implications for RFID and other similar technologies. For example, RFID tags can store important personal data and be linked to databases holding personal data. RFID tags are increasingly used to authenticate people and can include biometrics or other authenticating information in large scale identity systems such as passports or national identity cards. Furthermore, &⁄Ł˘˙°š£¯˙œ«±¨Ÿ˙³¡¨¨˙›¡˙±¯¡Ÿ˙š¯˙š°°šœ§˙²¡œ°«®¯ illustrates the continued importance of addressing security and privacy issues jointly and in close connection with the evolution of new communications technologies and applications.

Although their creation dates back to the Second World War, RFID technologies have in a few recent years experienced a rapid evolution and broad implementation throughout the economy. As intelligent sensor technologies continue to develop and ©šµ˙˙¥ª˙œ«ª¦±ªœ°¥«ª˙³¥°¤˙&⁄Ł˘¯˙˙œ®¡š°¡˙šª˙˙Łª impact of these technologies on the Internet and society be recognised. In this context, the findings of this study will also inform the 2008 Oɪ˛˘˙!¥ª¥¯°¡®¥š¨˙«ª˙˙(¤¡˙ °¤¡˙Łª°¡®ªª¡°˙ɪœ«ª«©µ˙˙˙

Objectives and scope

This paper seeks to clarify the capabilities of RFID in the short term and to identify the information security and privacy challenges raised by this technology, the implications of which may not always be reflected in existing instruments or policies. The OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Security Guidelines)* and the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)* serve as a reference point throughout the analysis. This paper aims at informing the further development of policy guidance by the WPISP in this area, that will be provided in a separate document, jointly with conclusions of the paper developed by the WPIE on business and government applications of RFID, economic impacts, and government policies to develop and diffuse RFID and related technologies.

The first section of this paper aims to provide an understanding of RFID which is a broad and somewhat vague concept used to refer to technologies that enable data collection, through use of contactless electronic tags and wireless transmitters (readers), for identification and other purposes. The second section focuses on information security and privacy issues related to RFID that are already present or likely to be raised in a three to four year time-frame as well as on possible solutions to address them.

Although RFID is seen as a subset of sensor-based computing, this paper does not address this broader category that also encompasses other technologies collecting information from the environment without tag devices. Nor does the paper examine issues that may arise when RFID becomes ubiquitous, is used in a manner that is not anticipated today, or in connection with other sensor-based technologies. These issues will be a topic for future work.

1. Understanding RFID

RFID has been described as the ³ « ® ¨ Ÿ ¯ ˙ « ¨ Ÿ ¡ ¯ ° ˙ ª ¡ ³ ˙ ° ¡ œ ¤ ª « ¨ « £ œ š ª ˙ › ¡ ˙ ° ® š œ ¡ Ÿ ˙ › š œ § ˙ ° « ˙ ° ¤ ¡ ˙ ¯ ˙ ³ ¥ ° ¤ ˙ š ¬ ¬ ¨ ¥ œ š identification of military aircrafts. The first commercial applications appeared in the 1960s in the area of electronic article surveillance to fight against product theft; an application that is still very much used today. Advances in semiconductor technologies led to significant improvements of the technology. Within the same time-frame, commercial success of the marketed applications generated a dramatic reduction of cost and an ever-increasing interest from businesses.

There are many indications that the proliferation of applications using RFID technology is only at its beginning. Figures provided by market analysts predict a huge market increase over the coming decade. According to a Gartner study (2005), ° ¤ ¡ ˙ & ∕ Ł ˘ ˙ © š ® § ¡ ° ˙ ¯ ˙ ® ¡ ² ¡ ª ± ¡ ˙ ˙ ¤ š ® Ÿ ³ š ® ¡ ˙ ˙ š ª Ÿ ˙ ¯ « ¢ ° between 2004 and 2005 (representing USD 504 million in 2005) and will be worth USD 3 billion by 2010. Research firm IDTechEx (2006a) predicts a global market for RFID including systems and services of USD 26.23 billion in 2016 (compared to an estimated USD 2.71 billion for 2006) and a total number of tags delivered of 585 billion, 450 times the amount of 2006. Benefits of RFID technology for business and individuals are very promising (OECD, 2006a).

One important driver for market growth today is that of improving traceability of goods in the supply chain in order to increase supply chain efficiency, reduce theft and fraud, and realise significant cost savings. In addition, many other types of RFID applications have been reported, and the use of RFID technology is now common in areas including passports, hospitals, transportation, ticketing, libraries, museums, counterfeiting, baggage tracking in airports and livestock tagging. With such widespread adoption, it is likely that RFID will affect business and government processes, as well as the lives of individuals and consumers. As stated by the European Article 29 Working Party[9] ˙ ° ¤ ¡ ˙ ¯ ¬ ¡ œ ¥ ¢ ¥ œ ˙ ¢ ± ª œ ° ¥ « can deliver in different sectors is also increasing and its possibilities are just › ¡ £ ¥ ª ª ¥ ª £ ˙ ° « ˙ ¡ © ¡ ® £ ¡

The use of RFID in the global supply chain requires a high degree of reengineering of complex business processes and it is not expected that RFID will become ubiquitous in the short-term at a level that would considerably impact society (*e.g.* item-level tagging or generalised usage of RFID after the point of sale, etc.). However, it is likely that the number of RFID applications will increase in many

---

9. The Article 29 Working Party is the independent advisory body on data protection and privacy in the European Union. It gathers representatives from European data protection authorities. It was established by the Article 29 of the European Directive 95/46/EC.

different areas, as the aforementioned figures suggest, and that the technology will evolve, enabling new applications.

One of the main findings of the ICCP Foresight Forum on RFID in October 2005 was that privacy and security are key challenges to the widespread adoption of RFID that need to be addressed. Understanding the technology, its capabilities and limitations, helps prevent understating or overestimating these risks. This section provides a general and conceptual overview of the technology, the characteristics of tags, readers and the environment in which RFID technologies operate.[10]

1.1. A broad concept for a complex technology

RFID is a convenient and popular concept to qualify a technology with many ¢šœ¡° ˙ ' (¤¡ ' ¡ ⁄ ®¡®⁺ ±¡ ¯¥œµ ¨ Ł ¥¡šˀ¥¥¢¥œš°¥« ª ˙ ®¡ ¢¡ ®¯ the technology: *i)* a technical aspect: radio-frequency and *ii)* a particular function enabled by the technology: identify objects, animals or people carrying or embedding a tag. In so doing, the term RFID can be misleading: RFID communication is not always based on radio-frequency communications — it can use electromagnetic induction — and RFID can be used in contexts in which identification is just one function among others. For example, RFID enables tracking, a function that has considerable economic and social implications. Further, some RFID tags can write data received from a reader onto their memory, as do some tags equipped with sensors to monitor environment conditions such as light, sound or temperature.

RFID would be better described as a technology that enables data collection with contactless electronic tags and wireless transmitters (readers) for identification and other purposes. Such a broad definition does not necessarily reflect the terminology used in international standards. Nonetheless, it grasps the breadth of RFID technologies.[11]

As described below, other factors cloud a clear definition of RFID. For example, different types of technologies may be called RFID, either because they are based on radio communications, or operate in the usual RFID frequency range, or perform similar functions. Sometimes, businesses associate the technology, products or ¯¡ ®²¥œ¡ ˙ ° ¤¡µ˙ ¥©¬ ¨ ¡acronym°for marketing or public image⁄ Ł ˘ purposes and this can skew public perceptions.

Understanding technology capabilities or limitations helps avoid unreasonable fears or unrealistic expectations.

RFID includes a software dimension with, for example, middleware components, back-end applications, communication protocols, etc. This dimension should not be neglected for a good understanding of the technology. However, the specificity and novelty of RFID lies in its hardware component (*e.g.* RFID tags, readers and

---

10. For a more detailed understanding of how the technology works, see, for example, Finkenzeller, 2003 and Lahiri, 2005.

11. For example, systems based on ISO 14443 standards are often not called RFID systems by ¡ ⁄ ¬¡ ®°˙ ' › ±° ˙ ˛ «ª ˙ š œ° ¨ ¡ ˙ ¥ªˀ¡ £®š ˀ¡ Ÿ ˙ œ¥®œ±¥˙ ˙ œš ®Ÿ fl« ³¡ ²¡ ® ˙ ³¤š° ¡ ²¡ ®µ › «Ÿ µ ˙ œš ¨ ˙ ˙° «Ÿ šµˀš ˙ &⁄ Ł ˘ ¬š distinctions are very subtle for the general public.

electromagnetic communication) which are governed by the laws of physics, like any other hardware components. This is a major difference with software technologies, such as data mining for example, which are governed by rules developed by engineers in the form of standards and as such, are mostly limited by their imagination.

The experience of information technology has been that many limitations are transient and overcome through new technological developments. For most information technologies, engineers have not yet approached theoretical limits, as exemplified by the Internet. This suggests that RFID technologies will also experience technological progress, that the current limitations of RFID technology will diminish and that some technology features that are limited and therefore acceptable today will, sooner or later, face technological breakthroughs that will remove these limitations. Tag and reader size, along with communication range are typical examples. Admittedly, technologies will continue to evolve, but the laws of physics will also continue to set theoretical limits on what the technology can and cannot perform. It is therefore important to understand where these boundaries set by laws of physics lie. Clarifying what characteristics of RFID are subject to technological evolution or not helps define adequate policy and may remove obstacles to acceptance by individuals without impeding innovation.

For scientists and other technical experts, RFID is an information technology defined in many standards. For example, the set of standards adopted by the International Organization for Standardization (ISO) is considered by some to be &/Ł ˘ ¯ · © š ¥ ¹² Several other standards apply to RFID, the list of which evolves continuously.[13]

Some technologies are occasionally presented as alternatives to RFID. One could ²¥¡³˙°¤¡¯¡˙š¯˙²š®¥š°¥«-&/Ł˘«¢˙˙°(¤q¡˙µœè«¥ªªœœœ¨±°Ÿ¡˙«"®¡˙š Communication (NFC), RuBee, ZigBee, Wi-Fi, Ultra Wide Band (UWB) and innovations ¯±œ¤˙š¯˙fl$˙«°˙˙!¡©«®@¡˙'«¢˙˙e.g. RuBee) are not fully «˙«£¥¡¯˙ standardised. Others (*e.g.* NFC) are not identified as RFID by their promoters for reasons that may include public perception considerations. Yet others (*e.g.* Wi-Fi) are related to RFID from a functional perspective rather than a technical one.[14]

Figure 1. RFID standards, from the core to the boundaries of the concept

See Annex I and II for the references of the standards
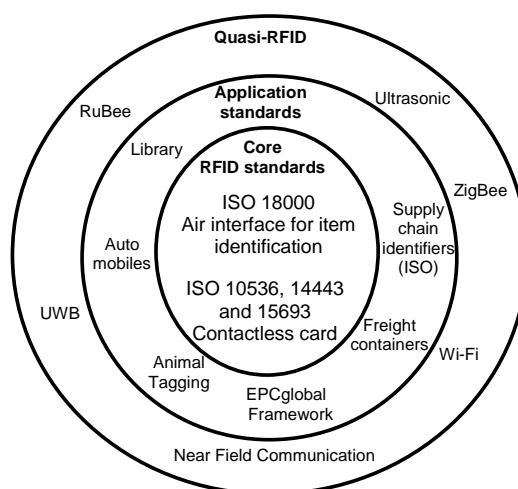
1.2. Hardware components

Tags and readers are core hardware components of an RFID system.

1.2.1. Tags

Tags, also called transponders, can be classified according to a number of characteristics. A distinction is usually made between passive and active tags. Memory capacity and read-write capability are also useful distinguishing factors. Tags of the future will certainly introduce new possibilities. Tags should not be confused with the objects to which they are attached or in which they are embedded.

1.2.1.1. Passive or active tags

Passive tags do not have an internal source of power and cannot send outbound signals without receiving energy from a reader. They use an incoming radio frequency signal to power up an integrated circuit and transmit a response. Their antenna must be able to both receive power from an incoming signal and transmit an outbound signal (see below). They can be as small as 0.15 mm (Figure 2, picture on the right) and as large as a postcard, depending to a large extent on the size of their antenna. Their lifetime is almost unlimited: they can be reactivated years after being manufactured. Systems operating in the Low Frequency (LF) and High Frequency (HF) bands are passive systems. Systems operating in the Ultra-High Frequency (UHF) and microwave frequency bands can be passive or active systems.

Figure 2. RFID tags

Left: Item level passive tag

Source: Left: Metro Group Future Store website, right: Hitachi. [15]

Unlike passive tags, active tags have their own energy source, to power the integrated circuit, which generates an outgoing signal. Compared to passive tags, this additional energy provides active tags with several advantages and has several consequences, in particular (QED Systems, 2002):

‹ *Signal strength*: active tags can receive very low power signals from the reader. Passive tags require very strong signals from the reader, up to 1 000 times the power level necessary for active tags, and the strength of the signal they return is very low.

‹ *Initiation of the communication*: passive tags require a reader to first send a signal in order to communicate. Active tags can initiate the communication. For example, active tags can be programmed to send data (*e.g.* environmental sensor data) at specific times or when external events occur.

‹ *Tag-reader distance* is shorter for passive tags than for active tags. Tags can be read from a few centimetres away, to a few meters for passive tags, and up to hundreds of meters for active tags. Reader distance depends on various of a passive tag, 16 times more power is required from the reader. By contrast, doubling the reading distance of an active tag only requires four times the power, since active tags benefit from their onboard battery.

‹ *Environmental sensors*: passive and active tags can be associated with sensors to monitor the environment. However, passive tags can only use their sensor capability when a reader is sending a signal. By contrast, active tags can continuously monitor the environment, regardless of the presence of a reader field, store sensor data and timestamp information, and send it to a reader at a specific time or when requested.

‹ *Read/Write capacity*: technology is available to enable passive and active tags to store information sent by the reader. However, energy constraints typically limit data processing features for passive tags which, in addition, do not usually feature large memory space. Data processing capabilities for active tags can include the use of more complex protocols, which limits, for example, transmission errors.

---

15.   The Hitachi chip is capable of transmitting a 128 bits (10^{38}) unique ID number. It was used in the 22 million tickets issued for the 2005 World exposition with a 0.001% incidence of ticket recognition error. See www.hitachi.com/New/cnews/060206.html.

ª ˙ ° ¤ ¡ ˙ « ° ¤ ¡ ® ˙ *lifetime* is limited to that of their battery, which itself depends on how often the tag is requested to process and/or send information.[16] Last, but not least, active tags are *larger* and *more expensive* than passive tags.[17] It is anticipated that in order to realise the full potential of item-level tagging, and thus enabling RFID to become more widespread, tags must become much cheaper than the current pricing. Some experts estimate cost-effective tags will enter the market in a couple of years, and will have a major impact on the efficiency and economy of the retail industry.

1.2.1.2. Tag Memory capacity

Another distinction between different types of tags can be made according to the © ¡ © « ® µ ˙ œš ¬ š œ¥ ° µ ˙ « ¢ ˙ ° ¤ ¡ ˙ š £ ¯ ˙ œ¤ ¥ ¬ ˙ (µ ¬ ¥ œš ˙ ˙ © identification tag is 64 bits to 1 kilobyte. More expensive tags, typically active tags, can hold more than 128 kilobytes.[18] Basic item-level tags used for item-level retail tagging ± ¯ ± š ¨ ˙ µ ˙ ¤ « ¨ Ÿ ˙ ˙ › ¥ ° ¯ ˙ ˙ › µ ° ¡ ¯ ˙ « ¢ ˙ Ÿ š ° š ˙ ± ¯ ¡ Ÿ identifier.[19] Passport RFID tags t µ ¬ ¥ œš ¨ ˙ µ ¯ ° « ® ¡ ˙ ° ¤ ¡ ˙ ® š ² ¡ ¨ ¡ ® ¯ ˙ › optionally, iris data and/or fingerprint) and passport data into a 32 kilobytes memory chip.

1.2.1.3. Tag memory capability

Read-« ª ¨ µ ˙ ° š £ ¯ ˙ š ®¡ ˙ › ± ®ª ¡ Ÿ ˙ « ª œ¡ ˙ afterwards by ¥ ª ¢ « ®© š ° ¥ « readers but cannot be overwritten or erased. However, data stored in read-write tags can be read, modified and erased by readers. Some critics find this to be a mislabelled term as readers have in this case the capability to both read and write.

Read-only passive tags with low memory capacity are well-suited for item, case or pallet-level tagging of goods. When the chip only stores a unique identifier, all other information associated with the item can be stored in databases. Therefore, this solution does not require being able to write onto the chip, but instead, requires a connection to the database when information beyond an item number is needed at a given collection point in the supply chain. Different chips used in different contexts can have much more memory capacity and read/write capacity. This can be useful, for example, when no connectivity to a database is possible or desirable, when the tag is re-used, or for applications with purposes beyond simple identification (FTC, 2005, p.7). For example, to contain an up-to-Ÿ š ° ¡ ˙ ¤ ¥ ¯ ° « ®µ ˙ « ¢ ˙ š ˙ ¬ š ° ¥ ¡ ª ° ˙ ˙ › « Ÿ µ ˙ ° ¡ © ¬ ¡ would need to have read/write capability. Finally, some chips may be hybrid, offering some memory space for read-only operations and some memory space for both reading and writing.

---

16. In some configurations, an active tag could live up to 10 years on its battery.

17. EUR 5 to hundreds of EUR versus under EUR 0.50 for passive tags (IDTechEx, 2005).

18. ˙ § ¥ ¨ « › µ ° ¡ ¯ ˙ © š µ ˙ ¯ ¡ ¡ © ˙ ² ¡ ®µ ˙ © š ¨ ¨ ˙ œ« © ¬ š ®¡ Ÿ ˙ ° « ˙ « ˙ players. However, the first version of the IBM PC launched in 1981 was shipped with only 16 kilobytes memory expandable to 256.

19. See Annex IV for a description of EPCglobal electronic product code structure.

1.2.1.4 *Auto-ID Labs/ EPCglobal classification of tags*

The Auto-ID Labs and EPCglobal have developed a tag classification. This classification has been refined with time (Table 1) and is often referred to in literature on RFID.

Table 1. Auto-ID labs RFID tags class structure

Class	Description
0	ID only, programmed at fabricator; read-only in the field
1	ID only, Write Once, Read Many (WORM) in field
2	Class 1, plus additional user memory and/or encryption
3	Class 2, plus battery-assist and sensors
4	Active (battery-powered) tags
5	Class 4, plus reader capability

Source:. EPCGlobal

Table 2. Differences between Active and Passive RFID technologies

	Passive RFID	Active RFID
Tag Battery	No	Yes
Tag Power Source	Energy transferred from the reader	Internal to tag
Availability of Tag Power	Only within the field of an activated reader	Continuous
Required Signal Strength from Reader to Tag	High (must power the tag)	Low (only to carry information)
Available Signal Strength from Tag to Reader	Low	High
Communication Range	Short or very short range (3m or less)	Long range (100m or more)
Tag lifetime	Very long	Limited to battery life (depends on energy saving strategy)
Typical tag size	Small	Large
Multi-Tag Collection	- Collects hundreds of tags within 3 meters from a single reader - Collects 20 tags moving at 8 Km/h or slower	- Collects 1000s of tags over a 28 000 m² region from a single reader - Collects 20 tags moving at more than 160 km/h
Sensor Capability	Ability to read and transfer sensor values only when tag is powered by reader; no date/time stamp	Ability to continuously monitor and record sensor input; data/time stamp for sensor events
Data Storage	Small read/write data storage (Bytes)	Large read/write data storage (KBytes) with sophisticated data search and access capabilities available
Typical applications	Rigid business process, constrained asset movement, basic security and sensing. Simple cargo security (one time tamper event detection), substantial business process impact. Individual item tagging, luggage, boxes, cartons, pallet, printed labels	Dynamic business process, unconstrained asset movement, security/sensing, data storage/logging Intermodal container, rail car Area monitoring, high speed multi-tag portals, sophisticated cargo security applications (continuous tamper detection, date/time stamp), electronic manifest
Cost	Low (below 0.5 EUR)	High (above 5 EUR, up to hundreds)

1.2.1.5 Future tags

Research continues in the area of RFID tags. For example, some analysts predict large success for chipless RFID tags, which do not contain a silicon chip and can be printed directly on products and packaging at very low cost (IDTechEx, 2006b).

1.2.2. Readers

&¡š Ÿ¡ ®⁻ ⁻ ³ ¤¥œ¤ š ®¡ « ¢are¡complementary¡toÁtags and¤ °¡ ®®« £š ° can be as technically diverse as tags. In a basic scenario, a reader sends a pulse of ¡ ª¡ ®£µ ° « °ª¤¡ ¢°«š®£ °š¤ª¡Ÿ °¨š¥£⁻ °¡ ®¡ ⁻¬« ª¡ (¤¡ °š ⁻¡ ªŸ⁻› š œ§ š ®¡ ⁻¬« ª¡ ° ¤š° œ«ªš¥ª⁻ ° ¤¡ °š£ ¥ª ¢« ®©š°¥« ª ⁻¨šⁿ⁻¥©¬¡¡ &∕Ł�‘⁻µ⁻°¡ © ⁻ ⁻ ° ¤¡ ®¡šŸ¥¥ off switch. In more sophisticeš°¡Ÿ ⁻µ⁻°¡ ©⁻ ⁻ -frequency signal can ® ⁻ ®šŸ¥¥« contain commands to the tag, instructions to read or write tag memory, and even ¬ š⁻ ⁻ ³ «20 The reader can emit the signal permanently, thus always searching for tags present, or the signal can be triggered by an external event such as an operator switch, to save energy and minimise interferences.

&¡š Ÿ¡ ®⁻ ⁻ ¥¶¡⁻ Ÿ¡ ¬¡ ªŸ⁻ «ª ©šµ ⁻¤š®š ⁻ ¥¶¡ š that of a personal assistant or personal computer (Figure 3). Readers can embed GPS capabilities and connectivity to information systems and networks. The cost varies from USD 100 to USD 1 000 for readers of passive tags to USD 1 000 to USD 3 000 or more for readers that communicate with active tags over long distances (RFID Journal, n.d.).

Figure 3. RFID readers

Handgun type reader (left), computer style reader (centre) and ultra small RFID reader (12 mm x 12 mm x 2 mm) (right)

Sources: Intermec (left), Alien Technology (center) and Innovision (right).

1.3.   Electromagnetic communication

The transmission of information between tags and readers relies on the laws of electromagnetism. The laws of physics that apply to RFID are the same as those that apply to any radio system: to operate, the receiver on the tag and reader must be

---

20.   Garfinkel, 2005, p.20.

able to detect a signal transmitted by the respective reader or tag above the level of background environmental noise.

Designers, developers, vendors and operators of RFID systems must contend with a large number of parameters for the systems to be operational. Frequency of operation and the physics of energy and information transmission are critical to &⁄ Ł ˇ ` ¯ µ ¯ ° ¡ © ¯ ` ¢ ± ª œ° ¥ « ª ¥ ª £ ` # ° ¤ ¡ ® ` ¥ ©¬ « ®° Š ª ° ` ¢ s interferences, reflection, absorption and mode of communication (half or full duplex). All these elements determine the range of operation of a system.

1.3.1.   *Frequency range*

Each RFID system operates within a given frequency range. The frequency range in which a RFID system operates determines key capabilities and limitations in the system, summarised in Table 4 below. For example, the higher the frequency, the shorter the wavelength and the harder for a radio signal to go around or through obstacles to reach a receiver. Some of these limitations are interwoven with other technical characteristics introduced below.

(¤ ¡ ` ° ¡ ® ©⁄ ® ¡ &‒ Š± Ÿ¡ ¥ª «œ µ ` ± ¯ ¡ Ÿ ` ¥ ª ` &⁄ Ł ˇ ` ® ¡ ¢ ¡ ® ¯ ° ° « ` within the radio frequency spectrum.[21]

Figure 4. Electromagnetic Spectrum Ranges, Frequencies, Wavelengths and energies

CLASS	FREQUENCY	WAVELENGTH		
γ	300 EHz	1 pm	The first column (colored) on the left represents the frequency ranges.	Radio waves: EHF = Extremely high frequency (Microwaves)
HX	30 EHz	10 pm		SHF = Super high frequency (Microwaves)
	3 EHz	100 pm	Legend:	UHF = Ultra high frequency
SX	300 PHz	1 nm	` fi š © © š ` ® š µ ¯	VHF = Very high frequency
	30 PHz	10 nm	HX = Hard X-rays	HF = High frequency
EUV	3 PHz	100 nm	SX = Soft X-Rays	MF = Medium frequency
NUV	300 THz	1 μm	EUV = Extreme ultraviolet	LF = Low frequency
NIR	30 THz	10 μm	NUV = Near ultraviolet	VLF = Very low frequency
MIR	3 THz	100 μm	Visible light	VF = Voice frequency
FIR	300 GHz	1 mm	NIR = Near infrared	ELF = Extremely low frequency
EHF	30 GHz	1 cm	MIR = Moderate infrared	
SHF	3 GHz	1 dm	FIR = Far infrared	
UHF	300 MHz	1 m		Audio frequency : 20 Hz 20 KHz
VHF	30 MHz	1 dam		
HF	3 MHz	1 hm		
MF	300 kHz	1 km		
LF	30 kHz	10 km		
VLF	3 kHz	100 km		
VF	300 Hz	1 Mm		
ELF	30 Hz	10 Mm		

Note: EHF and SHF are sometimes considered to be not part of the radio spectrum and form their own microwave spectrum. The radio spectrum is between 9 KHz and 300 GHz.

---

21.   The electromagnetic spectrum is the range of all possible radiations (see Figure 4). The radio frequency spectrum is a portion of the electromagnetic spectrum in which electromagnetic waves can be generated by alternating current fed to an antenna. Radio or electromagnetic waves consist of oscillating electric and magnetic fields generated by an antenna supplied with electric current. The distance between two consecutive waves is called the wavelength. The number of complete oscillation of wavelength (cycle) in a second is represented by the frequency, measured in hertz (Hz), kilohertz (KHz), megahertz (MHz) and gigahertz (GHz). For example, 132 KHz = 132 000 cycles per second.

Source ˙ + ¥ § ¥ ¬ ¡ Ÿ ¥ š ˙ ı ¨ ¡ œ° ® « © š £ ª ¡ ° ¥ œ˙ ' ¬ ¡ œ° ® ± © ˙

Governments have regulated and managed radio spectrum use in terms of operating frequency and power since the early days of radio communications.[22] One objective of such regulation is to share limited radio spectrum resources. Another is to minimise the interference that may be caused by one radio system to another. For example, it is important that RFID systems do not interfere with radio and television, mobile radio services (police, security and emergency services), mobile phones, as well as marine and aeronautical communications. As noted below (1.3.3), for health and safety reasons, regulation also limits power levels.

Table 3.   Frequencies and regions

Low Frequency (LF) 30-300 kHz	125 134 kHz in Canada, Europe, Japan, and the US
High Frequency (HF) 3-30 MHz	13,56 MHz in Canada, Europe, Japan, and the US
Ultra-High Frequency (UHF) 300 MHz-3GHz	433.05 434.79 MHz in most of Europe, US, and under consideration in Japan 865 868 MHz in Europe 866 869 and 923 925 MHz in South Korea 902 928 MHz in the US 918- 926MHz in Australia 952 954 MHz in Japan, for passive tags starting in 2005
Microwaves 2-30 GHz	2400 2500 and 5.725 5.875 GHz in Canada, Europe, Japan and the US

Source: US Department of Commerce, 2005b.

RFID systems operate at Low Frequency (LF), High Frequency (HF), Ultra High Frequency (UHF), and Microwave frequency ranges. Unlike some radio communications systems that operate at licensed frequencies (such as mobile telephony or television), RFID systems operate at specific unlicensed frequencies that are not fully harmonised internationally, in particular in the UHF and microwave ranges. Different frequencies for RFID in different regions can be challenging for those who advocate the deployment of global RFID applications, although technical solutions can cope with a certain level of divergence of frequencies (See Table 3).

1.3.2.   Electromagnetic induction and radio waves

A conductor supplied with electric current radiates energy in the form of radio waves. It also produces a magnetic field around it that can be used to generate electricity by induction. Induction is the creation of electric current in a conductive material (usually a coil) presented within a changing magnetic field. To transmit

---

22.   The first international discussions on the regulation of radio communications took place in 1903 in Berlin. The first radio conference took place in Berlin in 1906.

energy and information to a remote device, RFID systems operating at Low Frequency and High Frequency rely oª ˙ ¡ ¨ ¡ œ° ®« ©š £ ª ¡ ° ¥ œ˙ ¥ ª Ÿ ± œ° ¥ « ª ˙ œ« ± ¬ ¨ ¥ ª £ ˙ š ª Ÿ ˙ &⁄ Ł ˇ ¯ µ ¯ ° ¡ ©¯ ˙ « ¬ ¡ ®š ° ¥ ª £ ˙ š ° ˙) fl ⁄ ˙ radio waves (or radio communications).[23]

Induction and radio waves are two radically different, but related, physical phenomenon that were discovered by a number of scientists in the 19th century. For RFID engineers, they correspond to two very different engineering areas with different capabilities, limitations (*e.g.* operation range) and challenges to address (*e.g.* interferences, absorption, health issues, etc.). A communication system based on induction cannot be transformed into a radio communication system just by changing the frequency of operation and the size of the antenna. There is no simple method to go from magnetic induction to radio wave propagation without reengineering the whole system. In the same way, there is no technological link between an oil lamp and an electric lamp, even though they perform the same function of providing light. They are not the same technology; they face different constraints and do not produce the same light.

1.3.3. *Power level*

The signal transmitted by readers and tags using radio waves is transmitted at a certain power level, measured in watts. The higher the transmitted signal power in the direction of the receiver, the greater the probability that the receiver will be able ° « ˙ Ÿ ¡ ° ¡ œ° ˙ ¥ ° ˙ š £ š ¥ ª ¯ ° ˙ › š œ § £ ®« ± ª Ÿ ˙ ª « ¥ ¯ ¡ ˙ fl « ³ ¡ pose increasing threats to human health: radar, for example, usually operates at very high energy levels and can be dangerous to a person directly in front of an antenna. High power levels also increase the risk of interference with other radio-sensitive equipment. Government regulation in all countries imposes limitations on power levels to safeg± š ®Ÿ ˙ ¬ ¡ « ¬ ¨ ¡ ˙ ¤ ¡ š ¨ ° ¤ š ª Ÿ ˙ ¬ ®¡ ² ¡ ª ° ˙ ¥ induction systems obey the same rules, although in practice short operating distance compensates low power coils on readers.

---

23. Induction provides for the operation of electrical generators, induction motors and transformers. The *induction* phenomenon appears in the area between a reader antenna and less than one wavelength of the radio-frequency wave emitted by a reader antenna. In the RFID context, this region ¥ ¯ ˙ « ¢ ° ¡ ª ˙ œš ¨ ¨ ¡ Ÿ ˙ ª ¡ š ®˙ ¢ ¥ ¡ ¨ Ÿ ˙ ˙ ¨ µ ˙ œ« ª *radio communication* system takes place using propagation of radio waves, just like for a television, mobile phone, radar, and other radio communications. The region in which such propagation hš ¬ ¬ ¡ ª ª ¯ ˙ ª ¯ ˙ « ¢ ° ¡ ª ˙ œš ¨ ¨ ¡ Ÿ ˙ ¢ š ® ¢ ¥ ¡ ¨ Ÿ ˙ ˙ š ¯ ˙ « ¬ ¬ « a magnetic induction phenomenon would take place). Consequently, induction RFID is ¯ « ©¡ ° ¥ ©¡ ¯ ˙ ° ¡ ®©¡ Ÿ ˙ ª ¡ š ® ¢ ¥ ¡ ¨ Ÿ ˙ ° ¡ œ¤ ª « ¨ £ µ ˙ š ª Ÿ ˙ ®š Ÿ techno ¨ £ µ ˙ ˙ fl « ³ ¡ ² ¡ ® ˙ œ« ª ° ®š ®µ ˙ ° « ˙ ³ ¤ š ° ˙ ° ¤ ¥ ˙ ˙ ¡ ®© distinguishing factor is not the range of operation, but instead, the physical phenomenon that is taking place. Neither does it mean that communication based on electromagnetic induction œš ª ˙ ° š § ¡ ˙ ¬ ¨ š œ¡ ˙ « ² ¡ ® ³ ¤ « ¨ ¡ ˙ ª ¡ š ® ¢ ¥ ¡ ¨ Ÿ ˙ š ® actual communication range of electromagnetic induction systems to a much shorter ˙ ± › ˙ ¡ ° ˙ « ¢ ˙ ° ¤ ¡ ˙ ° ¤ ¡ « ®¡ ° ¥ œš ¨ ˙ ª ¡ š ® ¢ ¥ ¡ ¨ Ÿ ˙ ! « ®¡ ˙ « ª ¨ induction and radio waves RFID in Langheinrich, 2007.

1.3.4. Antenna

Tag and reader power level can be considerably enhanced by the nature of their antenna and in particular its design and orientation. Low gain[24] antennas emit radiations in all directions equally (omnidirectional). High gain antennas radiate in particular directions (unidirectional) with a longer range and better signal but must carefully be aimed towards a particular direction. When either the transmitter or the receiver is in movement, it may not be practical to use directional antennas at both ends of the communications link. Antenna design and orientation also influences tag and reader sensitivity.[25]

(š £ ¯ ˙ š ª Ÿ ˙ ® ¡ š Ÿ ¡ ®¯ ˙ š ª ° ¡ ª ª š ˙ ¯ ¥ ¶ ¡ ¯ ˙ š ® ¡ ˙ š ¨ ¯ « ˙ š radio wave RFID systems.[26] In general, electromagnetic induction tags require a smaller antenna[27] than radio wave systems. In some cases, radio tags are sold without an antenna and the size indicated by the manufacturer does not always reflect the size of the actual complete operational tag on an object.[28]

1.3.5. Interferences, attenuation and reflection

As noted above, communications of RFID systems can interfere with other RFID systems, in particular when the transmission power is high. Inductive coupling systems are less susceptible to interference because of higher signal attenuation (see below 1.3.7).

Low frequency signals penetrate liquids more easily because longer wavelength is less susceptible to attenuation. Therefore Low Frequency and High Frequency systems are better suited for tagging objects in environments containing water (like humans or animals). Metal stops radiofrequency signals and reflects them, creating interferences. Progress is being made regarding the management of interferences

---

24. Gain, measured in decibel or db, is a measure of performance of an antenna in a given direction. It is expressed as a value relative to a theoretical reference antenna called ¥ ¯ « ° ® « ¬ ¥ œ ˙ š ª ° ¡ ª ª š

25. Receiver sensitivity depends on the antenna gain and orientation, as illustrated by ¢ ¥ ¯ ¤ › « ª ¡ ˙ š ª Ÿ ˙ ¬ š ® Ÿ › « ¨ ¥ œ ˙ Ÿ ¥ ¯ ¤ ˙ š ª ° ¡ ª ª š ˙ ¯ ± ¯ ¡ Ÿ ˙ ¥ ª ˙ ° ¡ (and importantly their relatively small antennas) is sometimes more difficult to control than that of a television antenna. Often, tag and reader form factor is designed so that the user orientates the tag or the reader properly (*e.g.* tags in smart card and gun type readers) to compensate reading difficulties in basic systems.

26. Radio wave propagation requires antenna systems that are typically half a wavelength of the operating frequency in size: 150 cm at 100 MHz, 15 cm at 1 Ghz, 5 cm at 2.5 GHz, 2.5 cm at 5.8 GHz.

27. (¤ ¡ ˙ š ° ¡ ª ª š ˙ ˙ « ¢ ˙ š ˙ ¥ ª Ÿ ± œ ° ¥ ² ¡ ˙ œ ª ct±a¬cöi¥that˙ œ « © © ± ª ¥ œ generates a magnetic field, as in a wire electrical transformer.

28. The Hitachi µChip tag in Figure 2 (pictured on the right) does not include an antenna (Hitachi, 2003).

created by metallic environments. Low frequency magnetic coupling systems can communicate in a metallic environment under certain conditions.[29]

A wide variety of error-correcting coding techniques can be employed to try to mitigate the effects of noise. The greater the complexity of noise avoidance, mitigation and reduction techniques in data channel engineering, the greater the cost.

1.3.6 . *Half or full duplex communication*

The level of sophistication of the communication depends on whether it is happening in half duplex or full duplex mode. In half duplex, the sender transmits a complete message and does not know if the message has been received until the receiver switches over and replies. In full duplex, both ends of the communication channel are sending and receiving at the same time, enabling real-time communication channel management and more sophisticated protocols. However, sophisticated protocols require more data processing capabilities on the tag side, which implies an increase in power consumption and a higher cost.

1.3.7. *Range of operation*

Two sets of laws limit the operation range of RFID systems: laws of physics and laws of governments (frequency and power regulations). Laws of physics can be expressed according to: *i)* the physics theory as expressed in mathematical equations; *ii)* experiments made in laboratory conditions and *iii)* experiences in an uncontrolled, real life environment. Depending on which of these three frames of reference is used, assessment of the operating range of RFID systems can be very different.

Ranges of operations resulting from controlled laboratory conditions are typically larger than ranges obtained in real life conditions. But they sometimes require settings that would be practically difficult to deploy in real life conditions. For example, an unrealistically heavy and large coil would be necessary to generate a large magnetic field capable of activating a High Frequency tag placed only a few meters away. In addition to complex engineering challenges, cost considerations play also a key role in the availability of equipment operating at enhanced operation ranges. Research is making progress and cost is evolving so that one may expect operation range to improve with time, within the boundaries set by the laws of physics.

The main factor to consider with regard to the range of operation of RFID systems is the type of technology used: communication based on electromagnetic induction is associated with a shorter read range compared with radio communication.[30] In addition, the range of operation of RFID systems depends on a

---

29.   Information regarding the use of UHF tags in water and metal environments can be found in Desmons, 2006.

30.   Radio signal strength quarters every doubling of the distance travelled. The signal strength in magnetic induction is divided by eight every doubling of the distance travelled. See Langheinrich, 2007.

number of factors including transmission power, receiver sensitivity, antenna gain and orientation, and interference. Natural and man-© š Ÿ ¡ ˙ ª « ¥ ¯ ¡ ˙ ¥ ª ° ¡ ® ¢ ¡ ® ¡ ª an important role in radio communications: when distance increases, the level of natural noise remains stable, while the signal strength diminishes. Eventually, the overall noise level prevents detection. The communication range can be further shortened by additional man-made noise in the vicinity of the receiver.

Figure 5. Typical behaviour of the magnetic field strength versus distance (example), for a transmitting antenna with a diameter of 0.8 m.
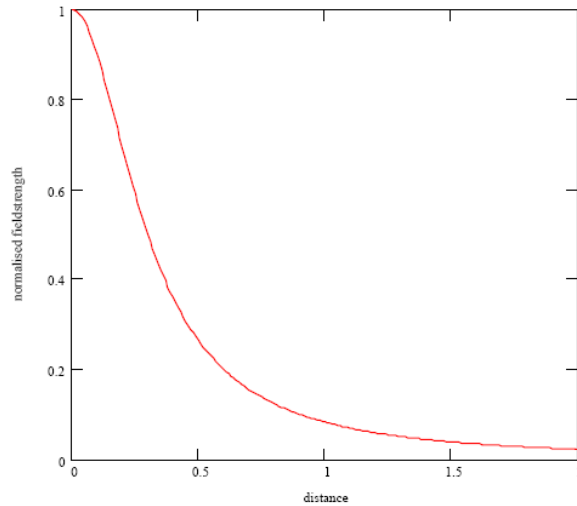
Source: AIM Frequency Forum, 2000.

Following ISO standards terminology, inductive coupling systems are sometimes divided into proximity and vicinity systems. Proximity cards[31] are intended to be used in the 10 cm range (*e.g.* for use with a vending machine) and vicinity cards[32] inside the 1 m range (*e.g.* for opening a parking door without rolling down the car window; ICAO standard for biometric passports mandates the use of ISO proximity cards standard).

Figure 6. Range of operation

Frequency Band	System type	Communication range						
		3 cm	10 cm	30 cm	1m	3m	10m	> 10m
LF	Passive							
HF	ISO 14443							
	ISO 15693							
UHF	Passive							
	Active							
Microwaves	Passive							
	Active							

Typical versus theoretical range attainable in a controlled environment

Source: *Atmel Applications Journal*, 2004.

---

31.   ISO 14443.

32.   ISO 15693.

Active UHF and microwave tags have a considerably longer range of operation than passive tags, since the battery provides more power than what can be drawn from the radio wave signal.

In passive radio systems, the reader to tag signal is usually more powerful than the tag to reader one and can be detected or received over longer distances (see section 2.1. Information Security).

1.3.8.   Summary table

The table below summarises and compares the limits of RFID according to frequency range. It also provides examples of different application areas in which either electromagnetic induction, or radio wave RFID, is likely to be found, as a consequence of the characteristics of each technology.

Table 4. Characteristics of RFID technologies

Parameter	Low frequency (LF)	High frequency (HF)	Ultrahigh frequency (UHF)	Microwave
Frequency range (see Table 3 for precise range per country)	30-300 kHz	3-30 MHz	300 MHz-3GHz	2-30 GHz
Transmission of energy and data	Electromagnetic Induction	Electromagnetic Induction	Radio Waves	Radio Waves
Reading range for passive tags (approx)	Typical : 20 cm. Maximum: 1.2 m	Typical : 20cm Maximum: 1.2 m	433 MHz : 100 m max 865-956 MHz : 0.5 to 5 m	Typical: 3 m Maximum: 10 m.
Moisture	no effect	no effect	negative effect	negative effect
Metal	negative effect	negative effect	no effect	no effect
Aiming of transponder during reading	not necessary	not necessary	sometimes necessary	necessary
Typical transponder shapes	glass tube transponders, transponders in plastic housings, smart cards, smart labels	smart labels, industrial transponders	smart labels, industrial transponders	large-format transponders
Typical application areas	access and route controls, brakes, laundry cleaners, gas readers, animal ID, car immobiliser	laundry cleaners, asset management, ticketing (ski, events, public transport), tracking and tracing, multi-access, library management, passports, payment card	palette tracking, container tracking	road pricing, container tracking, production control

Note: the influence of metal and liquids varies depending on the product. Reading range for active tags varies considerably according to the technology used.

Sources: adapted from BSI, 2005, p.23; Dressen, 2004; Metro Group RFID@Metro web site; Ward, 2006.

1.4. Software and network components

RFID tags and readers are often components of a broader RFID system, which, in turn, is a component of an enterprise information technology infrastructure, often interconnected with other information systems and networks, including via the Internet. Three types of RFID systems can be considered according to their level of connectedness with other systems:

‹ Standalone systems, not connected to other information systems and networks, including within the organisation.

‹ Closed-loop systems that track objects that never leave the company or organisation.

‹ Open-loop systems that involve multiple partners, like a retail chain and its suppliers.

˚ ‾ ˙ ©¡ ª ° ¥ « ª ¡ Ÿ ˙ ¥ ª ˙ ° ¤¡ ˙ # ¸ ˘ ˙ ¬ š ¬ ¡ ® ˙ « ª ˙ &⁄Ł ˘ ˙ ˙ ˘ ® ¥ ¸ « ª ‾ ¥ Ÿ ¡ ³® ˙ the information infrastructures associated with RFID, in particular with UHF RFID, will increasingly be accessed across IP networks, private intranets and the public Internet.

(¤¡ ˙ ª « ° ¥ « ª ‾ ˙ « ¢ ˙ &⁄Ł ˘ ˙ ‾ µ ‾ ° ¡ © ˙ « ® ˙ &⁄Ł ˘ ˙ ª ¡ ° ³ components included in such systems and networks are RFID specific. While tags and readers are obviously core RFID components, some of the other components are actually pre-existing, non-RFID technologies, systems, applications or protocols that either support RFID or are combined with RFID. At this early stage of the RFID policy debate, it is important to clarify which components are actually RFID or RFID specific and which components are not.

The efficiency of RFID systems within the broader IT infrastructure of an organisation depend ‾ ˙ « ª ˙ ° ¤¡ ˙ œš ¬ š œ¥ ° µ ˙ « ¢ ˙ š ª ˙ « ®£ š ¥ ‾ š ° ¥ « ª flows of RFID information efficiently. Middleware components connect the core RFID elements to the enterprise back-end. They enable information to flow from the tagged object to the heart of the company information infrastructure. The proper implementation of middleware components sometimes represents considerable investment and efforts.

Standardisation and interoperability factors also play a key role in the implementation of RFID systems. This is important to recognise in a globalised economy where the supply chain spans across a range of partners who may be spread all over the globe. As noted above, considerable efforts have been made to leverage existing RFID and Internet technologies to create the standards and components for a global architecture capable of conveying object information in real-time as these objects progress through the production supply chain and beyond.

For example, the EPCglobal Architecture Framework includes a set of inter-related standards for hardware, software and data interface for improving the efficiency of supply chains through the use of Electronic Product Codes (EPCs). The ι $ ¸ £ ¨ « › š ¨ ˙ ⁄ ® š ©¡ ³ « ® § ˙ ¡ ª š › ¨ ¡ ‾ ˙ ° ¤¡ ˙ ‾ ¤š ®¥ ª £ ˙ « ¢ ˙ °

---

33. OECD, 2006a, p.18.

trading partners in the global supply chain and tracking individual products in real-time. The Framework includes five categories of components: *i)* the Electronic Product Code (EPC), which identifies the tagged product,[34] *ii)* tags and readers, *iii)* middleware, which communicates the information that is read to EPC information services, *iv)* EPC Information Services[35], that allow trading partners to exchange EPC-related data through the EPCglobal network, and *v)* discovery services, including, but not limited to, the Object Naming Service (ONS), which can be queried with an EPC contained in an RFID tag to return the specific address of the application associated to the product code.[36] The EPCglobal Architecture ∕ ® š © ¡ ³ « ® § ˙ š ¨ ¯ « ˙ ¥ ª œ¨ ± Ÿ ¡ ¯ ˙ ° ¤ ¡ ˙ ¯ authentication ˙ ¢ ® š © ¡ ³ « data protection, and access control.

Other numbering schemes have been proposed for identifying objects, including the IPv6 numbering scheme, which is large enough to handle as much as 430 quintillion identifiers.[37]

---

34. See Annex IV.

35. EPCglobal has recently ratified its open standard for EPC Information Services. See www.epcglobalinc.org/standards/EPCglobal_EPCIS_Ratified_Standard_12April_2007_V1.0. pdf

36. The ONS is a mechanism to discover information about a product and related services. The š ® œ¤ ¥ ° ¡ œ° ± ® ¡ ˙ š ª Ÿ ˙ ¢ ± ª œ° ¥ « ª ¥ ª £ ˙ « ¢ ˙ ° ¤ ¡ ˙ # " ˙ ˙ ¥ ¯ ˙ ² ¡ ® µ Name System (DNS). When queried with an EPC code, the Root ONS directs the query to the servers of the EPCglobal Network member associated to the EPC code. The querying party can subsequently and independently of the Root ONS get the requested ¥ ª ¢ « ® © š ° ¥ « ª ˙ ¢ ® « © ˙ ° ¤ ¡ ˙ ι $˛ £ ¨ « › š ¨ ¯ ¡ ° ³ « ® § ˙ © ¡ © › ¡ ® ¯ maintains is limited to *i)* an EPCglobal issued number (EPC Manager ID) that identifies an EPCglobal Network member and *ii)* the server identifier for that EPCglobal Network member. EPCGlobal contracted VeriSign to operate the authoritative root for the EPC network on behalf of EPCGlobal. See EPCglobal, 2005b, Section 7.3.

37. 3.4 x 1038 addresses. On the use of IPv6 as a numbering scheme for RFID, see *RFID Journal*, 2003; Vadhia, 2004; Le Pallec, 2005.

2. Information security and privacy

RFID technology is at a stage of development where privacy and security have been identified as challenges for its widespread adoption.

Many RFID experts acknowledge that widespread deployment of RFID will take time but that applications that are being deployed and standards that are being designed and adopted are likely to influence the infrastructure to be in use in the next decades.[38] For security expert Ari Juels[39] ˙ ˙ ° ¤ ¡esig&s/of 2005 ˙Ỹwith all of their features and drawbacks ©š µ ˙ › ¡ ˙ ° ¤ ¡ ˙ ¬ ®¡ Ÿ « © ¥Similarly, « ª ¡ ¯ ˙ ¥ ª ˙ participants in the OECD ICCP Foresight Forum recognised that privacy and security should be integrated in the RFID infrastructure before widespread deployment of the technology, rather than having to deal with it afterwards, as has been required for the Internet. It was highlighted that for the Internet, ¯ ¡ œ± ®¥ ° µ ˙ ³ š ¯ ˙ › « ¨ ° ¡ Ÿ š ¢ ° ¡ ®³ š ®Ÿ ¯ ˙ ¥ ª ¯ ° ¡ š Ÿ ˙ « ¢ › ¡ ¥ ª £ ˙ › repeated with ª ˙ š ª Ÿ ˙ ° ¤ RFID. Such a consideration holds true also with regards to privacy protection.

There seems to be an agreement among experts that RFID security and privacy should be an urgent priority for all stakeholders in order to prevent large scale opposition by consumers and individuals, and facilitate the successful roll-out of ¢ ± ° ± ®¡ ˙ &∕ Ł ˘ ˙ ¯ µ ¯ ° ¡ © ¯ ˙ ˙ (¤ ¡ ˙ œ« ¨ ¨ ¡ œ° ¥ « ª ˙ š ª Ÿ ˙ ± ˉ ¡ ˙ through RFID technologies represents a key public policy challenge to the deployment and use o¢ ˙ &∕ Ł ˘ ˙ ° ¡ 40As stated by the European Commission ¥ ª ˙ ¥ ° ¯ ˙ ¸ « © © ± ª ¥ œš ° ¥ « ª ˙ « ª ˙ &∕ Ł ˘ ˙ ¥ ª ˙ ˙ I ± ®« ¬ ¡ ˙ ˙ š ˙ œ ¢ ®š ©¡ ³ « ®§ ˙ ¥ ¯ ˙ ª ¡ ¡ Ÿ ¡ Ÿ ˙ ° « ˙ © š § ¡ ˙ ° ¤ ¡ ˙ œ¤ š « ¯ ¡ consumer organisations consider that, in areas such as retail, there is a potential for public backlash regarding RFID and draw a parallel with such a backlash that happened in the area of genetically modified food.[41] At stake is the capacity of these frameworks to remove obstacles to the acceptance of RFID technology by individuals and to ensure privacy and security in new environments.

2.1. Information security

Academic researchers and security experts, often quoted by the press, have highlighted both theoretical and concrete security weaknesses discovered in some already widespread RFID systems. Annex III provides a selection of exploits which

---

38. US FTC, 2005, p.11, 15; EPCglobal, 2004a.

39. Juels, 2005b.

40. US Department of Commerce, 2005b.

41. Lace, 2004.

suggest that RFID systems can be vulnerable to security attacks, like other information systems, and also that RFID technology is still in its early days.

Some successful attacks targeted RFID products or applications deployed on a large scale[42] and/or could harm businesses and individuals (*e.g.* hotel keys, implantable chips). However, they relate mostly to lower cost RFID products that include either limited or no security feature at all. There are fewer reports of successful attacks against higher cost RFID products that contain sophisticated security features. Therefore it would be misleading to make general statements about the security of all RFID technologies based essentially on experiences with the use of low cost RFID products. To come to any conclusion, a more specific and detailed assessment is necessary.

This section provides a general overview of RFID security challenges and possible solutions. It is not intended to be detailed or comprehensive. In this section, threats are described in very general terms with a few specific examples detailed in Annex III and general risks associated with RFID systems, as well as some of the general security weaknesses that RFID systems might have and that might be exploited, are described in business terms.

2.1.1. Typology of risks

Risks result from threats posed by vulnerabilities or weaknesses that can be exploited and cause adverse effects. There are many ways to describe risks to RFID systems. For example, the US National Institute of Standards and Technology (NIST) Guidelines for Securing RFID Systems (2007) consider risks related to business process, business intelligence, privacy and externality risks (Table 5).

Table 5. Typology of risks by the US National Institute for Standards and Technology

Business process risks	Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.
Business intelligence risks	An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organisation implementing the RFID system.
Privacy risks	Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.
Externality risks	RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets and people.

Source: NIST, 2007.

The German Federal Office for Information Security (BSI) classifies basic types of attacks based upon the data/tag relationship, tag/tagged item relationship and tag/reader relationship (see Figure 8).

---

42.   *E.g.* (¡ ´ š ¯ ˙ Ł ª ¯ ° ® ± © ¡ ª ° ˙ ˉ ¥ £ ¥ ° š ¨ ˙ ' ¥ £ ª š ° ± ® ¡ ˙ (® š ª ¯ « ª Ÿ ¡ ®

**Figure 7. Basic types of attacks relating to data/tag relationship,
tag/tagged item relationship and tag/reader relationship**
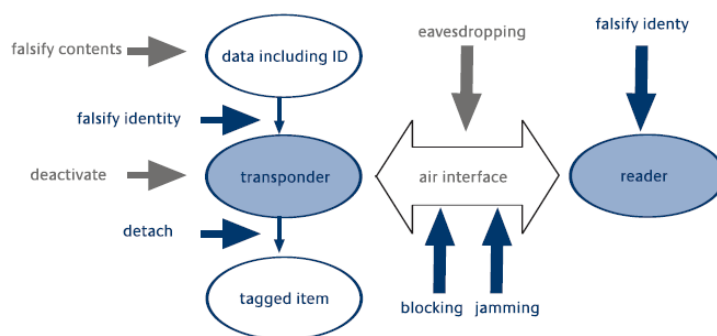
Note: transponder can be used as a more technical term for a tag.

Source: BSI, 2005.

BSI also presents types of attacks according to their purpose: spying, deception, denial of service, protection of privacy[43] (Table 6).

Table 6. Types of attacks according to their purpose

	Spying	Deception	Denial of Service	Protection of privacy
Falsifying content		›		
Falsifying tag identity		›		
Deactivating		›	›	›
Detaching		›		›
Eavesdropping	›			
Blocking		›	›	›
Jamming		›	›	›
Falsifying reader identity	›			

Source: BSI, 2005.

Security challenges raised by RFID can also be structured according to the traditional dimensions of information security: loss of availability, integrity and confidentiality.[44] Examples below help understand the nature of the general risk

---

43.   According to BSI, an attack aiming at protecting privacy could be carried out by an individual believing that his privacy is threatened by the RFID system. Presumably, such an attack would target the RFID system and not the information that may be contained within that system. The RSA Blocker Tag (Juels, 2003) may be an example of a means to perform such an attack.

44.   Availability, integrity and confidentiality are useful conceptual distinctions but, in reality, the separation is often artificial: a failure in one dimension can have consequences in another and therefore the concepts are interdependent and overlapping. Accountability and audit are often associated to these dimensions. They ensure allocation of responsibility for a security control and provide means for monitoring and measuring its effectiveness.

associated with each of these security dimensions and illustrate the potential consequences of attacks. Examples refer to transportation systems (*e.g.* subway access cards), supply chains (*e.g.* tracking of containers, pallets and goods), retail (*e.g.* inventory management, check out, warranty services, medicine tagging), identity documents (*e.g.* passports) and vehicle access or ignition. These applications were not chosen because they are more risky than others but rather because they are common and easy to understand.

Many of the threats and vulnerabilities to RFID systems are common to all information systems. The main component in RFID systems that distinguishes them from others is the transmission of information between tags and readers. But risks related to other, more traditional, components of the system should not be omitted. It is important to note that many security risks become privacy risks when information related to identified or identifiable individuals is involved.

2.1.1.1. Risks related to tags and readers

Many events can disrupt a RFID system. They can be categorised as interference or disruption of either the hardware, or the radio, or the data components of the system. Interference or disruption to the physical components of readers and tags can be deliberate or accidental, overt or covert. Accidental or deliberate disruption of the radio components can be of the reader or tag or both. Deliberate attacks can be active or passive. Interference or disruption on the data components can be of the tag or reader data or both.

```
Interference or disruption of:
      Radio components    ◄───────►    Data components
Can be:
         Deliberate    ◄───────►    Accidental
              Overt    ◄───────►    Covert
          On Reader    ◄───┼───►    On tag
                             Both
If deliberate, it can be:
             Active    ◄───────►    Passive
```
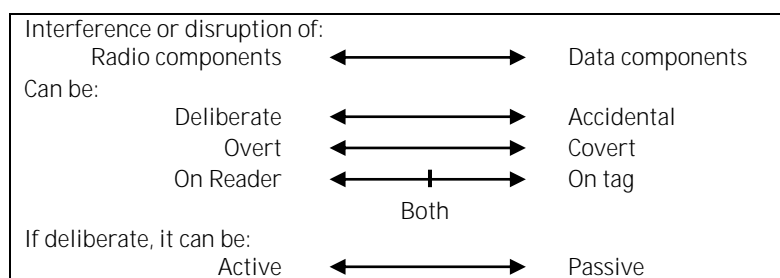
As mentioned earlier, RFID systems, as any information system, include software and hardware components. However, their main specificity lies in the hardware components, namely the tags and readers as well as the methods of energy exchange they use to communicate.

‹   Availability

Availability is the assurance of timely and reliable access to data services for authorised users. It ensures that information or resources are available when required. For instance, Denial of Service (DoS) attacks target the availability of a system. Consequences of disruption of availability of typical RFID systems could be, for example, delays in processing identity documents (*e.g.* disabled RFID passports) thus possibly disturbing airport border control processes, preventing individuals to access public transportation systems (*e.g.* subway access card) or work premises (*e.g.* access control cards), preventing an owner to access his/her vehicle (*e.g.* RFID car keys), preventing automatic processing of medicine information in a health context leading to dangerous errors for patients (*e.g.* medicine tagging).

Threats to the availability of the physical components of a RFID system can be overt or covert. Overt attacks on tags include cutting the electrical circuit on the tag, detaching the tag from the tagged item, discharging the battery of an active tag, or masking the antenna (shielding) with a conductive material or paint. Such strategies could be pursued to evade anti-theft RFID systems in stores. They could also be used for privacy protection purposes: companies have developed RFID blocking wallets (for RFID credit cards) and passport cases that are presented as privacy protective apparel.[45]

Covert attacks can be conducted by overloading receiving components to stop them from functioning or to destroy them, for example by subjecting a passive tag to a high energy field in close proximity. Hackers have demonstrated that a strong energy field generated by an inexpensive, modified, single-use camera flash light can produce this result.[46]

A RFID system can also be compromised by overwhelming the wanted signal at the receiver side (blocking), by preventing the receiving device from decoding the signal (masking) or by disrupting the data communication (jamming). For example, creating an unwanted signal noise in one or all of the RFID system receiver circuits could prevent the wanted reader signal being detected by the tags. A signal can also be tailored to prevent the reader or tags from synchronising with other transmitters, therefore disrupting the wanted signal decoding process.[47] Jamming noise sources can be accidental man-made interferences caused by machines and other electrical equipment. An attacker can also deliberately create jamming noises. In such cases, an unwanted signal competes with a wanted signal so that it is the relative power and geometry (obstacles, distances and orientation) of the wanted transmission versus the unwanted one that determines the degree of disruption. The complexity of this situation is such that a deliberate attack can be difficult to detect. Therefore it might be carried out covertly and be undetected by the RFID system. Both RFID systems using active and passive tags are susceptible to these threats.

‹   Integrity

Integrity is the underlying assurance that data has not been altered during a transmission from the point of origin to the point of reception. Consequences of loss of integrity in common RFID systems could include, for example, delays and misdirection in the supply chain or confusion in retail operations due to corrupt or

---

45.   For example, see DIFRwear website.

46.   RFID Zapper, see https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN).

47.   Decoding is an essential element of signal processing. Detection is a simple matter of receiving a signal above the noise threshold. The decoding process extracts the intelligence from the detected signal. To start decoding, the decoder must first synchronise with the incoming signal. This usually entails recognising a string of decoded bits as the point to start decoding. Not doing this prevents from knowing when one bit word (byte) begins or ends. An intelligent jammer could send a very short signal to disrupt this process using a blocking bit without disrupting the whole signal. The decoder then would go around a cycle and try to start again. The intelligent jammer knows this cycle and repeats the disruption to stop the receiver decoding the signal even though the receiver can detect it. This decoding should not be confused with cryptographic deciphering/decryption.

erroneous information. In some cases, loss of integrity generates loss of availability. For example, corrupt access cards would not enable individuals to access the transportation system. If car ignition key information is altered, then it is likely that access to the car will be impossible.

A man-made unwanted signal can also be used to inject a false signal, œ« © ¬ ® « © ¥ ¯ ¥ ª £ ˙ ˚ ¤ ¡ ˙ ¯ µ ¯ ˚ ¡ © ˙ ¯ ˙ ¥ ª ˚ ¡ £ ® ¥ ˚ µ ˙ & ¡ š Ÿ ¡ ® ˙ © « Ÿ ¥ ¢ µ ˙ « ® ˙ § ¥ ¨ ˙˙ š ˙ ˚ š £ ˙ ˙ / ould be sent before the tag is ˙ ˙ § ¥ ¨ ˙˙ ˙ read by the legitimate reader and lead to fraud in a retail context, or disrupt supply chain information. Tag cloning and emulation could be used to falsify the identity of goods, and, for example, replace them with cheaper item identifiers. Automobile ˚ ¤ ¥ ¡ ² ¡ ¯ ˙ œ« ± ¨ Ÿ ˙ œ¨ « ª ¡ ˙ œš ® ˙ § ¡ µ ¯ ˙ ˙ ˙̦ « ª ¡ Ÿ ˙ œ® ¡ Ÿ ¡ ª ˚ ¥ be stolen to enable access to restricted areas in the work environment. Cloning could lead to identity theft if the cloned credential can be used as a proof of identity.

Attacks based on deception can take advantage of cloning and emulation techniques. In 2005, researchers demonstrated the feasibility of a cloning attack of ˚ ¤ ¡ ˙ ˙ ˘ ¥ £ ¥ ˚ š ¨ ˙ ˙ ˙ ¥ £ ª š ˚ ± ®¡ ˙ ˙ (® š ª ¯ « ª ExxonMobil œ¤ ¥ ¬ ˙ ˙ ³ ¤ ¥ SpeedPass payment transponders and over 150 million automobile ignition keys. They cloned the chip using relatively cheap equipment, purchased gasoline at an ExxonMobil station multiple times and disarmed a Ford car immobiliser system. A securi˚ µ ˙ œ« ª ¯ ± ¨ ˚ š ª ˚ ¯ ± œœ¡ ¯ ˙ ¢ ± ¨ ˙ µ ˙ œ ª ¡ Ÿ ˙ $ ¤ ¥ ¨ ¥ ¬ ˙ card chip, which is the most commonly used key-access system. The implantable & / Ł ˘ ˙ ˙ * ¡ ® ¥ œ¤ ¥ ¬ ˙ ˙ ˙ š £ ˙ ³ š ¯ ˙ œ¨ « ª year-old Canadian ˙ ¯ ˙ ˚ ¤ š ª hardware developer for the purpose of an article in the magazine *Wired*. The tag, ¥ © ¬ ¨ š ª ˚ ¡ Ÿ ˙ ¥ ª ˙ ˚ ¤ ¡ ˙ ˙¦ « ± ® ª š ¨ ¥ ¯ ˚ ˙ ˙ ˙ š ® © ˙ ¢ « ® ˙ ˚ ¤ ¡ ˙ ¬ ± ® at all.[48]

A read-write tag can be subject to unauthorised modification of tag data or falsification of tag content to deny availability, or change the identity or information details of goods or people. According to the same *Wired* article, 5 millions RFID tags ¤ š ² ¡ ˙ › ¡ ¡ ª ˙ ˙ « ¨ Ÿ ˙ « ˙ ¥ › ® š ® ¥ ¡ ¯ ˙ ¥ ª ˙ š ˚ ± ª ˚ ¥ « œ§ ¡ Ÿ ˙ change the data ˙) ª ¢ « ® ˚ ± ª š ˚ ¡ ¨ µ ˙ ˙ ˚ ¤ ¡ ¯ ¡ ˙ š £ ¯ ˙ š ¨ ¨ « ˙ ¡ ª š software and hardware to write on the tag as well.

‹ Confidentiality

Confidentiality is the assurance that information is accessible only to those who are authorised to have access. When the data relates to an individual, loss of confidentiality results in data protection violations. Consequences of loss of confidentiality in typical RFID systems could include, for example, stealing competitor information in the supply chain or in the retail environment, stealing a vehicle by gaining access to electronic key information and cloning the chip. ˚ œœ« ® Ÿ ¥ ª £ ˙ ˚ « ˙ š ˙ Ł š ¬ š ª ¡ ¯ ¡ ˙ ª ¡ ³ ¯ ¬ š ¬ ¡ ® ˙ ˙ Ÿ š ˚ š ˙ š › « ± stations stored in a Japanese public transport access card (Suica card) can be read by basic RFID readers, such as the one embedded in Sony Clié PDA. A journalist claimed that the possibility to read such information at a distance could potentially facilitate stalking. The vulnerability of passport information (including biometric data) has been pointed out as a possible source of fraud or crimes involving identity

48. See Annex III.

theft (see Annex III). Unauthorised remote access to data is sometimes also called
¯ § ¥ © © ¥ ª £ ˙

Any system based on radio technology is susceptible to eavesdropping of the radio signal between transmitter and receiver, thus raising confidentiality challenges (as well as integrity challenges if the data can be reinjected). RFID systems based on magnetic induction also generate radio waves that an attacker equipped with the appropriate radio equipment could, in theory, intercept. However although theoretically possible, it is practically improbable because the energy levels would be relatively low and would be covered by noise, forcing the attacker to operate at short distance of the tags and reader (likely, in an overt manner).

RFID eavesdropping can be both passive and active. The attacker (or
¥ ª ° ¡ ® œ¡ ¬ ° « ®   ˙ © š µ ˙ š œ° ¥ ² ¡ ¨ µ ˙ ¯ ¡ ª Ÿ ˙ š ˙ ¯ ¥ £ ª š ¨ ˙ ° «
passively listen to the response prompted by a reader activating the tag. Some tags can only reply with data (*e.g.* š ª ˙ ¥ Ÿ ¡ ª ° ¥ ¢ ¥ œš ° ¥ « ª ˙ ª ± © › ¡ ®   ˙ ! « ®¡ ˙
send back a processed response akin to being actively interrogated with the objective of exploiting a vulnerability.

Eavesdropping on the transmission can reveal the existence of a communication between RFID devices potentially leading to the disclosure of valuable information for the attacker (*e.g.* the number of goods arriving in a warehouse or the presence of an individual in a given area). It enables tracking of the tag and the attached object. It can also reveal the content of the communications thus enabling unauthorised access to potentially valuable business, competitive or personal information and also enabling other attacks such as uª ³ š ª ° ¡ Ÿ ˙ © « Ÿ ¥ ¢ ¥ œš ° ¥ « ª ˙ « ¢ ˙ ° ¤ ¡ ˙ Ÿ š
© ¥ Ÿ Ÿ ¨ ¡ ˙ š ° ° š œ§ ˙ ˙ ³ ¤ ¡ ®¡ ˙ ° ¤ ¡ ˙ ¥ ª ° ¡ ® œ¡ ¬ ° « ®˙ © « Ÿ ¥ ¢ ¥
and the reader). Other elements regarding privacy risks related to loss of confidentiality are provided in the privacy section below.

‹ Considerations regarding the type of technology used

Risks vary according to the type of technology used to perform a specific function. As highlighted earlier, RFID is an umbrella concept for a variety of technologies with different characteristics. The risks mentioned above are theoretically applicable to all RFID systems. However, on a continuum of risks, the likeliness of certain risks is higher in some technical configurations than in others. Parameters such as the use of passive or active tags, of electromagnetic induction or radio-wave communications, of read only or read-write capable memory influence the degree of likeliness that certain risks materialise. The table below highlights some of these elements in a very general manner, but it is important to note that only a detailed consideration taking into account all the characteristics of a given system can provide relevant conclusions relative to the potential risks to the different systems. At a general level, the table shows that technology choices that do not take into account security considerations have an impact on the level of security risk.

Table 7. Risk comparison on a risk continuum

Risk	Risk continuum	Explanations
	Lesser risks ←————————→ Greater risks	
Eavesdropping	Induction ←————————→ Radio waves	The attacker needs to be in the operating range[49]
Jamming	Induction ←————————→ Radio waves	Idem
Covert tracking	Induction ←————————→ Radio waves	Idem
Radio noise interference	Induction ←————————→ Radio waves	Electromagnetic induction is not subject to radio interferences
Tag cloning	Authentication on tags ←————————→ Data only on tags	Authentication prevents unauthorised access
Tag data integrity attack	Read only memory ←————————→ Read-write memory	Read only memory cannot be modified (but, the chip could be destroyed)
Denial of service attack by tag blocking	Active tags ←————————→ Passive tags	Active tags can include smarter communication protocols to defeat attacks

Operating ranges discussed in the first section can be considered in relation to the type of attack that is anticipated, as highlighted in box 1 below.

<table>
<tr><td colspan="1">

Box 1. Operation ranges from a security perspective

˚ œœ« ®Ÿ¥ª£˙˚«˙"Ł'(˙ fi±¥Ÿ¡¨¥ª¡¯˙¢«®˙'¡œ±®¥ª£˙&šŸ¥«˙∕®¡−±¡ operation ranges can be distinguished:

‹ **Nominal operating range**: the distance, often specified by standard, over which authorised ˚®šª¯šœ°¥«ª¯˙š®¡¡´¬¡œ¡Ÿ˙°«˙«œœ±®˙'(¤¥¯˙¥¯˙°¤¡˙«¢¢¥α

‹ **Back channel eavesdropping range**: the distance over which a rogue receiver can reliably interpret š˙˙°š£˙¯˙®¡¯¬«ªª¡˙°«˙š˙š®¡˙¡£¥°¥©š°¡˙®¡šŸ¡®

‹ **Forward channel eavesdropping range**: the distance over which a rogue receiver can reliably listen to the transmissions of an authorised reader. Both back channel and forward channel eavesdropping can be considerably greater than the official operating ranges. Cover-coding technique, which has been included in EPCglobal class-1 Generation 2 specification, prevents a rogue receiver from deciphering exchanged data if it is not capable of eavesdropping also on the tag responses (the communication is encrypted using a key sent by the tag to the reader). This forces the eavesdropper to operate within the back channel eavesdropping range in order to decipher the communication.

‹ **Rogue skimming or scanning range:** the distance over which a rogue reader operating above the regulated power limits can reliably communicate with a tag.

‹ **Rogue command range**: the distance over which a rogue interrogator can execute a tag command that does not require the reader to successfully receive information from the tag.

‹ **Forward channel traffic analysis range**: the distance over which a rogue receiver can detect the ¬®¡¯¡¡ªœ¡˙«¢˙š˙®¡šŸ¡®˙¯˙˙¥£ªšš˙¯³¥°¤«±°˙ld enable the˙°«˙¥¥¥¥ª˙ arrival of a shipment and possibly count the number of items. Such an attack can be performed over much longer distances than eavesdropping.

</td></tr>
</table>

Source: Adapted from NIST, 2007, p. 2-13.

---

49. As noted in the first section of this paper, the law for radio waves signal propagation is different than for electromagnetic fields. Thus the operating range of radio waves tags (at UHF and microwave frequencies) can be much longer (meters) than that of electro-magnetic induction systems (centimetres).

2.1.1.2. Risks related to other components

Other components of RFID systems present security risks too. In particular, database security has been identified as a serious and sometimes underestimated concern, since databases containing information associated to tags are likely to be accessed by different enterprises and, sometimes, will be maintained by third parties.[50]

Likewise, RFID systems relying on the transmission of information over the Internet are exposed to the same variety of attacks as other information systems. For example, some academic researchers[51] have pointed out potential confidentiality / privacy, availability and integrity concerns relative to the Object Naming Service (ONS) designed by EPCglobal as a component of the EPCglobal network architecture, mentioned earlier. EPCglobal considers that although security risks need to be addressed, they are limited and not greater than the ones that exist today on communications over the Internet or other information systems.

Academic research has also demonstrated that classic Structured Query Language (SQL) and script injection attacks are capable of significantly damaging an RFID system through the use of just one infected RFID tag.[52] &⁄Ł˘˙°š£¯˙˙Ÿš°š˙œ« include unexpected code or instructions designed, for example, to damage the back-end database of an RFID system, compromise the whole system and/or self-replicate inside the system. In such scenarios, the exploits are not inherently linked to the RFID technology but rather to the quality of the design and coding of the middleware software components, which interact with the RFID devices. Researchers highlighted that RFID applications are potential candidates for exploitation by malware: they involve complex applications with a large amount of source code, rely on generic protocols and facilities as well as back-end databases, they process and store high-value data and, since nobody expects RFID malware yet, they convey a false sense of security.[53]

2.1.1.3. ɪ´¬ȷœ°˙°¤ȷ˙±ªȷ´¬ȷœ°ȷŸ

Tag technology is still relatively young. Therefore, innovative and unpredicted œ®šœ§¥ª£˙°ȷœ¤ª¥−±ȷ¯˙œ«±¨Ÿ˙ȷ©ȷ®£ȷ˙˙°˙¯°š°ȷŸ °¬¬˙¥œš°¥«ª¯˙˙ȷœ±®¥°µ˙šªŸ˙$®¥²šœµ˙˙˙3ȷ˙¤«±«ªȷ˙°¤¥ª£˙°¤š°˙¯˙œ¨ȷš®˙š›«±°˙°¤¥¯˙ª¥33«®˙Ÿ changes š¤ȷšŸ˙šªŸ˙¯±®54 For example, in February 2006, professor and well-§ª«3ª˙œ®µ¬°«£®š¬¤ȷ®˙˙Ÿ¥˙˙¤š©¥®˙˙±˙ȷŸ˙š˙Ÿ oscilloscope to monitor power use by RFID tags while they were being read. Patterns in power use could be analysed to determine when the tag was receiving œ«®®ȷœ°˙šªŸ˙¥ªœ«®®ȷœ°˙¬š¯¯3«®Ÿ¯˙›¥°¯˙˙˙¤š©¥®˙

---

50. US FTC, 2005, p. 16.

51. Fabian, 2005.

52. Rieback *et al.*, n.d.

53. #ª˙!š¨3š®ȷ˙¯ȷȷ˙°ªš¨µ°¥œš¨&ȷ¬«®°«ª˙!š¨¥œ¥«±¯˙˙˙

54. Garfinkel, 2006, p. xliv.

ingredients you need to conduct an attack and compromise all RFID tags in the ² ¥ œ¥⁵⁵ ¥ ° µ

The demonstration of the feasibility of such an attack scenario in laboratory conditions needs to be balanced against the cost of deploying the scenario in real life conditions and the benefits or limitations of such an attack. However, this example stresses that it would be good practice to consider technology evolution when defining a security strategy, to assess risk at the system design stage, and to periodically reassess it as in any security life cycle process.

2.1.2. Security controls[56]

Security is implemented through a combination of management, operational, and technical controls to mitigate risk. RFID systems vary considerably according to the technology used, the application contexts and scenarios. Effective security strategies rely on a mix of security controls that balance cost, performance and convenience for a given system within a given regulatory environment. Risk assessment is a key requirement to determine the threat and vulnerability level at a given time along with the appropriate combination of controls to mitigate them. In this respect, RFID is no different from any other information system.

Management controls include the policies, procedures and standards in relation to the oversight of the system. They detail how a business is run and how day-to-day operations are conducted. Management controls include IT security policies covering access control to RFID information, perimeter protection, password management, etc.; RFID usage policy that describes the authorised and unauthorised uses of RFID technologies; agreements with external organisations when data associated with RFID systems are shared across multiple organisations; and strategies to minimise the information stored on chips (*e.g.* in the case of personal information).

Operational controls correspond to actions performed by users of the system. They include physical access control (*e.g.* surveillance cameras, gates, walls, etc.); the appropriate placement of tags and readers (*e.g.* to minimise interference); training of personnel; use of identifier formats that do not reveal any information; etc.

Technical controls correspond to technology measures to monitor and restrict access to the information and the system. They include:

‹ ˛ « ª ° ® « ¨ ¯ ¯ ° « ˙ ¬ ® « ° ¡ œ° ˙ ° ¤ ¡ ˙ ° š £ ˙ Ÿ š ° š ˙ š ˙ ¢ ¡ š ˙
     functionalit¥ ¡ ¯ ˙ ³ ¤ ¡ ª ˙ ¥ ° ˙ ® ¡ œ¡ ¥ ² ¡ ¯ ˙ š ¯ ¬ ¡ œ⁵⁷¥ ¢ ¥ œ˙ § ¥ ¨

---

55.   # ® ¡ ª ˙ ª ˙ Ÿ ˙ ! ¡ ® ® ¥ ° ˙ ˙ ˙ ¡ side-o®˙¥šᵃµª ¡¡ ¨´¬š °®°° š œ§¤˙š ² ¡š ® not a new type of data attack and that RFID could benefit from mitigation techniques that have been used to protect contact-based smart cards, *e.g.* by masking the spikes in power œ« ª ¯ ± © ¬ ° ¥ « ª ˙ ˙ ¡ ¡ ˙ # ˛ « ª ª « ® ˙

56.   This paper does not aim to provide a detailed inventory of existing risk controls. Such more detailed inventories can be found in NIST, 2007 and BSI, 2005.

57.   Where cryptography is used a number of key management techniques such as key diversification can be used to limit the damages of a successful attack.

access control mechanisms, such as password protection to protect from anyone using the kill command in EPC Class-1 Generation 2 tags; authentication mechanisms where the tag authenticates the reader and/or the reader authenticates the tag; tamper resistance mechanisms to prevent the tag from being removed from the object to which it is attached.

‹ Controls to protect the radio-frequency interface: the use of a frequency which avoids specific interference (*e.g.* liquids); adjusting the power level to mitigate the propagation of radio-waves and risks of eavesdropping; shielding of the tag when it is not supposed to operate, to protect against unauthorised access, or shielding of the environment to protect against eavesdropping; and temporary deactivation of active tags[58].

Many technical security controls are available in various degrees of sophistication and robustness. However, complexity often increases with sophistication. For example, strong cryptography often involves key management processes and techniques that are not easily compatible with lightweight turnkey solutions. Chips embedding more processing power required by security features are also likely to require more energy, thus adding new constraints such as shorter reading range, larger form factor, need for batteries, shorter life span, etc. In the longer run, it is possible that some of these constraints can be minimised. Cost of RFID devices is also likely to be proportional to their level of sophistication, including to the robustness of their security feature. Eventually, market forces will play a role in the reduction of such cost.

Important research efforts are currently underway to develop innovative technical security measures[59] in areas such as authentication, cryptography, blocking, and policy embedded devices (trusted computing)[60]. Data-minimisation techniques are also being explored: the unique identifier data (*e.g.* the EPC number, cf. Annex IV) could be erased, either automatically or via active participation by the individual, which means that only data that corresponds to the product class would identify a specific object anymore but only a product class. Another technique consists in adding distance measurement capability to the chip and to vary the granularity of the information transmitted according to the computed distance of the reader. In this case, while a tag attached to a bottle of water might reply to a

---

58. Another technical control is cover coding, which takes advantage of the fact that a passive tag reflects the signal transmitted by the reader, a technique by which the reader encrypts the communication. A potential eavesdropper located beyond the reader would capture the encrypted data but would not be able to capture the cryptographic key. This technique is included in the EPC Class 1 Generation 2 standard.

59. For example, research is being carried out to improve the 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.

60. For a detailed overview, see Juels (2005a). See also Gildas Avoine's web page which lists research articles related to RFID security and privacy, as well as security and privacy requirements for open loop systems.

reader located far away, it might provide the brand only if the reader is closer and its actual identification number only if it is very close. None of these research efforts constitute a silver bullet, but they are useful and confirm the very large potential for
¯ ¡ œ ± ® ¥ ° µ ˙ ° « ˙ › ¡ ˙ › Š § ¡ Ÿ ˙ ¥ ª ° « ˙ ° ¤ ¡ ˙ ° ¡ œ ¤ ª « ¨ « £ µ ˙ ¥ ª

There is no one-size-fits-all security measure that would efficiently address a given class of risks in all possible situations. The appropriateness of each security control depends on various factors: not all controls are available for all types of RFID. For example, data encryption helps protect sensitive tag data but, as noted in NIST Guidelines,[61] it is not available on EPC and ISO 18000 standards systems. Similarly, all controls have benefits and weaknesses: password protection enables restricting access to tag information but password length is often very short;[62] data encryption on tags requires power for computing cryptographic functions, and it may introduce an unacceptable delay in systems that require fast reading/writing operations between reader and tag.

It has been noted that open standards for classifying and rating the security features of RFID cards and tags are virtually nonexistent. As a consequence, assessing the security of RFID systems may be a difficult task for RFID operators and even manufacturers.

Technical measures cannot mitigate all risks to a system. Operational and management controls are also essential. For example, security tools, such as encryption, are only useful if part of a wider framework of controls supporting a comprehensive security policy.

Table 8 below provides a summary of security controls for RFID security developed by the US National Institute for Standards and Technology.

---

61.   NIST, 2007, p. 5-17.

62.   *e.g.* EPC Class-1 Generation 1 tags provide 8-bit passwords, *i.e.* only 256 possible passwords; Class-1 Generation 2 tags provide 32 bits passwords, *i.e.* 4 294 967 296 possible passwords.

Table 8. RFID Controls Summary

Controls	Business process risks	Business Intelligence Risks	Privacy risks	Computer Network attacks
Management controls				
RFID Usage Policy	›	›	›	›
IT Security Policies	›	›		
Agreements with External Organizations:	›	›	›	
Minimizing Data Stored on Tags	›	›	›	
Operational controls				
Physical Access Control	›	›		›
Appropriate Placement of Tags and Interrogators	›	›		›
Secure Disposal of Tags	›	›	›	
Operator and Administrator Training	›	›		›
Separation of Duties	›	›		
Non-revealing Identifier Formats		›	›	
Technical controls				
Tag Access Controls	›	›	›	
Kill Feature			›	
Data Encryption	›	›	›	
Fallback Identification Technology	›			
Authentication	›	›	›	
Tamper Resistance	›	›		
Radio Frequency Selection	›			›
Transmission Power Adjustment		›		›
Electromagnetic Shielding		›	›	›
Cover-Coding				
Temporary Deactivation of Active Tags		›	›	

" « ° ¡ ˙ ¥ ª ˙ ° ¤ ¡ ˙ " Ł ' (˙ fi ± ¥ Ÿ ¡ ¨ ¥ ª ¡ ¯   ˙ œ« © ¬ ± ° ¡ ® ˙ §° ¡ ° ˙³ œŠ®°§¡˙ ßŠ«° ®˙µŠ˙œ§ ¯ ˙
that also includes hazards of electromagnetic radiation.

Source: NIST, 2007.

2.1.3 A holistic approach

Security controls can be applied at any and all stages of the deployment of an RFID system. In particular, many technical controls are likely to be most effective if introduced at the earliest stage of development of the system. The controls in place before tag deployment can broadly be considered as pro-active and preventative whilst the controls in the environment and in the system beyond (including the readers) can be broadly described as reactive and limiting risk. To control the inherent openness of the RFID component of the system, it is necessary to take a holistic view of the system with regards to time and space when assessing and

managing risks: *i*) at all stages of the system, including planning, deployment, operation, data processing and disposition (end of life),[63] *ii*) considering the RFID system in its broader sense, including both RFID specific and unspecific components, avoiding a focus only on the tag-reader relationship, and considering the system as part of a broader infrastructure of information systems and networks. A narrow approach focusing only on the tag/reader operational relationship would not capture all the controls that could be placed before and after that point to both prevent and limit damages. A narrow approach would also fail to detect potential risks related to the network, middleware, and back-end components that are key to the efficiency of an RFID system. It could also lead to an underestimation of the cost and overestimation of the effectiveness of the security controls that could be applied.

Technologies used and participants in RFID systems are complex and dispersed. Consequently, it is impossible to conform to a closed and rigidly controlled security model. The many interconnections and interdependencies combined with the complexities between the different components of technology, organisations and business processes make a physical and logical security perimeter for any RFID system a difficult task. Further, many security variables are beyond the control of some of the individual participants. Thus, one could argue that achieving security requires adopting a holistic approach that would consider all of the individual components within an overall security picture, accepting that there may be weaknesses in some of the individual components but that these weaknesses would be compensated for elsewhere in the design.

In some cases, controls, by way of policy and regulation, are already in place, and the introduction of RFID technology will have no impact on existing security models. In other cases, the introduction of RFID technology may necessitate new risk assessments that could lead to a conclusion that existing controls, including security policy and regulation, need to be strengthened.

2.1.4   *Adjusting security level to what is at stake*

Information security management requires controls to be balanced in terms of risk, cost and effectiveness. The cost/benefit ratio of security controls cannot be expressed in an absolute manner. Rather, it depends on the application context and, in particular, the value of the assets or business process that need to be protected. An RFID tag can be likened to a token carrying information. Its security value depends on the asset it is attached to (*e.g.* a car key) and the purpose for which it is being used (*e.g.* verifying identity, providing access to restricted areas, paying goods, etc.). If RFID tags are used as an electronic wallet or tickets in a subway card or to open doors, criminals may be interested in stealing, copying or modifying them. When RFID is used for access control to other systems and networks, a successful attack could compromise not just the RFID system itself but also all systems and networks it was supposed to secure.

---

63.   ˚ ¨ ˚ ¤ « ± £ ¤ ˙ ˚ ¤ ¡ ˙   ¡ ª Ÿ ˙ « ¢ ˙ ¨ ¥ ¢ ¡   ˙ « ® ˙ Ÿ ¥ ¯ ¬ « ¯ ¥ ˚ ¥ « ª ˙ ¯ ˚ Š £ ¡ ˙
destruction of information, for example, when it is no longer required, it may also involve activities such as the archiving of information or the transfer of information to a successor system.

Risk increases when the benefits of an attack outweigh its costs. Before committing crimes, even criminals perform risk assessments of existing systems to identify whether and how they could exploit weaknesses. They also perform a cost/benefit analysis to determine which attack strategy is the best for reaching a given objective. Criminals will for example decide whether cloning an RFID hotel door tag is easier than bribing the domestic staff or breaking in via a window. Appropriate security controls can boost the cost of a possible attack so the cost outweighs the benefits. Insufficient security controls with regards to the value of the asset to protect will likely trigger the interest of a potential attacker. A set of efficient security controls will likely not suppress the intention of an attacker to commit a crime, but it may force him or her to use another technique or to target other less-protected systems or victims, or to take more risk.

When the information stored in a tag can be related to an identified or identifiable individual, the protection of the information should be regarded from the double perspective of security and privacy. In some cases, the stored data can be sensitive: information identifying a medicine taken or carried by an individual can reveal personal health data; medical data recorded in a patient RFID wrist band can lead to life threatening situations if lost or corrupted; unauthorised access to biometric data in a passport or identity document can lead to identity theft. Some sensitive personal data, such as biometrics, require more sophisticated protections than others, such as the use of effective encryption and electronic authentication mechanisms. Even though security risk assessment can be considered similar to privacy impact assessment in terms of methodology, its scope is different: an organisation performs a risk assessment to protect its assets and business processes. When it carries out a privacy impact assessment, it needs to take into account any possible loss of privacy for the individuals concerned by the data processing, including when such loss would not directly impact the organisation. The use of RFID for human identity verification provides a good example of a case where extensive security and privacy assessment is required before the decision is made to adopt RFID technology (US Department of Homeland Security, 2006).

It is possible that, in a given scenario, a risk assessment concludes that the level of risk and the cost of the necessary security controls to cope with the risks versus the benefit of using RFID technology is not worth deploying the system or requires a partial or complete re-evaluation of the project. In a given context, one particular affordable RFID technology may appear to be insufficiently protected against a certain class of risks but sufficiently against another. A decision could be made to invest in a more secure type of RFID technology, or to associate the initial low-cost RFID technology with non-RFID security controls (*e.g.* video surveillance, human monitoring, etc.), or to use other technologies than RFID.

2.2. Privacy

Privacy ranks as concern number one in consumer surveys[64] regarding RFID as well as in comments received by consumer protection agencies such as the US Federal Trade Commission.[65] Several well-known public campaigns featuring anti-‾ ¬ µ œ⁶⁶¤£¥®‑« ‾ ± ¬ ¯ ˙ ¤ š ¨ ° ¡ Ÿ ˙ œ« © ¬ š ª ¥ ¡ ¯ ˙ & ⁄ Ł ˘ ˙ ° ® ¥ š ¨ ¯ ˙ š ª Ÿ the need to address public perception of privacy to enable widespread adoption of the technology. As one observer notes,[67] RFID was born in a technical environment, is designed, used and understood mainly by technical people. Originally designed for the supply chain, it is now extended to consumers and individuals but can be invisible, remains opaque and often unexplained. Perception issues cannot simply be dismissed as irrational fears. These concerns should be addressed by all stakeholders in a responsible manner in order not to jeopardise potential benefits for both the industry and the individuals.

In fact, surveys also highlight that consumer awareness regarding RFID is still relatively low. While some consider that privacy issues threaten to overshadow the benefits of RFID,[68] others question whether perceived benefits of the technology in some areas outweigh possible risks, in particular as some of these risks would not be immediately visible. More generally, the US National Research Council (2004, p. ˙ ®¡ œ« £ ª ¥ ¯ ¡ Ÿ ˙ ° ¤ š ° £ ¥ ¯Actual preferences regarding ˙ Ÿ ¥ ¢ ¢ ¡ ®¡ ª privacy, along with a range of social norms, the establishment of public trust with respect to RFID technology will be a complicated, long-° ¡ ® © ˙ ± ª Ÿ ¡ ® ° š § ¥ ª £ ˙

Several authors and public and private sector organisations have already performed privacy analyses of RFID and have issued reports and even guidance or principles to help stakeholders apply existing privacy frameworks. A list of references can be found in Annex V. This material forms a very useful basis on which the following elements are partly based. The following sections discuss privacy challenges RFID may raise as well as possible safeguards. The OECD *Privacy Guidelines* have been used to guide the discussion of privacy challenges.

2.2.1 Overview of privacy challenges

There is a broad variety of RFID hardware and software configurations deployed in many different contexts. RFID technology does not systematically or inherently

---

64. According to Cap Gemini (2005a), Privacy-related issues are the most significant concern about RFID among European consumers. US consumers expressed greater concern than Europeans about privacy-related issues, possibly as a result of the higher visibility of œ« ª ¯ ± © ¡ ® ˙ š Ÿ ² « œš œµ ˙ £ ®« ± ¬ ¯ ˙ š œ° ¥ ² ¥ ° ¥ ¡ ¯ ˙ ®¡ £ š ®Ÿ ¥ ª £ ˙ & ⁄

65. FTC, 2005, p.12.

66. ˙ ¡ ¡ ˙ ˙ ¬ µ œ¤ ¥ ¬ ¯ ˙ › µ ˙ Ž š ° ¤ ¡ ® ¥ ª ¡ ˙ ˙ ° ¨ › ®¡ œ¤ ° ˙ š ª Ÿ ˙ ž ¥ ¶ ˙ ! www.spychips.com

67. Pradelles (customer privacy manager, HP), 2006.

68. Cap Gemini, 2005b.

---

generate privacy issues and, when it does, the nature, scope and extent of these issues vary according to both the technology and the use context.[69]

In most cases, the potential invasion of privacy through the use of RFID is likely to be proportionate to several interrelated parameters including: *i)* š ˙ ° š £ ‾ ˙ œš ¬ š œ¥ ° µ to be read at a distance without the participation of the individual; *ii)* the possibility to reveal intrusive or sensitive information about individuals through inferences and profiling; *iii)* the degree of interoperability (who can read the tags, who can access the full information about the product); and *iv)* the tracking capabilities of RFID.

2.2.1.1 Invisibility of the data collection

An important characteristic of RFID is that the collection of data can happen without the knowledge of the individual: electromagnetic communication happens ¥ ª 2 ¥ ‾ ¥ › ¨ µ ˙ ¥ ° ˙ Ÿ « ¡ ‾ ˙ ª « ° ˙ ° « ± œ¤ ˙ ° ¤ ¡ ˙ ‾ ¡ ª ‾ ¡ ‾ ˙ ¥ clothes, the size of RFID tags and readers can be very small, and there may be no sign that they are in operation. This leads to both security concerns (*e.g.* jamming, eavesdropping, and replay attacks can be performed remotely) and privacy concerns.[70] Invisibility generates uncertainty and may lead individuals to think that ‾ « © ¡ ° ¤ ¥ ª £ ˙ ©¥ £ ¤ ° ˙ › ¡ ˙ ¤ š ¬ ¬ ¡ ª ¥ ª £ ˙ › ¡ ¤ ¥ ª Ÿ ˙ ° ¤ ¡ ¥ ® ˙ › š to a broad acceptance of the technology. However, what may lead to fear perceptions in some contexts may also foster usability in others: the possibility to automatically establish a communication between the reader and the tags, through obstacles, without direct line of sight is also the main advantage of RFID in supply chains, access control and other contexts. It can also bring convenience and choice to consumers when they shop.

2.2.1.2 Profiling

Access to tag information in objects owned or carried by individuals can reveal private elements of their life, such as interest in specific topics (tagged books), or holding of cash (in the case of RFID in banknotes) or other valuable objects. For ¡ ´ š © ¬ ¨ ¡ ˙ ± ª ¨ ¥ § ¡ ˙ š ˙ ¢ ± ¨ µ ˙ ®š ª Ÿ « © ˙ ± ª serial ¡ ˙ ª ± © › ¡ ® number, EPC data structure contains elements that identify the manufacturer of the ¬ ® « Ÿ ± œ° ˙ ˙ � I $ ¸ ˙ ©š ª š £ ¡ ® ˙ ª ± © › ¡ ® ˙ š ‾ ˙ 3 ¡ ¨ ¨ ˙ š ‾ ˙ ° similar to the barcode system. If accessed by a third party, the information in the tag could reveal details about the object itself and thus sensitive information, *e.g.* (¤ ¥ ‾ ˙ person carries Prozac, is likely to be depressive or in contact with a depressive ¬ š ° ¥[71] etc. However, prior to performing such an inference, the third party would need to read the content of the tag and convert the product code into the actual product name. It might already know the relationship between the code and

---

69. According to Ontario Information and Privacy Commissioner Ann Cavoukian (2006a), ¬ ® ¥ ª œ¥ ¬ ¨ ¡ ‾ ˙ ¢ « ® ˙ &/ Ł ˘ ˙ ‾ ¤ « ± ¨ Ÿ ˙ ¢ « œ± ‾ ˙ « ª ˙ &/ Ł ˘ ˙ Ł ª ¢ « ® ©š

70. Covert collection and transmission of personal data is not a new topic in the privacy realm. For example, it has been raised regarding the use of biometric technologies. See OECD, 2005.

71. Stapleton-Gray, n.d.

the product from a previous search. Or it might send the EPC manager number to an Object Naming Service (ONS) in order to retrieve the network address of the manufacturer of the product. Then, to retrieve the actual name of the product, it would have to send a query to this address with the product code.[72] Finally, it would need to perform the inference mentioned above. It is worth noting at this stage that such a scenario remains speculative as item-level tagging is still limited.

Revealing the type of soap or toothpaste bought in a supermarket may not be considered as a real privacy issue. But, in some cases, profiles and inferences that could be made from a cluster of RFID tags carried by an individual could become very precise and reveal much more intrusive information, including identifying ¤ ¥ © ¤ ¡ ® ΄ ' ¡ ª ¯ ¥ ° ¥ ² ¡ ΄ ¥ ª ¢ « ® © š ° ¥ ¥ ª or biometric ΄ š ¯ ΄ ¥ ª Ÿ ¥ information could also be revealed by unprotected biometric passports.

Making inferences from available data to enhance existing profiles is not new. Credit companies, banks and insurance companies have long been using profiling techniques to associate a level of risk to customers. Popular websites such as Amazon suggest books and DVDs to returning customers based on their buying and browsing habits. Often, this leads to increased convenience and options for consumers, and enables companies to provide better, and sometimes more tailored ¯ ¡ ® ² ¥ œ¡ ¯ ΄ š ° ΄ š ΄ œ± ¯ ° « © ¡ ® ΄ ΄ ®¡ − ± ¡ ¯ ° ΄ & ⁄ Ł ˇ ΄ Ÿ « ¡ ¯ technologies but: *i)* the invisibility of the technology would enable such profiling to happen covertly[73] and *ii)* if widespread, it could make profiling technologies more accurate and efficient by providing more data to be processed.

2.2.1.4 *Tracking*

Tracking of objects, goods, cases, pallets and animals is a key functionality of RFID. Tracking of people is possible if they carry or wear objects that include RFID tags. For example, RFID is used in amusement parks to enable parents to find their children. It is used in ski resorts to help friends find each other, in hospitals to keep track of patients, and in prisons to track inmates throughout the facility.

Tracking is enabled by the collection or processing of location and time data and can be performed either after the fact with data already stored in a database, or in real time.

After the fact tracking can result from bringing together location, time and other ¥ ª ¢ « ® © š ° ¥ « ª ΄ ¬ ®¡ ² ¥ « ± ¯ ΄ μ ΄ ¯ ° « ®¡ Ÿ ΄ ¥ ª « ª ¡ ΄ « ® ΄ ¡ ² ¡ ¢ « « ° ¬ ® ¥ ª ° ΄ / « ® ΄ ¡ ΄ š © ¬ ¨ ¡ ΄ & ⁄ Ł ˇ ΄ ° ¥ œ§ ¡ ° ΄ ΄ ¢ « ® ΄ time and place corresponding to when the buyer entered the stadium or the theatre. Badges used for access control in a work environment help restrict access to certain premises to authorised people and often keep track of employee presence and work hours. Subway RFID cards like the Parisian Navigo Pass, the London Oyster Card or

---

72. Ł ° ΄ ¥ ¯ ΄ ¨ ¥ § ¡ ¨ μ ΄ ° ¤ š ° ΄ ° ¤ ¡ ΄ © š ª ± ¢ š œ° ± ®¡ ® ΄ ® ΄ ΄ μ ¯ ° ¡ © ΄ ³ « ± ¨ Ÿ
deployed in a B2B context.

73. One often cited hypothetical example of covert basic inference is related to criminals accessing information about objects carried by a person in order to select that person as a target for a crime (*e.g.* a person wears a designer suit and is therefore likely to have other valuable objects on or with him/her).

the Tokyo Suica Card allow only individuals who have paid the fee to enter in the transportation system and take the journey they have paid for. All these RFID systems need to process location information in order to perform their access control feature but if such information is stored and can be linked to the individual, it could then be used for broader tracking purposes.

According to privacy protection frameworks, personal data should not be disclosed, made available or otherwise used for purposes other than those originally specified except with the consent of the data subject or by the authority of law. Digital footprints are not a new concept in the online environment and have long been used for criminal investigation purposes. One objective of privacy protection is to prevent the generalisation of their use. Privacy impact assessments can help detect system functionalities that would enable breaching Privacy principles such as alternatives can prevent function creep, like privacy-enhancing technologies, data minimisation and anonymisation strategies.

Real time tracking typically involves monitoring the movements of an identified person, but RFID might also be used to track an unidentified person, *i.e.* distinguishing an individual in a group and monitoring his/her behaviour without that individuals be provided with functional (neither deactivated nor blocked) tags that can be read later on, and that the trackers deploy readers at appropriate locations, taking into account the operation ranges of the RFID technology used and other technical constraints. Whether the tags would later be readable by the original party that provided them to the individual, by a larger number of parties, or by anyone with the appropriate equipment, would depend on the nature of the security possibility for such real time tracking to happen in a covert manner, or for criminal purposes have been expressed by opponents to RFID chips but few cases have actually been reported yet.

The challenges raised by the operation of an open infrastructure that could be used for tracking objects as well as individuals are not in the scope of this paper, as such an infrastructure is not envisioned in the short term. Similarly, the hypothetical generalisation of ubiquitous sensor equipped environments where all objects would embed tags that can be read by anyone and interact with the environment (smart office, smart home, smart streets, etc.) might also raise real time and after the fact tracking concerns. However, being a speculative long-term scenario, it falls outside of the scope of this paper. Both topics could be monitored in relation to the broader issue of infrastructures of surveillance.

2.2.1.3 Interoperability

The context in which the collection of RFID data and its association to individuals may occur is important. In a closed loop context, where tag data is essentially read and modified by the organisation which originally deployed it, it is not clear whether the use of RFID would lead to substantially different outcomes than those occurring with the use of non-RFID systems, such as contact cards or barcodes. Barcodes already enable the collection of information on what individuals buy and its association with names or other personal data (with *e.g.* credit cards, cheques or

loyalty cards). This information enriches profiles and is widely used for optimising marketing campaigns. Existing privacy protection frameworks can be applied and RFID, though adding a level of convenience at the data collection stage, would not add more information to the organisat¥ « ª ¯ ˙ Ÿ š ° š › š ¯ ¡ ˙ fl « ³ ¡ ² ¡ ® ˙ ¯ « © consider that RFID would enable more information to become available, such as real-time location data or product history.

The situation is likely to be different in an open loop context, where RFID data potentially related to identified or identifiable individuals could be accessed or read by many actors due to interoperability, and mass aggregation of such personal data would become possible. Although currently most RFID applications are not taking advantage of interoperability and standardisation, those features may be attractive for those seeking large-scale RFID applications. Some stakeholders consider that interoperability might enable broader dissemination of personal data (a collection, purpose and use limitation issue). For example, if interoperability of tags carried by individuals would result in tags being readable by anyone with the appropriate equipment, it might encourage some actors to collect personal data that they would not otherwise collect. Progressively, personal data collection could become the default instead of being an exception.

Interoperability might also facilitate the adoption of data protection requirements. For example, the proposal made by academic researchers to incorporate explicit privacy policies based on the OECD principles into the standard of the reader-to-tag ISO protocol (Floerkemeir, 2004) shows both that privacy-friendly RFID devices can be envisioned and suggests that standardisation bodies and process could facilitate their generalisation. In another example, at the policy level, the European Commission (2007a) called upon the European standardisation bodies to ensure that international and European standards meet European requirements in particular as regards privacy and security, to identify gaps and to provide the appropriate framework for the development of future RFID standards.

While interoperability may bring benefits to business and remove a technical obstacle to the dissemination of personal information, there are many cases where › ± ¯ ¥ ª ¡ ¯ ¯ ˙ © š µ ˙ œ« ª ¯ ¥ Ÿ ¡ ® ˙ ˙ ° ¤ š ° & ⁄ Ł ˙ -Wal-Mart does ¥ ¯ ˙ ° « « ˙ ¯ not want its competitors to read tags that are from Wal-Mart stores. Wal-Mart probably does not want its suppliers to read information about its other suppliers. (¤ ¡ µ ˙ ³ š ª ° ˙ ° « ˙ œ« ª ° ® « ¨ ˙ ˙ ° ¤ š ° ˙ ¥ [74] ¢ « ® © š ° ¥ « ª ˙ ¢ « ® ˙ œ« ©

Finally, another issue often mentioned with regards to RFID and large-scale implementation is the creation of an additional pillar supporting the emerging infrastructure of surveillance, *i.e.* a global and fully interoperable RFID infrastructure that might enable tags provided to individuals to be read by anyone operating the appropriate connected equipment. While this is not likely to happen in the short term and therefore is not in the scope of this paper, it is important to keep in mind that any exploration of the concept of infrastructure of surveillance should attempt to grasp the measure of convergence of several potentially surveillance-enabling technologies and processes, including RFID and sensor-based networks, biometrics, digital identity management, etc.

---

74.   US FTC, 2005, p.15.

2.2.2   Possible safeguards

The 1980 *OECD Privacy Guidelines* represent international consensus on general guidance concerning the collection and management of personal data. However, their implementation in the context of RFID may raise a number of questions. Furthermore, a number of concepts and policy tools may facilitate their implementation.

2.2.2.1   Privacy principles

+ ¤ ¡ ª ˙ ¥ ¯ ˙ & ∕ Ł ˘ ˙ ¥ *OECD Privacy Guidelines* ˙ « ₵©˙š ̌ µ ¤ ¡› ¡ ˙ ° ¤ ¡ ˙ ₵ ¥ ® basic question raised when considering using the *OECD Privacy Guidelines* for protecting privacy in the context of RFID. The next two sections attempt to address this question by analysing when RFID data may be considered personal data and when an RFID operator is a data controller. The following section discusses questions raised by the invisibility of RFID and in particular issues related to knowledge and consent. Naturally, and consistent with the Security Safeguards Principle of the *Privacy Guidelines*, the security safeguards discussed in the security section of this report are essential for the protection of privacy in RFID systems.

2.2.2.1.1 When is RFID in the scope of the *Privacy Guidelines*?

According to the *OECD Privacy Guidelines* ˙ ˙ ¬ ¡ ®¯ « ª š ¨ ˙ Ÿ š° š ˙ ©¡ š ª ¯ ˙ š ª µ ®¡ ¨ š° ¥ ª £ ˙ ° « ˙ š ª ˙ ¥ Ÿ ¡ ª ° ¥ ₵ ¥ ¡ Ÿ *Privacy Guidelines* ˙ ® ¥ š › ¨ ¡ ˙ ¥ ª Ÿ ¥ š › ¨ ¡ ˙ ¥ ª ˙ apply to personal data, when RFID technologies are used in contexts where RFID data is not related to an identified or identifiable individual, privacy principles do not apply. However, as we will see below, there may be privacy risks if the RFID data is associated to an individual even when the possibility to identify that individual is low. In any case, as acknowledged by the explanatory memorandum of the OECD *Privacy Guidelines* ˙ ° ¤ ¡ ˙ ¬ ®¡ œ¥ ¯ ¡ ˙ Ÿ ¥ ² ¥ Ÿ ¥ ª £ ˙ ¨ ¥ ª ¡ ˙ › ¡ ° ³ ¡ ¡ ª ˙ ¬ ¡ information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member œ« ± ª [75] ®µ

In some cases, RFID data is personal without ambiguity (*e.g.* in many access control applications). In other cases, RFID data may become personal data when it is possible to relate it to an identifiable individual. For example, when RFID is used in supply chain systems, the unique number stored on an RFID chip attached for example to a box of medicine to identify and track it, is not personal data. But the same RFID data can become personal data if it is collected or processed in such a manner as to enable a party to associate it with another set of information relating to an individual, *i.e.* by a nurse to track which patient has been provided with which medicine or by a drugstore to provide assistance services to patients.

Therefore, while some data are personal by nature (*e.g.* a name), other data can become personal once related to an identified or identifiable individual, which depends on context. One consequence is that parties who implement RFID systems are not systematically subject to data protection frameworks. A careful analysis of

---

75.   Explanatory memorandum of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, paragraph 41.

the nature and use of the RFID data at each step of its lifecycle is needed to help determine whether it should be considered personal and avoid turning it into personal data when it is not necessary for the purpose of the system.

One grey area still being debated relates to the possibility to use RFID unique data to distinguish an individual from other members of a group. This type of usage is in fact very similar to an HTTP cookie, with the difference that a cookie can be read only by the server that sent it to the client machine while RFID interoperability could, if enabled, allow for store A to read the RFID tags of objects sold by store B. The customer could benefit from such recognition, but could also in some cases consider the data collection an invasion of privacy; *a fortiori* where one of the stores would link the RFID data to the customer.

The European Article 29 Data Protection Working Party takes the view that the collection of a unique set of data, included in one or several RFID tags, which could be related to a specific individual, makes the information personal data within the scope of European data protection law. This view has been challenged by industry representatives who consider that data protection frameworks should apply only in cases where data processed through the use of RFID technology either contains personally identifiable information such as name, account or registration number or is combined with other personal data (*e.g.* personal data stored in a database or smart card).[76]

Privacy advocates argue that the capacity to determine that a set of characteristics belongs to a unique person can lead in some cases to damaging that person whether the person can be named or not. From a sufficiently high level of identification probability to raise privacy issues, even when the person cannot be formally identified. The risks associated to techniques that enable picking individuals out in a crowd relate to potential discrimination, dynamic pricing schemes or criminal activities. However, some businesses stress that considering RFID data as personal data in such cases would make some obligations such as the right of individuals to access the data related to them impossible to fulfil.[77]

At this stage, and while the debate is still ongoing,[78] one may consider that the ability to treat an individual uniquely is likely to raise privacy issues in some contexts, the level of privacy risk being proportional to several factors: *i)* the uniqueness of tag data (*e.g.* EPC numbers are fully unique. Proprietary numbers may not be as unique. Encrypted unique numbers are still unique numbers) or the

---

76. International Chamber of Commerce *et al.*, 2005, section 4.2; EPCglobal, 2005a, section 3.1; EPCglobal, 2007.

77. If person A is requesting access to his/her personal data, how would the data controller decide which record in its database corresponds to him/her? Person A would need to provide the tag(s) that have been associated to that person by the controller in order for the controller to retrieve the data in its system and give access. But nothing would prove that the tag(s) really belong to person A and therefore that the profile that would be accessed would not in fact be disclosed to another individual impersonating Person A.

78.

number of tags carried by an individual (the more tags, the higher the probability of uniqueness), *ii)* the probability that the tag(s) will or will not be shared with other persons and *iii)* the capacity to read the tag at a sufficient distance without the actual participation and knowledge of the individual.

Another key question is whether any RFID operator is a data controller.

The effectiveness of privacy and data protection frameworks relies to a great extent on the ability to assign responsibility to an entity for complying with data protection rules and being held accountable for failures in compliance. The notion of data controller was defined with this objective in mind and, in particular, to avoid imposing liability on organisations and individuals acting as agents for others. It is therefore, as mentioned in the *OECD Privacy Guidelines* explanatory memorandum, "anyone in a position to control".

According to the *OECD Privacy Guidelines*, a data controller is someone who is "competent to decide about the contents and use of personal data".[79] As stated above, whether RFID data is related to an identified or identifiable individual depends on the context: the identification number of a box of medicine is not personal data. But it becomes personal data if it is collected with the purpose of associating it with other information relating to an identified or identifiable individual.

A narrow interpretation of the definition of data controller is likely to lead to difficulties in the RFID context because deciding about the content of the RFID data is not the same as deciding about the content of personal data. In most cases, the manufacturer of a good will be competent to decide about the content of the RFID data but will not know whether it will ever be associated with individuals. Conversely, a store that implements RFID can decide to use the tag data on the goods to profile its customers. Therefore, in the context of RFID, the notion of data controller could be interpreted keeping in mind that deciding about the content of personal data will most often be closely related to deciding about the association of the tag data with individuals. To some extent, it is the use of the tag data that makes the data personal or not.

As a result, when a party reads an RFID tag and associates its data with an individual buying, carrying or wearing the tag, this party may be viewed as a data controller, taking over all the corresponding responsibilities derived from the Privacy Guidelines. But when a party provides an individual with a functional (not deactivated) tag and does not collect or store any RFID data associated with that individual, that party may be viewed as not subject to any obligation under the existing privacy protection frameworks. It would not be considered as a data controller, although providing functional tags to individuals would possibly enable a third party to track the individual in real time, potentially in a covert or illegal manner.

---

79.   "A party who is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf in *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, paragraph 1.

This case raises the question of whether or not this party would nevertheless have a responsibility to remove or deactivate the tag before passing the item to the individual or *i)* inform the individual that the good includes a functional tag that may be read by a third party at a distance and *ii)* provide him or her with information on the content of the tag, and how to prevent distance reading, or other intrusions. This ¥ ¯ ˙ ª « ° ˙ ° « ˙ ¯ ± £ £ ¡ ¯ ° ˙ ° ¤ Š ° ˙ ¯ ± œ¤ ˙ ¬ Š ®° ¥ ¡ ¯ ˙ ¯ ¤ « ± ¨ Ÿ ˙ › responsible for other duties assigned by the *Guidelines* to data controllers such as individual participation or purpose specification.

One approach to solving this question is that taken by the Ontario Privacy ˛ « © © ¥ ¯ ¯ ¥ « ª ¡ ®˙³¤ « ˙ ¯ ° Š ° ¡ ¯ ¯ ° ¤ Š ° ˙ « ® £ Š ª ¥ ¯ Š ° ¥ « ª ¯ contact and primary relationship with the individual should bear the strongest responsibility for ensuring privacy and security, regardless of where the RFID-tagged items originate or end-up in the product life-œµ œ¨ ¡ ˙ ˙ ! ¡ Š ¯ ± ®¡ ¯ ¯ ¯ ± œ¤ Š ¬ ¬ « ¥ ª ° © ¡ ª ° « ¢ ˙ Š ˙ ¥ ª ¢ « ® © š, from whom individuals ¥ ¯ ˙ ®š ° « ® can seek information, advice, assistance and remedies, have also been proposed. The $ ® ¥ ² š œµ ˙ ˝ ¡ ¯ ° $ ®š œ° ¥ œ¡ ¯ ˙ ¢ « ® ˙ ¡ ¬ ˙ « µ ©¡- ª ° « ¢ & ⁄ Ł › š ¯ ¡ Ÿ ˙ ˛ ¡ ª ¡ ® ˙ ¢ « ® ˙ ¡ © « œ® š œµ ˙ š ª Ÿ ˙ (bility for ª « ¨ « £ µ ˛ providing notice lies with the company having the direct relationship with the œ « ª ¯ ± © ¡ ® ˙ Ł ª ° ¡ ® ¡ ¯ ° ¥ ª £ µ ˙ ° ¤ ¡ ˙ Ÿ « œ± © ¡ ª ° ª « ° ¡ ¯ relationship with the individual may not know that the products they receive contain & ⁄ Ł ¯ ˙ š £ ¯ ˙ ˙ (¤ ¡ ® ¡ ¢ « ® ¡ ˙ ¯ ° ˙ ® ¡ œ« © © ¡ ª Ÿ ¯ ˙ ° ¤ incorporating RFID systems within its products should give notice to its direct purchasers of that fact, and to the extent practicable encourage its direct purchasers to give similar notice to their purchasers, and so on, with the objective of enabling the company having the direct relationship with consumers to give proper notice of ° ¤ ¡ ˙ ± ¯ ¡ ˙ « ¢ ˙ & ⁄[80] Ł ¯ ˙ ° ¡ œ¤ ª « ¨ « £ µ

In considering the disclosure responsibilities of parties providing tags to individuals, examination of other policy frameworks may be instructive. For ¡ ´ š © ¬ ¨ ¡ ˙ ° ¤ ¡ *Guidelines on Consumer Protection in the Context of Electronic Commerce* provide guidance on disclosure to consumers, calling on › ± ¯ ¥ ª ¡ ¯ ¯ ¡ ¯ ° « ˙ ¬ ® « ˙ ¥ Ÿ ¡ easily accessible information describing the goods or services offered; sufficient to enable consumers to make an informed Ÿ ¡ œ¥ ¯ ¥ « ª ˙ š › « ± ° ˙ › ¤ ¡ ° ¤ ¡ ® ˙ ° « ˙ ¡ ª ° ¡ ® ˙ ¥ ª ° « ˙ ° ¤ ¡ ˙ ° ® š in scope to transactions occurring electronically. However they are based on established consumer laws and policies governing fair commercial conduct applying both online and offline. It may therefore be useful to adapt this general information disclosure principle to all parties involved in the provision of RFID tags to individuals.[81] Another parallel could be drawn with the example of product safety and consumer information on risks.

---

80. See CDT, 2006. The Best Practices have been developed by a group of representatives from software and hardware vendors, organisations that use the technology, and industry and consumer organisations.

81. Although organisations that do not collect personal data from individuals do not have a disclosure obligation, many consider that informing individuals that they do not collect their personal data creates a trustworthy climate with potential benefits for the individuals, the company, and the general perception of the information technology involved, thus facilitating the adoption of the technology.

2.2.2.1.3. Knowledge and consent

The invisibility of the technology discussed above is a key characteristic of RFID and also acts as a risk multiplier for other potential privacy challenges such as profiling and tracking. For example, RFID-enabled profiling might be a less acute problem if deployed in a fair and transparent manner where individuals would have been informed and have agreed to it.

When RFID data is related to an identified or identifiable individual, several privacy principles reinforce each other to address the invisibility problem as well as most of the challenges mentioned in the previous section, such as tracking and profiling. In the *Privacy Guidelines* [illegible] requirement to specify the purpose of the collection by the time data is collected [illegible] only for that purpose and compatible purposes except with the consent of the individual [illegible] secret data processing on individuals and this approach is strongly supported by the [illegible]

While the need for knowledge or consent is reflected in most stakeholders' RFID guidance, the interpretations vary regarding what and how information should be provided, and when consent is appropriate.

There appears to be an emerging consensus among several consumer and privacy bodies as well as some industry stakeholders[82] that the provision of information to individuals is a fundamental requirement[83] and helps address the psychological challenge related to the invisibility of the technology by making it more visible.

While there may also be a consensus with regards to the necessity to inform individuals about the existence of data collection using RFID technologies, the issue of the content and effectiveness of information is a matter for discussion. A number of information elements might be included in RFID notices, beyond information about the purpose of the collection and the right of access. They include further information such as *i)* the existence of the tags, *ii)* their content, use and control, *iii)* the existence of an RFID environment; *iv)* the reading activity, *v)* the ability to disable tags and *vi)* where to obtain assistance.

The importance of privacy notices has long been recognised by the OECD, in particular in the online context.[84] However, research suggests that the efficacy of online notices is inversely proportional to the quantity and complexity of the information to be

---

82. Including the International Chamber of Commerce and EPCglobal Guidelines on EPC for [illegible] the presence of EPC on products or their packaging and will be informed of the use of EPC technology. This notice will be given through the use of an EPC logo or identifier on the [illegible]

83. [illegible]

84. OECD work on online privacy recognises the need for online privacy notices and OECD guidance (2003, p.29) encouraged business and government to develop such notices and post them on their websites.

conveyed (OECD, 2006b). In the case of RFID, providing full notification to consumers may not be feasible when items do not have sufficient space to accommodate detailed text and when data collection and sharing may be happening in real time.[85] One can expect that developing effective RFID privacy notices may be a greater challenge than in the case of online privacy notices that could take advantage of interactivity, hypertext links and the overall information driven nature of the web medium. Finally, it is unclear whether individuals would have the interest and capacity to understand and digest technical information related to RFID prior to making choices.

More research may be necessary to address this challenge. Possible solutions include innovative means of notifying people, such as audio, video alerts and the use of a universal symbol.[86] However, further work remains to be done to generate a consensus on the essential information to be delivered and effective means of conveying it.

When RFID data is related to an identified or identifiable individual, the opportunity for the individual to consent to the collection of personal RFID data and to the association of RFID data to his/her personal data is an important parameter both from the privacy/data protection and from the psychological (or trust) perspectives. The difficulty of providing efficient notices in RFID contexts may make consent an even more important consideration.

The explanatory memorandum of the *OECD Privacy Guidelines* suggests that, in general, knowledge should be the minimum requirement and recognises that consent is sometimes not practical or may be contrary to the public interest. The examples provided to illustrate cases where knowledge or consent cannot be considered necessary suggest, however, that they should remain a minority: routine updates and law enforcement.[87]

For the Article 29 Working Party consent is almost always appropriate unless the RFID system is authorised by law or is in the vital interests of an individual, as is the case for some health applications. Some businesses, official privacy bodies, and representatives from civil society also agree that consent is sometimes not necessary, but their views diverge regarding the criteria for dropping the need for consent.[88] Further work upon the consent issue might be necessary to narrow this difference.

---

85. See CIPL (Center for Information Policy Leadership), 2007.

86. The Center for Information Policy Leadership launched an initiative to develop such an RFID Transparency Symbol. See CIPL, 2007.

87. $ š ˜ ® š £ ® š ¬ ¤ ˙ 　 　 ˙ 　 ˙ 　 (¤ ¡ ˙ § ª « ³ ¨ ¡ Ÿ £ ¡ ˙ « ® ˙ œ« ª ¯ tial, ° ˙ « ¢ ˙ ° ¤ ¡ ˙ knowledge being the minimum requirement. On the other hand, consent cannot always be ¥ © ¬ « ¯ ¡ Ÿ ˙ ˙ ¢ « ® ˙ ¬ ® š œ° ¥ œš ¨ ˙ ®¡ š ¯ «ª ¯ ˙ ˙ Ł ª ˙ š Ÿ Ÿ ¥ ° ¥ « ª ˙ ¯ š ® š ¬ ¬ ® « ¬ ® ¥ š ° ¡ ˙ ˙ ° ¤ š ° ° ¤ ¡ ® ¡ ˙ š ® ¡ ˙ ¯ ¥ ° ± š ° ¥ data ¯ ³ ¤ ¡ ® ¡ ˙ ¢ « subject's knowledge or consent cannot be considered necessary. Criminal investigation activities and the routing up-Ÿ š ° ¥ ª £ ˙ « ¢ ˙ © š ¥ ¨ ¥ ª £ ˙ ¨ ¥ ¯ ° ˙ © š µ ˙ › ¡ ˙ © ¡ ª ° ¥ «

88. ˙ œœ« ® Ÿ ¥ ª £ ˙ ° « ˙ ¤ ¡ ˙ (® š ª ¯ ˙ ° ° š ° ¥ œ¡ ˙ sparently so ® ˙ ¨ ¥ š ¨ « £ ± ¥ ° ¤ š ˙ « « ª ¯ ± © ¡ ® ¯ ˙ § ª « ³ ¨ ˙ š Ÿ ˙ œš ª ˙ œ¤ « « ¯ ¡ ˙ ³ ¤ ¡ ª ˙ & ∕ Ł ¨ ˙ ¥ Clearing House recognises that, for some applications, it would be sufficient to inform individuals but that individuals should be able to disable tags, and calls for the prohibition « ¢ ˙ ° ® š œ§ ¥ ª £ ˙ ³ ¥ ° ¤ « ± ° ˙ œ« ª ¯ ¡ ª ° ˙ ∕ « ® ˙ ° ¤ ¡ ˙ Ł ª ° ¡ ® ª š œ° ¥ « ª choice, where possible and appropriate, is an essential element in developing consumer ° ® ± ¯ ° ˙ š Ÿ ˙ š œœ¡ ¬ ° š œ¡ ˙ (¤ ¡ ˙ I $ ˙ ducts (2005d) also ± ¨ Ÿ ¡ ˙ ¥ ¤ ª ¡ ¯ ˙ ˙ ¤ š ¡ ˙ ¯

Overall, knowledge and consent may be interpreted as a condition for individuals to make appropriate choices. However, one may argue that, sometimes, the individual has no real choice but to accept the collection of data in order to benefit from an associated service. For example, it is likely that public transportation systems that have started to deploy RFID systems for controlling access will ultimately remove the infrastructure for delivering and processing paper tickets. Individuals' choice will then be reduced to either accepting the collection of personal data or not using the transportation system. When the alternative to consenting to the collection of personal data is extremely costly for the individual, then the value of consent can become meaningless. Knowledge and consent are not a panacea for privacy protection.

2.2.2.2 Other safeguards

The following measures are not explicitly part of the OECD *Privacy Guidelines*, but may be useful to support or facilitate their implementation.

2.2.2.2.1. Technical measures

Generally, it may be worthwhile to consider using technical measures to prevent RFID information from being used in contexts where it could be linked to individuals. Privacy can be embedded in the design of RFID products and of RFID systems.

For example, specific data minimisation or aggregation/anonymisation techniques may help remove risks of function creep. The collection of the serial number segment of EPC numbers could for example, be technically prevented when it is not necessary for the purpose of the application. Generally, removing the possibility of linkage between ° ¤ ¡ ˙ & ∕ Ł ˇ ˙ ° Š £ ˙ Ÿ š ° š ˙ š ª Ÿ ˙ ¥ ª Ÿ ¥ ² ¥ Ÿ ± š � ˉ ˙ © Š µ ˙ › ¡ ˙ š ª ˙ ¡ ¢ ¬ ¡ ® ˉ « ª š ¨ ˙ ˙ Ÿ š ° š ˙ œš ° ¡ £ « ® µ ˙ š ª Ÿ ˙ ° ¤ ± ˉ ˙ ° « ˙ ¬ ® « ° ¡ œ° ˙ unlinking RFID data to individuals can also be performed at the back-end level.

Technical measures that empower both operators of RFID systems and individuals to control the technology may also help prevent or mitigate the risks. A number of research programmes are exploring technical means to protect privacy[89] but some mechanisms are already available. For example, the EPCglobal Class 1 Generation 2 ¬ ® « ° « œ« ¨ ˙ ˙ § ¥ ¨ ˙ ˙ œ« © © š ª Ÿ ˙ œš ª ˙ › ¡ ˙ ¥ ª ¥ ° ¥ š ° ¡ Ÿ ˙ š ° ˙ permanently.[90] The tag antenna of the IBM Clipped Tag can easily be removed by the customer or by the merchant thus turning a long distance (10 m) UHF tag into a short distance (2 cm) tag for warranty, traceability or other services (See Figure 8). Reducing the read range to a few centimetres can make participation by the individual to data collection a prerequisite and, in some cases, may mitigate — if not eliminate — the privacy risks in an innovative manner. However, as for security, given the complexity and

---

recognise Choice as one core principle and calls for additional efficient, cost effective and reliable alternatives to further enable customer choice.

89.   Ł ª ˙ ® ¡ ˉ ¬ « ª ˉ ¡ ˙ ° « ˙ ° ¤ ¡ ˙ ® ¡ ˉ ± ¨ ° ° ˉ ˙ « ¢ ˙ ° ¤ ¡ ˙ l ± w@ll « ¬ ¡ š ª ˙ , « ª ˙ support further development of privacy-enhancing technologies as one means to mitigate ¬ ® ¥ ² š œµ ˙ ® ¥ ˉ § ˉ ˙ ˙ l ± ® « ¬ ¡ š ª ˙ , « © © ¥ ˉ ˉ ¥ « ª ˙ ˙ š ˙ ∕ « research, see Juels (2005a) and Gildas Avoine ˉ ˙ & ∕ Ł ˇ ˙ ¡ œ± ® ¥ ° µ ˙ š ª Ÿ ˙ $ ® ¥ ² š œµ

90.   Consumer groups endorse the automatic deactivation of RFID tags at the point of sale, unless the consumer expressly agrees otherwise. See ANEC/BEUC, 2007.

variety of RFID technology and possible use scenarios, there is no one-size-fits-all perfect technical solution to protect privacy.

Figure 8. IBM Clipped Tag

Note: The UHF RFID tag can be read at a distance of 10 meters until the consumer tears it apart, removing the antenna. The RFID tag remains functional but can only be read at a distance of a few centimetres.

Source: Markowitz, 2006.

In addition, it should be noted that technical measures always have a cost that, in some cases, may discourage RFID manufacturers to embed privacy protection in the design of tags and RFID operators to include them in the design of their RFID systems. Moreover, in a competitive environment, it is unclear whether higher product prices (or a reduction in business profit margins per product) due to the use of privacy-friendly technologies can be easily converted into a market advantage for a given company and product. Strategies to provide incentives to businesses for designing and using RFID technologies that include sufficient privacy protections may be pursued.

Minimisation of data collection, anonymisation and the use of technical measures embedding privacy in the design of a system should not however prevent data controllers from providing individuals with notice to seeking their consent or active participation. And reciprocally, providing notice and requiring consent should not prevent data controllers from using privacy friendly technologies.

2.2.2.2.2. Privacy impact assessment

Because of the wide variety of technical configurations and use scenarios, there ¥ ¯ ˙ ª «-size-fits-˚š ¡ ¨ ˙ ° ¡ œ¤ ª ¥ œš ¨ ˙ ¯ « ¨ ± ° ¥ « ª ˙ ° ¤ š ° ˙ ³ « ± ¨ Ÿ ˙ c consent in all situations and balance adequately privacy, cost, convenience and usability. In-depth examination of whether and to what extent the use of the technology actually gives rise to privacy concerns in a given system may be required. Such analysis would involve examining the RFID application, the kind of data collected, the nature and technical specification of the RFID technology used and the potential that the collected data will be related to an identified or identifiable individual.

Approaches that include an assessment, at design stage, of the impact on privacy of an RFID system enable identifying and understanding privacy risks and best

strategies to mitigate them. They may be considered good practice. Echoing a consideration mentioned above regarding security risk management, the need for a holistic approach for privacy management may be considered as a good practice, considering each stage and each component of the overall system. In particular, the ³ ¤ « ¨ ¡ ˙ ¨ ¥ ¢ ¡ œµ œ¨ ¡ ˙ « ¢ ˙ ° ¤ ¡ ˙ & ⁄ Ł ˘ ˙ Ÿ š ° š ˙ ³ ¥ ° ¤ ¥ ª ˙ ˙ ° ¤ ¡ system should be considered. When considering the deployment of systems using interoperable RFID tags, the scope of such assessment may expand beyond the boundaries of the initial information system to include privacy risks associated with the whole life cycle of the tag.

As indicated in the section on security challenges, not all RFID technologies are equal regarding the likeliness of certain risks and, depending on the context in which they are used, some pose little or no specific risk at all. The choice of one RFID technology over another may have important consequences on privacy. A typical example is the operation range of radio wave systems compared to that of some magnetic induction systems that operate only at very short range, sometimes requiring individuals to actively take part in the reading process. One may suggest, as a good practice, to include privacy protection as one of the criteria for determining the characteristics of a planned system.

2.2.2.2.3. Awareness and understanding

Research in the United States and Europe[91] indicates that there is very limited public awareness of RFID and its implications but that consumers are looking for information.[92] The US FTC, the Ontario Privacy Commissioner, and European Commissioner Viviane Reding, to name a few, have called for greater efforts to increase public understanding of the benefits and risks of the technology. Increasing the general level of awareness and understanding about the possibilities and limitations of the technology may contribute to alleviate perceived or real psychological obstacles and may increase the efficacy of relevant privacy notices. It may help individuals differentiate among RFID technologies, understand how the technology is implemented where they interact with it, and ask the right questions with respect to security and privacy.[93] Beyond the legal obligation to provide notice to individuals, policy makers may want to consider the encouragement of operators to provide open, comprehensive, transparent and educational descriptions of RFID systems, with a view to providing essential information on how they work and how privacy has been taken into account.

Efforts to enhance the general level of awareness and understanding of the technology could also aim at using simple language and avoid the confusion that

---

91. Nearly two-thirds of the responses to the online public consultation carried out by the European Commission in 2006 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 (European Commissi« ª ˙ š ˙ ¸ š ¬ ˙ fi ¡ © ¥ ª ¥ ¯ ˙ ¯ ± ® ² ¡ µ ˙ although a bit higher in the United States, general awareness regarding RFID was low in both the United States and Europe.

92. Cap Gemini (2005a).

93. Awareness campaigns instructing individuals how to shield RFID tags so that they only expose personal data to those who need it could also be considered.

technical jargon may generate as the technology becomes more widespread and reaches out to the general public. Using RFID vocabulary with educational needs in mind, in particular with a clearly defined and understood terminology, may certainly help in this respect. For example, as mentioned earlier, the very acronym RFID is itself misleading and termino¨ « £ µ ˙ ¨ ¥ § ¡ ˙ ª ¡ š ® ˙ ¢ ¥ ¡ ¨ Ÿ ˙ š ª Ÿ ˙ ¢ š ® meaningful technically, is likely to create confusion for the general public.

Another source of confusion might come from generalisations regarding the level of risk associated with RFID, either to highlight or to downplay the risks, that may easily be inappropriate in specific situations and likely to create confusion. Debate over the risks and benefits of the technology frequently features scenario-specific examples leading to inaccurate generalisations. There are different RFID technologies with different properties and a large variety of ways to implement RFID systems. Sometimes, there may be compelling reasons for concern regarding privacy protection; sometimes the impact on privacy might be considered non existent. It is therefore important to avoid drawing general conclusions from specific examples: the drawbacks or the advantages of one implementation do not necessarily apply to another. Instead of focusing on the technology itself as being good or bad for privacy in general terms, a more balanced approach could consist in focusing on how it is implemented and whether and how risks are managed.

Efforts towards awareness and education may play an important role to reduce confusion and facilitate the deployment of RFID technologies for the benefit of business and individuals. However, as illustrated by the first section of this paper, RFID is a complex technology and will likely remain so. Therefore, there is a limit to the results that awareness and education can achieve. It cannot be expected that the average individual understands the ins and outs of RFID security and privacy prior to buying groceries at the supermarket, taking the subway, using a company badge, or his/her passport. Like for all information technologies that reach the general public, education is part of the answer to privacy and security issues, but cannot be the only answer.

Conclusion

RFID technologies are often p®¡ ¯¡ ª ° ¡ Ÿ ˙ › µ ˙ ˙ ° ¤ ¡ ¥ ® ˙ š Ÿ ² « œš ° ¡ ¯ ˙ š ¯
®¡ ² « ¨ ± ° ¥ « ª ˙ š ª Ÿ ˙ š ®¡ ˙ ¯ ± › ¦ ¡ œ° ˙ ° « ˙ š ˙ œ« ª ¯ ¥ Ÿ ¡ ®š › ¨ ¡
¯ « © ¡ ° ¥ © ¡ ¯ ˙ Ÿ ®¥ ¢ ° ¥ ª £ ˙ ˙ ° « ˙ ° ¡ œ¤ ª « ¨ « £ µ ˙ š ª Ÿ ˙ © š ®§ ¡ ° ¥
phenomenon may increase the visibility of a technology with significant potential
benefits to business and individuals. But it may also be counterproductive. The
complexity of RFID technologies, their technical variety, and the very large range of
possible applications they enable make them prone to being misunderstood. Like any
information technology, if RFID were implemented without appropriate consideration
of how to address privacy and security risks, it might damage the organisation that
has deployed it, and cause harm to the individuals involved. Should significant risks be
detected in existing or planned sensitive (*e.g.* passports, credit cards), large-scale
(*e.g.* transportation systems) or striking (*e.g.* RFID implants) RFID systems, there
³ « ± ¨ Ÿ ˙ › ¡ ˙ š ˙ ®¥ ¯ § ˙ ° ¤ š ° ˙ & ∕ Ł ˙ ¨ ing the perception of the « © ¡ ¯ ˙ & ∕ Ł ˙
technology by the general public and handicap its promising future. Such a scenario
has already arisen. A number of RFID systems have been deployed without sufficient
consideration for security and privacy, have been the target of severe criticisms by
privacy and consumer organisations and have led to the creation of opposition or anti-
¯ ¬ µ œ¤ ¥ ¬ ¯ ˙ £ ®« ± ¬ ¯ ˙ #ª ˙ ° ¤ ¡ ˙ « ° ¤ ¡ ® ˙ ¤ š ª Ÿ ˙ ° ¤ ¡ ˙ ¥ ª Ÿ
organisations have initiated a dialogue towards the development of privacy and
security best practices.

Transparency requires that individuals understand what the technology can do
and cannot do. Raising awareness about technology capabilities and limitations may
be essential to prevent individuals and organisations deploying RFID from perceiving
risks that do not exist or neglecting risks that actually exist, and to help them make
appropriate choices.

The OECD *Security Guidelines* provide a flexible and technology-neutral framework
that can be applied to RFID systems and networks. All the principles of the *Security
Guidelines* are relevant in the RFID context.

The OECD *Privacy Guidelines* are also applicable to RFID systems when personal
data is involved. The paper suggests that dialogue is still necessary to clarify or to
reach a consensus on a number of points, such as *i)* the notion of personal data and
data controller, *ii)* the nature of the information to provide to individuals and the best
means to communicate it to achieve efficient transparency and *iii)* the cases where
consent should be or not be required. Transparency, both from the data controllers
and from organisations providing tags to individuals without being considered as data
controllers has been pointed out as a key notion.

Although the OECD *Privacy* principles provide an essential framework for privacy
protection including for RFID systems, the report also highlights other practices and
measures that are incorporated into the 2002 *Security Guidelines* and could support
the implementation of the privacy principles and reinforce their effectiveness.

Echoing the essential requirement for security risk assessments, methodologies such as privacy impact assessment may help identify privacy issues from the outset of a project and select the most appropriate and cost-effective prevention and mitigation measures. They may prevent the development of systems that can breach privacy and ° ¤ š ° ´ ³ « ± ¨ Ÿ ´ › ¡ ´ ¡ ´ ´ ° ® ¡ © ¡ ¨ µ ´ œ « ¯ ° ¨ µ ´ ° « ´ ° ± ® ª ´ ¥ ª ° « ´ – cannot be expected that RFID security and privacy issues be solved totally at the RFID level, a holistic approach to security risk assessment, privacy impact assessment and their management has been highlighted throughout this paper as essential. It results from the variety of RFID technologies, possible applications and uses, from the constantly evolving nature of technologies and risks and from the interdependencies between RFID systems and the other systems they are connected with.

The availability and adoption of cost-effective and convenient technical safeguards for privacy protection and security might be key success factors for the successful deployment of the RFID. A number of such technical security and privacy controls are already available. Still, cost and technical complexity may remain an obstacle to their deployment in some application areas. Research is ongoing but efforts to foster it and initiatives to provide incentives for the adoption of such technical safeguards could be welcomed. Nevertheless, security and privacy should not solely rely on technical measures but rather on a mix of management, operational and technical safeguards. Finally, building privacy into the technology rather than bolting it on afterwards has been identified by several technical and policy experts as one potentially efficient © ¡ ° ¤ « Ÿ ´ ° « ´ ¬ ® « ° ¡ œ ° ´ ¬ ® ¥ ² š œ µ ´ ´ ' « ´ œ š ¨ ¨ ¡ Ÿ ´ $ ® ¥ ² š œ Enhancing Technologies, at the tag/reader or backend levels, could be encouraged.

Overall, RFID concerns a wide variety of stakeholders, from technologists and system designers to those who purchase the technology and their customers, including individuals who can carry tagged objects. Some stakeholders (*e.g.* on the supply side) are more likely to focus on preventive measures to reduce risk while others may focus on measures to mitigate the consequences of failures (*e.g.* on the use side). Effective communication and close co-operation by all stakeholders, including individuals, can help achieve increased security and privacy in RFID systems.

This report is the first step in OECD work to address security and privacy issues in the context of sensor based environments.[94] The findings and the present conclusions of this report are related to current and short-term uses of RFID technologies. But RFID technologies and uses evolve rapidly. It is therefore essential to monitor this evolution and detect potential new trends that would require further analysis and, possibly, modify these findings and lead to other conclusions. In particular, a number of anticipated developments are likely to raise challenges that are not addressed in this paper. These developments include for example the generalisation of objects tagging and open loop RFID applications processing personal data. The creation of an Ł ª ° ¡ ® ª ¡ ° ´ « ¢ ´ development and pervasiveness of ¡ other sensor-based technologies, ultimately blurring the boundaries between the virtual and the physical worlds could modify the nature of privacy and security challenges in the longer term and remain to be analysed and addressed.

---

94. It is complemented by work carried out by the Working Party on Information Economy (WPIE). See OECD 2007b and 2007c.

ANNEX I. Examples of RFID Standards

RFID standards include (AIM, n.d. 2006):

‹   A number of standards developed and adopted by national and regional standardisation organisations such as the American National Standards Institute (ANSI), the European Telecommunication Standards Institute (ETSI) and the European Committee for Standardization (CEN).

‹   Standards and specifications adopted by sector specific standards organisations, such as the specification for RFID biometric passports adopted by the International Civil Aviation Association (ICAO) which defines how ISO 14443 standard on contactless smartcards should be implemented for travel documents (ICAO, 2004) and the Automotive Industry Action Group (AIAG) ˚ ¬ ¬ ¨ ¥ œš ° ¥ « ª ˙ ' ° š ª Ÿ š ® Ÿ ˙ ¢ « ® ˙ & ⁄ Ł ˘ ˙ ˘ -1) ² ¥ œ ¡ ¯ ˙ ¥ ª ˙ « ® ˙ (¥ ® ¡ ˙ š ª Ÿ ˙ + ¤ ¡ ¡ ¨ ˙ Ł Ÿ ¡ ª-1°1)¥and¥ œš ° ¥ « ª ˙ ž š › ¡ ¨ ˙ ' ˙ °

‹   The MIT Auto-ID Center (now Auto-ID Labs)[95] specifications related to the Electronic Product Code (EPC), now included in the work of GS1/EPCglobal,[96] as well as EPCglobal Architecture Framework which includes a collection of interrelated standards for hardware, software, and data interfaces, with core services for enhancing the supply chain. EPCglobal/GS1 Class 1 Generation 2 standard has been ratified by ISO in July 2006 as ISO 18000-6C.

---

95.   The Auto-ID Center, created in 1999 was replaced in 2003 by the Auto-ID Labs which is a network of academic research labs.

96.   EPCglobal is a joint venture between GS1 (former EAN International) and GS1 US, former Uniform Code Council, both bodies regulating barcode in Europe and in the United States respectively.

The table below highlights the main international RFID standards.

Table 9. Main International RFID Standards

ISO 10536	Identification cards Contactless integrated circuit(s) cards (cards operating at very short proximity, < 1cm)
ISO 14443	Identification cards Proximity integrated circuit(s) cards (cards operating at 10 cm distance and include a microprocessor). For example, this is the standard chosen by ICAO for passports (ICAO, 2004)
ISO 15693	Identification cards contactless integrated circuit(s) cards Vicinity cards (cards operating at 1 meter and usually not containing a microprocessor)
ISO 18000	RFID for Item Management - Air Interface (description of the standard air interface operating below 135 KHz, at 13.56 MHz, 2.45 GHz, 860 MHz to 960 MHz, 433 MHz)
ISO 10374	Freight containers -- Automatic identification (includes a container identification system, data coding systems, description of data, performance criteria and security features)
ISO 11784, ISO 11785, ISO 14223	Animal tagging
ETSI TS 102.190, ISO 18092, and ECMA 340	Near Field Communications Interface and Protocol-1 (NFCIP-1)
Standards directly related to Electronic Product Codes (EPC):	
Auto-ID Center Specifications	‹ 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification (communications interface and protocol, RF, and tag requirements, operational algorithms for 900MHz communications) ‹ 13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification (communications interface and protocol, RF, and tag requirements). ‹ 860MHz -- 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification (defines communications interface and protocol, RF, and tag requirements). ‹ Conformance Requirements Specification v. 1.0.4 for Class-1 Generation2 UHF RFID (compliance for physical interactions (the signaling layer of the communications), operating procedures, and commands; between interrogators and tags for 860 MHz 960 MHz communications.)
EPCglobal Architecture Framework	A collection of interrelated standards for hardware, software, and data interfaces, with core services for enhancing the supply chain through the use of Electronic Product Codes (EPCs). Includes standards for : ‹ Tag Data ‹ EPC Tag Data Translation ‹ ... became ISO 18000-6C in July 2006 ‹ Reader Protocol ‹ Reader Management ‹ Application Level Events ‹ Object Naming Service (ONS) ‹ Certificate Profile ‹ Drug Pedigree ‹ EPC Information Service version 1.0, approved on 12 April 2007

Sources: Pedris-Lopez, 2006; RFID Association Australia website (www.rfidaa.org/standards) ; EPCglobal website (www.epcglobalinc.org/standards/);

ANNEX II. NFC, UWB, ZigBee, RuBee, Wi-Fi, Ultrasonic Technologies

Near Field Communication (NFC): is a short-range technology that enables two devices to communicate when they are brought into actual touching distance. Sponsored by the NFC Forum which groups more than 100 companies including Sony, NXP (Philips) and Nokia, NFC enables sharing power and data using magnetic field induction at 13.56MHz (HF band), at short range, supporting varying data rates from 106kbps, 212kbps to 424kbps. A key feature of NFC is that it allows two devices to interconnect. In reader/writer mode, an NFC tag is a passive device that stores data that can be read by an NFC-enabled device (*e.g.* smart poster, for which a technical specification was developed). In Peer-to-Peer mode, two NFC devices can exchange data. For example, Bluetooth or Wi-Fi link set up parameters can be shared using NFC and data such as virtual business cards or digital photos can be exchanged. In Card Emulation mode, the NFC device itself acts as an NFC tag, appearing to an external reader as a traditional contactless smart card. This enables contactless payments and e-ticketing, for example. NFC is backed by 14 mobile operators representing 40% of the global mobile market.[97] NFC standards are acknowledged by major standardisation bodies and based on ISO/IEC 18092.

NFC mode	Applications
Peer to peer mode	Connect electronic devices
Read/Write mode	Access digital content (*e.g.* poster)
Card emulation mode	Make contactless transactions

ZigBee[98]: developed and promoted by the association of companies called ￥£ ˝ ¡ ¡ ˙ Š ¨ ¨ ￥ š ª œ¡ ˙ ° ¤ ¡ ˙ . ￥£ ˝ ¡ ¡ ˙ ¯ ¬ ¡ œ￥ ¢ ￥ œš ° ￥ « ª network layers to IEEE 802.15.4 standard for wireless low-rate personal area networks. It operates in the UHF/microwave bandwidth with battery powered tags that communicate with each other. ZigBee adds to IEEE 802.15.4 the option of AES-128 encryption security. ZigBee protocols are intended for use in embedded applications requiring low data rates and low power consumption, enabling devices to form a mesh network of up to 65 000 nodes, covering a very large area.[99] It

---

97.   ! « › ￥ ¨ ¡ ¯ ˙ fl « ¬ ¡ ˙ ° « ˙ › ¡ ˙ ¯ © š ® ° ˙ ³ š ¨ ¨ ¡ ° ˙ ˝ ˝ ˛ " ¡ ³ ¯
       November 2006, http://news.bbc.co.uk/2/hi/technology/6168222.stm.

98.   See the Zigbee Alliance web site: www.zigbee.org. The name ZigBee comes from the zigzag path of bees which serves to signal new food location to other members of the colony, an analogy of mesh network topology.

99.   «' « ˙ + ¤ « ˙ " ¡ ¡ Ÿ ¯ ˙ . ￥£ ˝ ¡ ¡ ˙ ˙ " « ² ¡ © › ¡ ® ˙ ˙
       http://rfdesign.com/next_generation_wireless/who-needs-zigbee/ See also
       www.zigbee.org/en/press_kits/092706/Documents/ZigBeeTutorial.pdf.

targets general-purpose, inexpensive, self-organising, mesh networks that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, domotics, etc. The resulting network will use very small amounts of power so individual devices might run for a year or two using the originally installed battery.

RuBee is a commercial name for a peer to peer communication protocol designed for active or passive tags operating at Low Frequency (using magnetic induction), suitable in environments containing water and/or metal. It is being ¯ ° š ª Ÿ š ® Ÿ ¥ ¯ ¡ Ÿ ˙ › µ ˙ Ł ı ı ı ˙ š ¯ ˙ $ ˙ Ł ı ı ı ˙ ' ° š ª Ÿ š " ¡ ° ³ « ® § ˙ $ ® « ° « œ « ¨ ˙ ˙ ˙ ° œœ« ® Ÿ ¥ ª £ ˙ ° «time‑ tag¡ ı ˙ ˙ ° ¤ ¡ ¯ ¡ š ® œ ¤ š › ¨ ¡ ˙ ¬ ® « ° « œ « ¨ and subnet addresses linked to asset® ¡ ¯ ¯ ¡ ¯ taxonomies that run at speeds of 300 to 9 600 Baud. RuBee Visibility Networks are managed by a low-cost Ethernet enabled router. Rubee enables tag networks and telepresence applications. Individual tags and tag data may be viewed as a stand-alone, webserver from anywhere in the world. Each RuBee tag, if properly enabled, can be discovered and monitored over the World Wide Web using popular search engines (*e.g.* Google).[100]

Wi-Fi and **Bluetooth** communication protocols are usually not considered as RFID or sensor technologies since they were originally designed for connecting devices such as PCs, laptops and printers. They are commercial names for communication protocols IEEE 802.11 and IEEE 802.15.1. Both operate in the same frequency range (near 2.4 GHz). Bluetooth is a building block for personal area networks (PAN) or short distance wireless networks which connect together devices such as PC, Personal Digital Assistants (PDA), peripherals (keyboard, © « ± ¯ ¡ ˙ ˙ œ¡ ägers, etc.¤ Wi-Fi ¡ was developed to be used for laptop connectivity to local area networks but is now increasingly used for more services, including Internet and voice over IP, and connectivity of computer devices such as printers, webcams, DVD players, etc. However, several vendors have developed Wi-Fi active tags that allow for the use of existing Wi-Fi coverage and access points instead of deploying a specific RFID communication infrastructure. They are being used for example for asset tracking in power plants and hospitals, by theme amusement parks such as in Legoland (Denmark) to help parents find their children « ® ˙ ° « ˙ § ¡ ¡ ¬ ˙ ° ® š œ § ˙ « ¢ ˙ š ± ° « © « ° ¥ ² ¡ ˙ ² ¡ ¤ ¥ œ ¨ ¡ ¯ ˙ ¥ ª ˙ * ¡ (Malykhina, 2005; Collins, 2004; Aeroscout, 2005).

Ultra Wide Band[101] can enable wireless connectivity at very large bandwidth for very close electronic devices (*e.g.* computer and monitor). UWB technology transmits information spread over a very large bandwidth (25% or more of the

---

100. Ł ı ı ı ˙ ″ ¡ £ ¥ ª ¯ -Wavelength Standard for Health Care, Retail and Livestock * ¥ ¯ ¥ › ¥ ¨ ¥ ° µ ˙ " ¡ ° ³ « ® § ¯ ˙ ˙ ˙ Ł ± ª ¡ ˙ ˙ ˙ Ł ı ı ı ˙ ˙ ˙ http://standards.ieee.org/announcements/pr_p19021Rubee.html.

101. Elements of information about UWB come from the following sources: Ultrawideband planet, FAQ, www.ultrawidebandplanet.com/faq/ ˙ ° ª ¥ ª ° ® « Ÿ ± œ ° ¥ « ª ° « ˙) ˙ ° ® š) + ″ ³ ¥ ® ¡ ¨ ¡ ¯ ¯ & š ¢ š ¡ ˙ ˙ Ž « ¨ ¥ œ ˙ / ¡ › ® ± š ® µ www.deviceforge.com/articles/AT8171287040.html Ł ª ° ¡ ¨ š ª Ÿ) + ″ www.intel.com/standards/case/case_uwb.htm.

center frequency or at least 500 MHz)[102] but at very low power levels thus not interfering with other narrower band devices nearby. The receiver translates the pulses into data by listening for a familiar pulse sequence sent by the transmitter. As the data is moving on several channels at once, it can be sent at high speed, up to 1 gigabit per second. It also has the ability to penetrate walls. Frequency regulations limits UWB to low power levels in order to keep interferences at or below the level of noise produced unintentionally by electronic devices such as TV sets. As a consequence, UWB is limited to short-range applications, enabling wireless connectivity (*e.g.* wireless monitors, camcorders, printing, music players), home or office networking, automotive collision detection systems, medical imaging, etc. It is promoted by two industry associations, the WiMedia Alliance and the UWB Forum.[103] UWB is a fairly new technology that was regulated in 2002 by the US Federal Communications Commission (FCC), in 2006 in Japan and in 2007 in Europe (Yomogita, 2006; Holland, 2007). As it has been regulated only recently, the type of innovative applications it will enable in the future is still unclear.

Ultrasonic (based on ultrasound waves) technology enables tags to transmit unique 20 kHz to 40 kHz acoustic signals to a receiver. The signal does not require a line of sight between the reader and the tag, but it does not penetrate solid walls and the receiver has to be located in the same room. It is not subject to electromagnetic interferences and does not create such interferences. Tags are battery powered. This technology has been tested and deployed in the hospital environment.[104]

Hewlett Packard ¯ ¯ fl $ ¡ ´ ¬ ¡ ® ¥ © ¡ ª ° š ¨ ˙ ! ¡ © « ® µ ˙ ' ¬ « ° ˙ œ suggests that technological innovation is li§ ¡ ¨ µ ˙ ° « ˙ ¢ « ® œ ¡ ˙ ± ¯ ˙ ° « ˙ ® ¡ ² ¥ ¡ ³ š ª Ÿ ˙ Ÿ ¡ ¢ ¥ ª ¥ ° ¥ « ª ¯ ˙ « ¢ ˙ & ⁄ Ł ˘ ˙ › « ± ° ˙ ° ¤ ¡ ¯ ¥ ¶ ¡ ˙ « ¢ ˙ š ˙ broadcast data at 10 megabit per second, has a built-in antenna and a storage capacity ranging from 32 kilobytes to 512 kilobytes. It uses microwaves (2.45 GHz) but needs to be positioned very close (1 mm) to the reader for the communication to take place. It has read/write capacity and enables cryptography. These chips, which could reach the market within two or three years, can store large amounts of text, sound, pictures and even video clips. For example, they could enable adding a video œ ¨ ¥ ¬ ˙ ° « ˙ š ˙ ¬ « ¯ ° œ š ® Ÿ ˙ ˙ š ˙ © ¡ Ÿ ¥ œ š ¨ ˙ ® ¡ œ « ® Ÿ ˙ ° « ˙ š ˙ instructions to a consumer medicine bottle, storing a document electronically on the ¬ ® ¥ ª ° ¡ Ÿ ˙ œ « ¬ µ ˙ ˙ ˙ ˙ š ° ° š œ ¤ ¥ ª £ ˙ š ˙ œ « ¬ µ ˙ « ¢ ˙ ° ¤ ¡ ˙ © š ± š ¯ ˙ ³ š µ ˙ § ª « ³ ³ ¤ ¡ ® ¡ ˙ ° « ˙ ¢ ¥ ª Ÿ ˙ ¥ ° ˙ « ° ¡ Ÿ ˙ › µ ˙ š œš ¬ š œ ¥ ° µ ˙ ˙ ¬ ® « œ ¡ ¯ ˙ ¯ ¥ ª £ ˙ š ª ˙ š ¡ ° ³ « ® §Æ tion like œš ¬ š › ¥ ¨ ¥ ° µ mini-œ « © ¬ ± ° ¡ ® ¯ ˙ ® š ° ¡ ® ˙ ° ¤ š ª ˙ ˙ ¥ § ¡ ˙ ¬ š ¯ ¯ ¥ ² ¡ ˙ ° š £ ¯ demonstrates that the differences between a tag and a computer are decreasing. (Kanellos, 2006; Krill, 2006; HP, 2006; Taub; 2006)

---

102.   ° ¨ ˙) + ¨ ˙ ¯ ¥ £ ª š ¨ ¨ œ ¡ ª ° ¡ ®¡ Ÿ ˙ š ° ¨ fi fl ¶ ˙ ³ « ± ˙ Ÿ ˙ ¤ š ² ¡ ˙ š ˙ © ¥ ª š minimum bandwidth of a UWB signal centered at 4 GHz would be 1 GHz. The most common technique for generating a UWB signal is to transmit pulses with durations less ° ¤ š ª ˙ ˙ ª š ª « ¯ ¡ œ « ª Ÿ ˙) + ¨ ¯ ®¡ ¯ « ± ® œ ¡ ˙ œ ¡ ª ° ¡ ® ˙ $ š ˙ « ³ ¥ Ù www.palowireless.com/uwb/tutorials.asp.

103.   See www.wimedia.org and www.uwbforum.org.

104.   (¡ ¯ ° ¥ ª £ ˙) ¨ ° ® š Ÿ š « ª « « ¬ ˙ (® š œ ¡ See O'Connor, *RFID Journal*, "Aethon Gets Ready to Ship New Tug", 15 March 2006, www.rfidjournal.com/article/articleprint/2199/-1/1/. See www.sonitor.com.

Figure 9. HP Memory Spot

° ° ° Š œ¤ ˙ Š ˙ œ¤ ¥ ¬ ˙ ° « ˙ ˙ ° ¤ ¡ ˙ ¬ ® ¥ ª ° ¯ ˙ « ¢ ˙ ¬ ¤ « ° « £ ®Š ¬ ¤ ¯ ˙ Š ª Ÿ ˙ Š Ÿ Ÿ ˙ ©

Source : HP Memory Spot.

ANNEX III. Security Exploits

This Annex provides a list of security exploits found in the literature.

Lack of basic security:

‹ Of the ten different types of RFID systems used in hotels, a hacker found that none used encryption. He also found out that many systems which use encryption failed to change the default key set by the manufacturer, or that they used sample keys provided in user manuals sent with the cards. He created a database of such sample keys to conduct dictionary attacks and was able to open about 75% of all the cards collected. In addition, he created a master key card to open every room in a hotel, office or other facility. He œ¨ « ª ¡ Ÿ ˙ $ ¤ ¥ ˉ ¥ ¬ ˉ ˙ ı ¨ ¡ œ° ®« ª ¥ œ¯ ˙ ˙ ! ¥access®¡ ˙ ˙ ° ¤ ¡ ˙ system. To create a master key he simply needed two or three key cards for different rooms to determine the structure of the cards. (Zetter, 2006)

‹ The same hacker was also able to crash RFID-enabled alarm systems designed to sound when an intruder breaks a window or door to gain entry. Such systems require workers to pass an RFID card over a reader to turn the system on and off. The hacker found that by manipulating data on the RFID chip, he could crash the system, opening the way for a thief to break into the building through a window or door.

‹ According to a Japanese news¬ š ¬ ¡ ® ˙ Ÿ š° š ˙ š › « ± ° ˙ ° ¤ ¡ ˙ ¬ š ˉ ¡ ª £ ˙ and exit stations stored in the Suica card[105] can be read by basic RFID readers, such as the one embedded in Sony Clié PDA. The journalist claimed that the possibility to read such information at a distance could facilitate stalking.[106] Similarly, a British newspaper reports that access to data œ« ®®¡ ˉ ¬ « ª Ÿ ¥ ª £ ˙ ° « ˙ ˙ ¡ ² ¡ ®µ ˙ ¦ « ± ®ª ¡ µ ˙ ° š § ¡ ª ˙ ¥ ª ˙ ° Oyster card is possible by keying in its serial number on a website or taking the card to a reader machine in the underground. The journalist reports that this information can be used in divorce procedures.[107]

‹ (¤ ¡ ˙ ¥ ©¬ ˙ š ° ° š › ¨ ¡ ˙ &⁄ £ ˇ ˙ ˙ ˙ * ¡ ®¥ œ¤ ¥ ¬ ˙ ³ š ˉ ˙ œ¨ « ª ¡ Ÿ year old Canadian hardware developer for the purpose of an article in the magazine *Wired* ˙ (¤ ¡ ˙ ° š £ ˙ ¥ ©¬ ˙ š ° ¡ Ÿ ¥ ª ˙ ° ¤ ¡ ˙ ¦ « ± ®¡ š ˙ the article, featured no security at all (Newitz, 2006).

---

105. 10 million Suica cards were issued between 2001 and 2004. See www.jreast.co.jp/e/press/20041003/.

106. http://kodansha.cplaza.ne.jp/digital/it/2003_08_27/content.html, article in Japanese.

107. ƒı ³ ˙ š ª ˙ # µ ¯ ° ¡ ® ¸ š ® Ÿ ˙ œ*The Independent on Sunday*¸ reproduced at ˙ £ ¡ ˙ www.theabi.org.uk/press/p0602.htm

‹ According to the same *Wired* article, 5 million RFID tags have been sold to easier for libraries to change the software and hardware to write on the tag as well.

Insufficient security

‹ million tags ExxonMobil SpeedPass payment transponders and over 150 million automobile ignition keys has been cloned in 2005 by RSA Laboratories using inexpensive off-the-shelf equipment. The team purchased gasoline at an ExxonMobil station multiple times with the cloned pass and spoofed a Ford car immobiliser system (Bono *et al.*, 2006).

‹ Electronic passports have been under intense scrutiny since their announcement:

　! A German computer security consultant successfully cloned an ICAO compliant RFID electronic passport using an off-the-shelf RFID reader and software tools (Zetter, 2006).

　! The same consultant conducted a successful attack against RFID passport readers by cloning a passport chip and modifying the image it contained to exploit a known vulnerability in the software library used to decode the image (Zetter, 2007).

　! A shielding solution planned for the US e-passport that is aimed at preventing remote reading of the passport when the document is not open was found to allow such reading when the booklet is only a half inch open, such as in a pocket or handbag (Flexilis, 2006). The prototype Dutch RFID passport, featuring the Basic Access Control[108] protection, was cracked by security specialists and they claimed that the attack was possible at a 10m range (Lettice, 2006).

‹ Expensive cars secured by software methods can be stolen using a simple X5 SUVs in the last six months did [used] software programs on a laptop to wirelessly break into the car's computer, open the doors, and start the

---

108.　Basic Access Control is an optional feature which unlocks the RFID chip only if the data exchanged using information derived from the content of that zone.

ANNEX IV. The Electronic Product Code (EPC) Number Structure

01	0000A89	00016F	000247DC0
Header 8 bits	EPC manager 28 bits	Object class 24 bits	Serial number 36 bits

(¤ ¡ ´ ı $ ˛ ´ ¥ ¯ ´ Š ´ £ ¡ ª ¡ ® ¥ œ ´ ± ª ¥ ² ¡ ® ¯ Š ¨ ´ ª ± © › ¡ ® ¥ ª £ ´
¥ ª ´ ¯ œ « ¬ ¡ ´ ° « ´ ° ¤ ¡ ´ › Š ® œ « Ÿ ¡ ´ ª ± © › ¡ ® ¥ ª £ ¯ ¯ œ ¤ ¡ © ¡ ´ ´) $
capability to identify every single, ¥ ª Ÿ ¥ ² ¥ Ÿ ± Š ¨ ´ ´ ¬ ® « Ÿ ± œ ° ´ ¥ ° ¡ © ´
number identifies the company involved in the production of the item
(manufacturer) and the object class defined the product itself. The Serial
number is unique (within the scope of the other numbers) for an individual
product entity. The 96-bit code can thus provide unique identifiers for 268
millions companies (2²⁸). Each manufacturer can have 16 million (2²⁴) object
classes and 68 billion serial number (2³⁶ ´ ¥ ª ´ ¡ Š œ ¤ ´ œ ¨ Š ¯ ¯

(*Source*: JISC Technology and Standards Watch, May 2006).

(¤ ¡ ´ ¯ ° ® ± œ ° ± ® ¡ Ÿ ´ ¤ ¥ ¡ ® Š ® œ ¤ µ ´ « ¢ ´ ı $ ˛ ´ ª ± © › ¡ ® ¯ ´ ª ¡ ¯
*distinct segments of the EPC string (*i.e. *the EPC Manager Number segment*
identifies who, the Object Class segment identifies what, and the Serial Number
segment identifies which). As a result, each segment conveys a different level of
¥ ª ¢ « ® © Š ° ¥ « ª ´ Š › « ± ° ´ ° ¤ ¡ ´ ¥ ° ¡ © ´ ´ ³ ¤ ¥ œ ¤ ´ ° ¤ ¡ ´ ı $ ˛ ´

Source: EPCglobal, EPCglobal Position Paper, Implementation of the EPCglobal Network Root ONS,
Release 1, 2005.

ANNEX V. Examples of Privacy References

A large number of resources related to RFID privacy are available. This list reflects only a subset of the documents that the Secretariat has gathered to date. It only contains documents with a policy guidance dimension, issued either by governmental bodies or by organisations with a public policy focus or international orientation. It is complementary to the bibliography.

A.   RFID in general

DPAs and other official bodies

International
25th International Conference of Data Protection and Privacy Commissioners   Sydney
www.cnil.fr/fileadmin/documents/uk/Resolution_RFID-VA.pdf

Regional
Article 29 Working Party
January 2005
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

www.rfidconsultation.eu

Canada
Ontario - Information and Privacy Commissioner
www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf
www.ipc.on.ca/images/Resources/up-rfidtips.pdf

Germany
Resolution of the 72nd German Data Protection Conference of the Federation and the
Länder held in Naumb

Federal Commissioner for Data Protection and Freedom of Information
www.bfdi.bund.de/cln_029/nn_672292/EN/Topics/technologicalDataProtection/Artikel/RFID_E2_80_93RadioTagsForAllOccasions.html

Italy
GarantePrivacy
www.garanteprivacy.it/garante/doc.jsp?ID=1121107

France
CNIL
Address by Philippe Lemoine relating to Radio-Tags (RFIDs), 2003
www.cnil.fr/fileadmin/documents/uk/CNIL-lemoine-RFID_102003_VA.pdf

Japan
fi ± ¥ Ÿ ¡ ¨ ¥ ª ¡ ¯ ˙ ¢ « ® ˙ $ ®¥ ² š œµ ˙ $ ®« ° ¡ œ° ¥ « ª ˙ ³ ¥ ° ¤ ˙ & ¡ £ š ® Ÿ ˙
www.rfidconsultation.eu/docs/ficheiros/JP_RFID_PrivacyGLsRev_METI.pdf

Korea
& ∕ Ł ˘ ˙ $ ®¥ ² š œµ ˙ $ ®« ° ¡ œ° ¥ « ª ˙ fi ± ¥ Ÿ ¡ ¨ ¥ ª ¡ ˙ ± ª « ¢ ¢ ¥ œ¥ š ¨
www.worldlii.org/int/other/PrivLRes/2005/3.html

Netherlands
Minister of Economic Affairs,
& ∕ Ł ˘ ˙ ¥ ª ˙ ° ¤ ¡ ˙ " ¡ ° ¤ ¡ ®¨ š ª Ÿ ¯ ˙ ˙ ' ¡ ¬ ° ¡ © › ¡ ®˙
Parliament)

United Kingdom
ICO ˘ š ° š ˙ $ ®« ° ¡ œ° ¥ « ª ˙ ° ¡ œe¤ ª ± ¥ œš ˙ ° ¨ £ ± ¥ Ÿ š ª œ¡
www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides
/radio_frequency_indentification_tech_guidance.pdf
www.rfidconsultation.eu/docs/ficheiros/RFID_Ofcom_statement.pdf

United States
« The use of RFID for Human Identification» (Draft Report),
Department of Homeland Security
www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf

& ∕ Ł ˘ ˙ š ¬ ¬ ¨ ¥ œš ° ¥ «ª ¢ « ® ª œ« ª¥ ©± © ¡¥ ®eš ° ¥ « ¥ «!ª š ® œe¤ ˙
Federal Trade Commission
www.ftc.gov/os/2005/03/050308rfidrpt.pdf

Business

Enterprise Privacy Group A privacy code of conduct for RFID technologies 3 May
2005
www.rfidconsultation.eu/docs/ficheiros/EPG_RFID_Privacy_Code_of_Conduct.pdf

EPCglobal Guidelines on EPC for consumer products
www.epcglobalinc.org/public/ppsc_guide/

EPCglobal ı $ ¸ £ ¨ « › š ¨ ˙ ' ± › © ¥ ¯ ¯ ¥ « ª ˙ « ˙ ° ¤ ¡ ˙ ® ° ¥ œ¨ ¡ ˙ +
Working Document 10107/05 WP 105 of 19 January 2005 on Data protection issues
related to & ∕ Ł ˘ ˙ (¡ œe¤ ª « ¨ « £ µ
http://ec.europa.eu/justice_home/fsj/privacy/docs/rfid/epcglobal_en.pdf

EPCglobal ı $ ¸ £ ¨ « › š ¨ ˙ & ¡ ¯ ¬ « ª ¯ ¡ ˙ ° « ˙ ° ¤ ¡ ˙ ı) ˙ & ∕ Ł ˘ ˙ # ª ¨ ¥ ª ¡ ˙
www.rfidconsultation.eu/docs/ficheiros/EPCglobal_Response_to_EU_RFID_Online_Cons
ultation.pd

EuroCommerce Position paper
www.rfidconsultation.eu/docs/ficheiros/EuroCommerce_Position_on_RFID.pdf

International Chamber of Commerce Ł ˛ ˙ ¯ ¬ ® ¥ ª œ ¥ ¬ ¨ ¡ ¯ ˙ ¢ « ® ˙ ® ¡ ¯ ¬ « ª ¯ ¥ › ˙
« ¬ ¡ ® š ° ¥ « ª ˙ « ¢ ˙ ¡ ¨ ¡ œ ° ® « ª ¥ œ ˙ ¬ ® « Ÿ ± œ ° ˙ œ « Ÿ ¡ ¯
www.iccwbo.org/home/statements_rules/statements/2005/EPC_principles.asp

UK RFID Council - UK Code of practice for the use of RFID in retail outlets
www.rfidconsultation.eu/docs/ficheiros/code_release_1_0_120406__logos.pdf

Civil Society

˛ ¡ ª ° ¡ ® ˙ ¢ « ® ˙ ˘ ¡ © « œ ® š œ µ ˙ š ª Ÿ ˙ (¡ œ ¤ ª « ¨ « £ µ ˙ + « ® § ¥ ª £ ˙ fi ® «
¢ « ® ˙ ˘ ¡ ¬ ¨ « µ © ¡ ª ° ˙ « ¢ ˙ & ⁄ Ł ˘ ˙ (¡ œ ¤ ª « ¨ « £ µ
www.cdt.org/privacy/20060501rfid-best-practices.php

EPIC Guidelines on Commercial Use of RFID Technology
www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf

Privacy Rights Clearinghouse - & ⁄ Ł ˘ ˙ ¬ « ¯ ¥ ° ¥ « ª ˙ ¯ ° š ° ¡ © ¡ ª ° ˙ « ¢ ˙ ˛ « ª ¯ ± ©
Ž ¥ › ¡ ® ° ¥ ¡ ¯ ˙ # ® £ š ª ¯ š ° ¥ « ª
www.privacyrights.org/ar/RFIDposition.htm

Trans Atlantic Consumer Dialogue & ¡ ¯ « ¨ ± ° ¥ & ˝ Ÿ ¥ ‹ ˙ ⁄ ® ¡ ¯ ± ¡ ª œ µ ˙ Ł Ÿ ¡ ª ° ¥
April 2005.
www.tacd.org/docs/?id=274

B. RFID in specific areas

Libraries
 $ ® ¥ ² š œ µ ˙ š ª Ÿ ˙ ˛ « ª ¢ ¥ Ÿ ¡ ª ° ¥ š ¨ ¥ ° µ ˙ fi ± ¥ Ÿ ¡ ¨ ¥ ª ¡ ¯ ˙ ˙ ° © ¡ ® ¥
www.ala.org/ala/oif/statementspols/otherpolicies/rfidinlibraries.pdf

Ontario Information and Privacy Commissioner
 fi ± ¥ Ÿ ¡ ¨ ¥ ª ¡ ¯ ˙ ¢ « ® ˙ ± ¯ ¡ š £ ˙ & ⁄ Ł ˘ ˙ ° š £ ¯ ˙ ¥ ª ˙ # ª ° š ® ¥ « ˙ $ ± › ¨
www.ipc.on.ca/images/Resources/rfid-lib.pdf

Drugs & healthcare
RFID Feasibility Studies and Pilot Programs for Drugs / Compliance policy guide
www.fda.gov/oc/initiatives/counterfeit/rfid_cpg.html

Workplace
) " Ł ˙ & ⁄ Ł ˘ ˙ ¥ ª ˙)° "¤ ł ¨ œ « Ÿ ® ¡ § ¬ « ˝ $ œ efi « « Ÿ ˙ $ ® š œ ° ¥ œ ¡
www.union-
network.org/uniindep.nsf/2702f48e48fad7dac125718e0034fd79/$FILE/RFIDdraft.pdf

 $ ¡ ® ² š ¯ ¥ ² ¡ ˙ ˛ « © ¬ ± ° ¥ ª £ ˙ (® ¡ ª Ÿ ¯ ˙ š ª Ÿ ˙ Ł © ¬ š œ °
www.bsi.de/literat/studien/percenta/Percenta_eacc.pdf

Bibliography

Aeroscout (2005), *Port of Venice Deploys Aeroscout Visibility System for Vehicle Inventory Management*, Aeroscout, San Mateo, www.aeroscout.com/viewItem.asp?type=press&itemId=23.

AIM (n.d.), *RFID Standards*, AIM website. www.aimglobal.org/standards/rfidstds/RFIDStandard.asp, accessed 8 June 2007.

AIM (2001), *Shrouds of time. The history of RFID,* AIM, Pittsburg. www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

AIM Frequency Forum (2000), *Draft paper on the Characteristics of RFID systems*, Version 1.0. www.aimglobal.org/technologies/rfid/resources/RFIDCharacteristics.pdf

Alberganti, Michel (2007), Actes Sud, Paris.

Albrecht, Katherine and McIntyre, Liz (2005), *Spychips*, Plume.

ANEC/BEUC (2007), *Joint ANEC/BEUC Comments on the Communication on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007) 96*, Bruxelles, www.anec.org/attachments/ANEC-ICT-2007-G-059.pdf.

Article 29 Working Party (2005), *Working Document on data protection issues related to RFID technologies*.

Article 29 Working Party (2007), *Opinion 4/2007 on the concept of personal data*.

Avoine, Gildas (n.d.), *RFID Security and Privacy*, website. http://lasecwww.epfl.ch/~gavoine/rfid/.

Australian Government, Department of Communications, Information Technologies and the Arts (2006), *Getting the most out of RFID. A starting Guide to Radio Frequency Identification for SMEs*, www.dcita.gov.au/__data/assets/pdf_file/41249/Getting_the_most_out_of_RFID.pdf

RFID Journal, July 2006, www.rfidjournal.com/article/articleview/2509/.

BMWi (German Federal Ministry of Economics and Technology) (2007), *European Policy Outlook RFID*, Berlin,

www.nextgenerationmedia.de/Nextgenerationmedia/Redaktion/en/PDF/Final_20ve
rsion_20European_20Policy_20Outlook_20RFID,property=pdf,bereich=nextgeneration
media,sprache=en,rwb=true.pdf

Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A. and Szydlo, M. (2006), *Security
Analysis of a Cryptographically-Enabled RFID Device* ˙ ¥ ª ˙ $ ® « œ¡ ¦ʰ Ÿ ¥ ª £ ¯ ˙ « ¢ ˙ °
) ¯ ¡ ª ¥ ´ ˙ ' ¡ œ± ® ¥ ° µ16.' µ © ¬ « ¯ ¥ ± ©   ˙ ¬ ˙
https://db.usenix.org/events/sec05/tech/bono.html.

BRIDGE (Building Radio Frequency Identification for the Global Environment)
(2007), *Security Analysis Report*, BRIDGE,
www.bridge-
project.eu/data/File/BRIDGE%20WP04%20Security%20Analysis%20Report.pd
f

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2005), *Security aspects
and Prospective Applications of RFID Systems,* BSI, Bonn,
www.bsi.bund.de/fachthem/rfid/RIKCHA_englisch_Layout.pdf

Cap Gemini (2005a), *RFID and Consumers. What European Consumers Think About
Radio Frequency Identification and the Implications for Business*, Cap Gemini,
Paris. www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf

Cap Gemini (2005b), *Consumer education is key to boosting awareness and
overcoming misconceptions about RFID*, Cap Gemini, Paris,
www.capgemini.com/news/2005/0209RFID.shtml

Cardullo, Mario,   fi¡ ª ¡ ¯ ¥ ¯ ˙ « ¢ ˙ ° ¤¡ ˙ *RFID Journal*,° ¥ ¨ ¡ ˙ & ⁄ Ł ˘ ˙ (š £
www.rfidjournal.com/article/articleview/392/1/2/.

Cavoukian, Ann (2004), *(š £   ˙ µ « ± ®¡ ˙ ¥ ° of Radio Frequency ˙ Ł © ¬ ¨ ¥ œš ° ¥ « ª
Identification (RFID) Technology*, Information and Privacy
Commissioner/Ontario, Toronto, www.ipc.on.ca/images/Resources/up-rfid.pdf.

Cavoukian, Ann (2006a), Privacy Guidelines for RFID Information Systems (RFID
Privacy Guidelines), Information and Privacy Commissioner/Ontario, Toronto,
www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf.

CDT (Center for Democracy and Technology) (2006), *CDT Working Group on RFID:
Privacy Best Practices for Deployment of RFID Technology*,
www.cdt.org/privacy/20060501rfid-best-practices.php

CIPL (Center for Information Policy Leadership) (2007), *RFID Transparency Symbol
Project*, Hunton & Williams,
www.hunton.com/files/tbl_s47Details/FileUpload265/1948/RFID_Two-
Pager.pdf.

¸ « ¨ ¨ ¥ ª ¯ ˙ ˙ Ʌ « ª š ° ¤š ˙   *RFID Journal*, ° ˙ š ª Ÿ ˙ ⁄ « ± ª Ÿ ˙ ¥ ª ˙
www.rfidjournal.com/article/articleview/921/1/1/.

Desmons, Dimitri (2006), *UHF Gen 2 for Item-Level Tagging*, Impinj Inc,
www.impinj.com/files/Impinj_ILT_RFID_World.pdf

DIFRwear website, www.difrwear.com, accessed on 11 July 2007.

˘ ® ¡ ¯ ¯ ¡ ª · ˘ Š ² ¥ Ÿ ·   · «*Atmel Applications* š ¥ « ª ¯ · ¢ « ® · & /
Journal, www.atmel.com/dyn/resources/Prod_documents/secrerf_3_04.pdf.

Dutch DPA (Data Protection Authority), R. Beugelsdijk, (2006) RFID, *Promising or Irresponsible? Contribution to the Social Debate about RFID*, Dutch DPA, The Hague, www.dutchdpa.nl/documenten/en_rap_2006_rfid.shtml

Engels, D.W. and Sarma, S.E. (2005), *Standardization requirements within the RFID class structure*, Auto-ID Labs, MIT, January 2005, Cambridge MA, USA. http://autoid.mit.edu/CS/files/11/download.aspx.

EPCglobal (2004a), *The EPCglobal network: Overview of Design, Benefits, & Security*, EPCglobal Inc., www.epcglobalinc.org/news/EPCglobal_Network_Overview_10072004.pdf.

EPCglobal (2004b), *EPCglobal Object Name Service (ONS) 1.0*, EPCglobal Inc., www.epcglobalinc.org/EPCglobal_ONS_1.0.pdf.

EPCglobal (2005a), *Submission to the Article 29 Working Party in Response to its Working Document 10107/05, WP 105 of 19 January 2005 on Data Protection issues related to RFID Technology*, EPCglobal Inc., http://ec.europa.eu/justice_home/fsj/privacy/docs/rfid/epcglobal_en.pdf.

EPCglobal (2005b), *The EPCglobal Architecture Framework*, EPCglobal Inc., www.epcglobalinc.org/standards/Final-epcglobal-arch-20050701.pdf.

EPCglobal (2005c), *EPC Radio-Frequency Identity Protocols Class 1 Generation 2UHF RFID. Protocol for communications at 860 Mhz -960 Mhz. Version 1.0.9*, EPCglobal Inc., www.epcglobalinc.org/standards/Class_1_Generation_2_UHF_Air_Interface_Prot ocol_Standard_Version_1.0.9.pdf.

EPCglobal (2005d), *Guidelines on EPC for Consumer Products*, EPCglobal Inc., www.epcglobalinc.org/public/ppsc_guide/.

EPCglobal (2007), *Position Paper on the Definition of Personal Data in the Context of RFID/EPC Technology Applications*, EPCglobal Inc.

EPIC (Electronic Privacy Information Center) (n.d.), *RFID Privacy Page*, www.epic.org/privacy/rfid/.

European Commission (2007a), *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions*, European Commission, COM(2007)96 final, Brussels. http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf.

European Commission (2007b), *The RFID Revolution: Your voice on the Challenges, Opportunities and Threats. Commission Staff Working Document. Results of the Public Online Consultation on Future Radio Frequency Identification Technology*

Policy, European Commission, SEC(2007)312,
http://ec.europa.eu/information_society/policy/rfid/doc/rfidswp_en.pdf.

European Commission (2007c), Communication from the Commission to the
European Parliament and the Council on the Follow-up of the Work Programme
for Better Implementation of the Data Protection Directive, COM(2007)97 final,
European Commission, Brussels.
http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_e
n.pdf

European Parliament (2007), *RFID and Identity Management in Everyday Life.
Striking the balance between convenience, choice and control*,
IPOL/A/STOA/2006-22, PE 383.219,
www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf.

Fabian B., Olivier, G. and Spiekermann, S (2005), *Security Analysis of the Object
Name Service (ONS) for RFID,* International Workshop on Security, Privacy and
Trust in Pervasive and Ubiquitous Computing, SecPerU'05, IEEE,
http://lasecwww.epfl.ch/~gavoine/download/papers/FabianGS-2005-
sptpuc.pdf.

Finkenzeller, Klaus (2003), *RFID Handbook: Fundamentals and Applications in
Contactless Smart Cards and Identification*, 2nd Edition, Wiley & Sons.

Finkenzeller, Klaus (2006), *Standardization of RFID*, RFID Handbook website,
www.rfid-handbook.de/rfid/standardization.html.

Flexilis (2006), *RFID E-Passport Vulnerability*, Flexilis,
www.flexilis.com/epassport.php

Floerkemeir, C., Schneider, R., Langheinrich, M. (2005), *Scanning with a purpose
Supporting Fair Information Principles in RFID Protocols.,* 2nd International
Symposium on Ubiquitous Computing Systems, UCS 2004, 8-9 November 2004,
Tokyo, Japan.

Garfinkel, Simson and Holtzman, H. (2005), *Understanding RFID Technology*, in
fi š ® ¢ ¥ ª § ¡ ¨ ʼ ' ¥ © ¯ « ª ˙ š ª Ÿ ˙ & « ¯ ¡ ª › ¡ ® £ ˙ ˝ ¡ ° ¤ ˙   & ⁄ Ł ˇ
Addison-Wesley Professional, Boston.

Gartner (2005), *Gartner Says Worldwide RFID Spending to Surpass $3 Billion in 2010*,
Gartner, Stamford, www.gartner.com/press_releases/asset_141469_11.html.

HP (Hewlett-Packard) (2006), *HP Unveils Revolutionary Wireless Chip that Links the
Digital and Physical Worlds*, HP,
www.hp.com/hpinfo/newsroom/press/2006/060717a.html.

Hitachi (2003), *Hitachi to Sell Inexpensive μ-Chip Inlets at Fraction of the Cost of
Existing Inlets, Open the Way to Use in Various Applications*, Hitachi press release,
www.hitachi.com/New/cnews/031204.html

Holland, Colin (2007), *Europe approves UWB regulations*, EETimes Europe,
http://eetimes.eu/showArticle.jhtml?articleID=197800214.

IDTechEx (2005), *Active RFID - A profitable business*, IDTechEx, www.idtechex.com/products/en/articles/00000396.asp

IDTechEx (2006a), *RFID Market $2.71Bn in 2006 to $12.35Bn in 2010 RFID Forecasts 2006 to 2016: The latest research from IDTechEx*, IDTechEx, www.idtechex.com/products/en/articles/00000409.asp.

IDTechEx and Das, Raghu (2006b), *Chipless RFID The End Game*, IDTechEx, www.idtechex.com/products/en/articles/00000435.asp.

ICC (International Chamber of Commerce), EICTA (European Information, Communications and Consumer Electronics Technology Industry Association), ICRT (International Communications Round Table) and JBCE (Japan Business Council in Europe) (2005), *European Commission DG Internal Market Art.29 Data Protection Working Party Working Document on data protection issues related to RFID technology WP 105/ Response by ICC, EICTA, ICRT and JBCE to the public consultation,* ICC, EICTA, ICRT and JBCE, http://ec.europa.eu/justice_home/fsj/privacy/docs/rfid/eicta_en.pdf.

ICAO (International Civil Aviation Organisation) (2004), *Annex I - Use of Contactless Integrated Circuits in Machine Readable Travel Document. Version 4.0*, ICAO, Montreal. http://mrtd.icao.int/component/option,com_remository/Itemid,32/func,fileinfo/id,2/

ITU (International Telecommunication Union) (2005), *The Internet of Things*, ITU, Geneva. http://mrtd.icao.int/component/option,com_remository/Itemid,32/func,fileinfo/id,2/.

Kanellos, Michael (2006), fl $ ¯ ˙ ! ¡ © « ® µ ˙ ' ¬ « ° ˙ ¬ ± °, CNET ¥ Ÿ ¡ «   ˙ š ± Ÿ ¥ « News.com, http://news.zdnet.com/2100-1040_22-6094586.html.

Krill, Paul (2006), *HP hails Memory Spot chips to extend content access*, Infoworld www.infoworld.com/article/06/07/17/HNmemoryspotpalo_1.html,

ł ± ¡ ¨ ¯ ˙ ˙ °   ˙ & ¥ ² ¡ ¯ ° ˙ & ˙ š ª Ÿ ˙ ' ¶ µ Ÿ ¨ « ˙ ! ˙ RFID Tags for Consumer Privacy , in V. Atluri, ed. 8th ACM *Conference on Computer and Communications Security*, pp. 103-111. ACM Press.

Juels, A. (2005a), *RFID Security and Privacy: A Research Survey*, RSA Laboratories, www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf

Juels, A. (2005b), *RFID Privacy: a technical primer for the non-technical reader*, RSA Laboratories, www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/rfid_privacy/DePaul23Feb05Draft.pdf.

Lace, Susan (2004), *Calling in the chips? Findings from the first summit exploring the future of RFID technology in retail*, National Consumer Council, London, www.ncc.org.uk/technology/calling_in_chips.pdf.

ž š ¤ ¥ ® ¥   ˙ ' š ª Ÿ ¥ ˚ ¬ ˙ (¡ œ ¤ ª « ˙ « ˙ £ *RFID Sourcebook*, IBM Press.

ž š ª £ ¤ ¡ ¥ ª ® ¥ œ ¤ ˙ ! š ® œ ˙ & / Ł ˘ ˙ š ª Ÿ ˙ $ ® ¥ ² š œ µ (Eds.), *Security, Privacy, and Trust in Modern Data Management*, Springer, Berlin Heidelberg New York, www.vs.inf.ethz.ch/publ/papers/langhein2006rfidprivacy.pdf.

Le Pallec, Sophie (2005), *La convergence des identifiants numériques,* CGEMP, Université Paris Dauphine, http://2005.jres.org/resume/70.pdf.

Leftnane News (2006), *Gone in 20 minutes: using laptops to steal cars*, Leftlane news, www.leftlanenews.com/2006/05/03/gone-in-20-minutes-using-laptops-to-steal-cars/

Lettice, John (2006), *Face and Fingerprints Swiped in Dutch Biometric Passport Crack*, The Register, www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/.

Malykhina, ı ¨ ¡ ª š ˙ ° œ ¥ ¥ ² ¸ ¨ & ž Ł ¡ ¨ ! ¡ ¡ ¡ ° ° ¨ (⊕ š œ § ¥ ª £ *InformationWeek*. www.informationweek.com/story/showArticle.jhtml?articleID=57701494.

Merritt, Rick (2006), *Cellphone could crack RFID tags, says cryptographer*, EEtimes online, www.eetimes.com/showArticle.jhtml?articleID=180201688.

Moore, Bert (2006), *RFID: A Plethora of Standards*, AIM, Warrendale, Pennsylvania. www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=1615&zoneid=43.

! « ˉ § « ³ ¥ ° ¶ ˙ $ ž š ± ® ¥ ˉ ˙ °-Enhancing Radio Frequency Identification Tag: Implementation of t¤ ¡ ˙ ¸ ¨ ¥ ¬ *RFID Journal Live*, www-03.ibm.com/solutions/businesssolutions/sensors/doc/content/bin/Clipped_Tag_White_Paper.pdf?g_type=hpfeat.

National Research Council, Committee on Radio Frequency Identification Technologies, (2004), *Radio Frequency Identification Technologies: a Workshop Summary*, National Research Council, Washington.

" ¡ ³ ¥ ° ¶ ˙ ° ª š ¨ ¡ ¡ ˙ š œ § ¥ ª £ ˙) ª (Ÿ ¥ ® £ & / « ± ˉª Ÿ fl *Wired*. www.wired.com/wired/archive/14.05/rfid.html

NIST (National Institute of Standards and Technology) (2007), *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, Special publication 800-98, NIST, Gaithersburg, http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

¸ « ª ª « ® ˙ ! š ® µ ˙ ¸ š ° ¤ ¡ ® ¥ ª ¡ ˙ *RFID* ı $ ¸ ˙ (š £ ˉ ˙ ' ± *Journal*, www.rfidjournal.com/article/articleview/2167/1/1/

¸ « ª ª « ® ˙ ! š ® µ ˙ ¸ š ° ¤ ¡ ® ¥ ª ¡ ˙ ˙ ˝ ± ¥ ¨ Ÿ ¥ ª £ ˙ ° Ÿ « ¬ ° *RFID Journal*, www.rfidjournal.com/article/articleview/2943/1/1/.

OECD (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris.

OECD (1999), *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce*, OECD, Paris.

OECD (2002), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris.

OECD (2003), *Privacy Online. OECD Guidance on Policy and Practice*, OECD, Paris.

OECD (2005), *Biometric Based Technologies*, OECD, Paris

OECD (2006a), *Radio Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations*, OECD, Paris.

OECD (2006b), *Making Privacy Notices Simple: an OECD Report and Recommendations*, OECD, Paris.

OECD (2006c), Foresight Forum *& š Ÿ ¥ « ˙ ⁄ ® ¡ – ± ¡ ª œµ ˙ Ł Ÿ ¡ ª ° ¥ ¢ ¥ œš ° ¥ « ª and $ ± › ¨ ¥ œ ˙ $ « ¨ ¥ œµ* Proceedings, OECD, Paris.

OECD (2007a), *Malicious Software(Malware): A Security Threat to the Internet Economy*, (forthcoming), OECD, Paris.

OECD (2007b), *RFID: Challenges and Benefits in Technology Implementation*, DSTI/ICCP/IE(2007)6/FINAL, OECD, Paris.

OECD (2007c), *RFID: Outline of Further Work*, secretariat working paper, OECD, Paris.

Oehlmann, H. (2006), ISO RFID application standards published in 2006, Odette.se, www.odette.se/files/seminariet%202006-04-11/Oehlmann.pdf.

Ohkubo M., Suzuki K., Kinoshita S., (2003), *¸ ® µ ¬ ° « £ ® š ¬ ¤ ¥ œ ˙ ° ¬ ¬ ® « š œ ¤ ˙ ° « ˙ ⁄ ® ¥ ¡ ª Ÿ ˙ ¸* Paper presented at the RFID Privacy Workshop at MIT 2003, www.rfidprivacy.us/2003/papers/ohkubo.pdf.

Oren, Y. and Shamir, A. (n.d.), *Power analysis of RFID ˙ - « ¯ ¯ ¥ ˙ # ® ¡ ª ¯ ˙ ³ ¡ › ¯ ¥ ° ¡* www.wisdom.weizmann.ac.il/~yossio/rfid/.

Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, Juan. and Arturo Ribagorda (2006), *RFID Systems : A Survey on Security Threats and Proposed Solutions*, http://lasecwww.epfl.ch/~gavoine/download/papers/PerisHER-2006-pwc.pdf.

Pradelles, Daniel, *RFID & Privacy. Perception of Reality?*, Presentation at the European Commission Consultation on RFID Workshop on 17 June 2006, www.rfidconsultation.eu/docs/ficheiros/Daniel_Pradelles.pdf.

QED Systems (2002), *Part 1: Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility*, QED Systems,

www.autoid.org/2002_Documents/sc31_wg4/docs_501-520/520_18000-7_WhitePaper.pdf.

Rees, Richard (2004), *ISO Supply chain RFID Standards*
http://portal.etsi.org/docbox/ERM/open/RFIDWorkshop/RFID_20%20Richard%20Rees_BSI.pdf.

Resolution of the 72nd German Data Protection Conference of the Federation and the Länder held in Naumburg from 26 to 27 October 2006 (2006), *Binding Rules for the Use of RFID Technologies*.

RFID Journal (n.d.), *Frequently asked question. The cost of RFID equipment*, *RFID Journal*, www.rfidjournal.com/faq/20/86, accessed on 23 May 2007.

RFID Journal (2003), *Military's RFID Alternative: IPv6*, *RFID Journal*, www.rfidjournal.com/article/articleprint/609/-1/1/.

with www.rfidvirus.org.

Simpson, Richard and St. Arnaud, Bill (2007), Position paper on *Economic Factors Shaping the Future of the Internet for the* hosted by the NSF and the OECD*.

Song, Jieun *et al* (2005), *Transactions*

Stapleton-Gray, Ross (n.d.), *RFID, Surveillance and Privacy: The Sorting Door Project*, Stapleton-Gray & Associates, Inc.

Swedberg, Claire (2006), *Chicago Fire Dept. Tests ZigBee-based RFID System, RFID Journal*, www.rfidjournal.com/article/articleview/2717/1/1/.

Taub, Howard and Genuth, Iddo (2006), *HP's Memory Spot Chip is Spot On*, The Future of Things website, www.tfot.info/content/view/79/59/.

US Department of Commerce (2005a), *RFID in 2005: Technology and Industry Perspectives Workshop Summary Wednesday 6 April 2005*, US Department of Commerce, Washington DC, www.technology.gov/Events/2005/RFID/0406_Summary.pdf.

US Department of Commerce (2005b), *Radio Frequency Identification. Opportunities and Challenges in Implementation*, Department of Commerce, Washington. www.technology.gov/reports/2005/RFID_April.pdf.

US Department of Homeland Security, Data Privacy & Integrity Advisory Committee (2006), *The Use of RFID for Human Identify Verification*, www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.

US FTC (Federal Trade commission) (2005), *Radio Frequency Identification: Applications and Implications for Consumers. A workshop report from the staff of*

the Federal Trade Commission, FTC, Washington,
www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

Vadhia, D. and Gupta, R. (2004), *IPv6 vs EPC,* Silicon Valley World Internet Center.
www.worldinternetcenter.com/Pubs/Pubs2004/feb05/IPv6vEPC.pdf

Ward, Matt and Kranenburg, Rob van (2006), *RFID: Frequency, standards, adoption
and innovation*, JISC Technology and Standards Watch, London.
www.jisc.ac.uk/uploaded_documents/TSW0602.pdf

Yomogita, Hiroki (2006), ⁄ š ¬ š ᵃ ¯ ˙) + ˝ ˙ ⁄ ¥ ᵃ š ¨ ¨ µ ˙ (š § ¡ ¯ ˙ « ¢ ¢ ˙ ³ ¥ ° ¤
Enabling Devices, Nikkei Electronics,
http://techon.nikkeibp.co.jp/english/NEWS_EN/20060803/119881/.

· ¡ ° ° ¡ ® ˙ Ž ¥ © ˙ -$ š ¯ ¯ ¬ ⁊ š œ . § ¡ ®¯ ˙ ¸ ¨ « ᵃ ¡ ˙ �incₑⅆ,
www.wired.com/news/technology/1,71521-0.html.

· ¡ ° ° ¡ ® ˙ Ž ¥ © ˙ -$ š ¯˙ ¯ ¬ « œ š°ᵃ ˙ š(ᵃ¤Ÿ¥ ¯ +˙ šfⁱ° ±œ¤ ˙ ¯ - ˙ « ⅼ ± ® ˙ ˙ ' µ ¯ ° ¡
Wired, www.wired.com/politics/security/news/2007/08/epassport.

RFID APPLICATIONS, IMPACTS AND COUNTRY INITIATIVES

FOREWORD

This report was presented to the Working Party on the Information Economy at its meeting in December 2007 as part of its work for the 2008 Seoul Ministerial on *The Future of the Internet Economy.* It was recommended to be made public by the Committee for Information, Computer and Communications Policy in March 2008.

The report was prepared by Verena Weber, consultant, in conjunction with Graham Vickery, OECD Secretariat, as part of work on the economic and social impacts of ICTs and new technologies. It is published under the responsibility of the Secretary-General of the OECD.

© OECD / OCDE 2008.

Table of contents

SUMMARY

Radio frequency identification (RFID) technology is currently one of the most promising and discussed auto-identification and data capture (AIDC) technologies. Although it is not a new technology, the range of applications is broadening rapidly and new applications which integrate other technologies such as sensors are developing. Eight major fields of application are analysed in this study, comprising: *i*) asset utilisation, where mobile assets are tagged for their use along the supply chain; *ii*) asset monitoring and maintenance, where mostly fixed and high value assets are tagged to store information, *e.g.* for maintenance purposes; *iii*) item flow control in processes, where RFID tags are attached to items which are moving along the supply chain; *iv*) inventory audit, for example in warehouses where pallets are tagged to improve the speed and efficiency of stock taking; *v*) theft control; *vi*) authentication to provide secure identification mechanisms for persons and objects; *vii*) payment systems to secure transactions; *viii*) automatic display of information where items are tagged to provide additional information on products and services when read.

It is difficult to quantify the impact of the technology, in part because most RFID applications are recent. Market analysis shows rapidly growing markets for RFID systems and, apart from very detailed mainly qualitative evaluations of particular applications, there are few aggregate impact studies. Available aggregate studies show large impacts in terms of benefit/cost ratios and productivity gains; however calculations are based largely on current good practice case studies, leading to a potential overestimation of aggregate benefits.

Country initiatives are divided into three main categories: *i)* the use of RFID by the public sector; *ii)* information, awareness and education programmes; and *iii)* incentives for business R&D and public funding of projects. The review of initiatives draws largely on replies to the *Information Technology Outlook 2008* policy questionnaire. This review suggests that government support for RFID technologies is focused on government applications for own use, often with a large demonstration component, and supporting multi-stakeholder projects to meet technological and industry needs, often to develop new technologies or applications. There are potentially large gains in innovation and efficiency from more widespread applications. Due to technological and business uncertainties education and awareness activities could be further emphasised, particularly for small businesses and more advanced applications where potential impacts are high, for example, those involving sensors.

Introduction

Radio frequency identification (RFID) technology is currently one of the most promising and discussed auto-identification and data capture (AIDC) technologies. It uses electromagnetic waves to transmit real-time data to identify specific objects (Garfinkel and Rosenberg 2005, p. xxvii). The technology is already in broad use in different fields of application such as toll collect systems, car keys and applications along the supply chain of companies.

There is high business and policy interest in this promising technology and the OECD has published a series of studies dedicated to RFID. The 2004 and 2006 editions of the *OECD Information Technology Outlook* as well as the Background ®¡¬«®°˙ ŠªŸˋ $®«œ¡¡Ÿ¥ª£¯ˋ ¢®«©ˋ°¤¡ˋ∕«®¡¯¥£¤°ˋ Ł Ÿ¡ª°¥¢¥œš°¥«ªˋ &∕Ł˘ˋˋ°¬¬¨¥œš°¥«ª¯ŠªŸˋ$±›¨¥œ 2005, give an introduction to the technology and its impacts. The Working Party on the Information Economy country study for Germany analyses in detail how œ«©¬Š¥¡¯±¯¡ª¡³¡®ˋ&∕Ł˘ˋŠ¬¬¨¥œš°¥«ªˋ Š¨«ª£ implementation in Germany: Challenges and B¡ª¡¢¥°¯ˋ°˙ˋˋ˘'(Ł Ł˛˛$ Łɪ Studies by the Working Party on Information Security and Privacy summarised in &šŸŸ¥«ˋ∕®¡‒±¡ªªªœµˋŁŸ¡ª°¥¢¥œš°¥«ªˋ&∕Ł˘ˋˋ°˙ˋ°∕ [DSTI/ICCP/REG(2007)9/FINAL] focus on trust-related challenges when deploying RFID systems.

Some of these studies briefly discuss possible roles of the public sector as well as touch on the economic impacts of the technology. As technological development has occurred at a rapid pace, estimates on the economic impact of the technology have varied and public sector projects have become more concrete. This document aims at addressing the following three questions:

What is the historical development of RFID technology and which fields of application in the public and private sector can be identified?

‹ What is the economic impact of RFID technology according to selected studies?

‹ What government RFID initiatives are there in OECD countries?

Section 3 on country initiatives is based in particular on 27 replies to the Information Technology Outlook Policy Questionnaire 2008.

1. Development and applications of RFID

The first part of this section summarises the historical development of RFID, the second part gives an overview of different RFID fields of application in the public and private sector.

1.1 Historical development of RFID

RFID is not a new technology despite rapidly growing interest in RFID ° ¡ œ¤ ª « ¨ « £ µ ˙ ¥ ª ˙ ®¡ œ¡ ª ° ˙ µ ¡ š ® ¯ ˙ (¤ ¡ ˙ œ« ª œ¡ ¬ ° ˙ « ¢ ˙ ° ¤ 1940s, following on from technological developments in the 1930s and the Ÿ ¡ ² ¡ ¨ « ¬ © ¡ ª ° ˙ « ¢ ˙ ®š Ÿ š ® ˙ Ÿ ± ®¥ ª £ ˙ + « ® ¨ Ÿ ˙ + š ® ˙ Ł Ł ˙ fl « 1950s, several technologies related to RFID technology were developed. One ¬ ® « © ¥ ª ¡ ª ° ˙ ¡ ´ š © ¬ ¨ ¡ ˙ ¥ ¯ ˙ ° ¤ ¡ ˙ ¥ Ÿ ¡ ª ° ¥ ¢ ¥ ¬ š ° ¥ « ª ˙ ¢ ® ¥ ¡ ª Ÿ ˙ « ® ˙ ¢ « ¡ ˙ ƃ ŋ ƃ ż aircraft which is a long-range transponder system. An active IFF system was first developed for British aircraft whereby each aircraft was equipped with a transponder. When radar stations emitted signals from the ground, the aircraft transmitted a signal back to identify itself as friendly (*RFID journal*, 2007).

The first commercial applications emerged in the 1960s and 1970s. The electronic article surveillance (EAS) equipment was developed by new companies such as Sensormatic and Checkpoints (Landt and Catlin, 2001) to prevent theft of goods at the point of sale. This system is currently in widespread use. With generally a 1-bit transponder, it is the most basic use. The data is sufficient to tell the reader whether a transponder is located in a certain area or not (Finkenzeller, 2006). Overall, this period was characterised by important further development of RFID technology. Research focused on applications for animal tracking, vehicle tracking, car keys, as well as process automation in production facilities (Landt and Catlin, 2001, *RFID Journal*, 2005).

Besides the development of these commercial applications, governments also began the development of RFID systems in the 1970s. For example, the US Department of Agriculture spurred the development of animal tracking and the US Department of Energy promoted the development of a system to track nuclear materials (*RFID Journal,* 2007) which was put in place in the mid-1980s.

Ł ª ° ¤ ¡ ˙ ˙ ¯ ¡ ˙ ˙ ° ¤ ¡ ˙ œ« © © ¡ ® œ¥ š ¨ ˙ ¡ ´ ¬ « ¥ ° š ° ¥ « ª initially › µ ˙ © š ¨ ¨ ˙ œ« © ¬ š ª ¥ ¯ ˙ fl « Ÿ £ ¡ ¯ ˙ š Ÿ ˙ ! œ∕ š ® ¨ š ¡ for the expansion of the technology was the development of the Personal Computer (PC) facilitating data management.

Whereas the exploitation of RFID was a common point in different countries, the interest in special fields of application diverged. The main interests in the US were for applications including access control of persons and transportation. European

countries were mainly interested in toll collection systems and industrial applications as well as short-range systems for the tracking of animals (Landt and Catlin, 2001). Overall, from a technological point of view, applications developed to this point were mainly operating at low-frequency and high frequency ranges.[1]

In the early 1990s, applications operating at ultra high frequency (UHF) emerged (*RFID journal*, 2007). These systems attained a higher read range and faster data transmission than systems operating at lower frequency ranges. The very first pilot projects started in the retail sector for the tracking of consumer goods along the supply chain. However, due to low volumes, these RFID systems were expensive (*RFID Journal*, 2007). A further obstacle to widespread use was that applications to this date were niche applications. As a consequence, a large number of proprietary systems were developed which were incompatible with each other (Landt and Catlin, 2001). The development of standards was thus crucial both for price decline and the use of RFID technology beyond niche applications.

Standardisation activities emerged in the late 1990s. The International Organisation for Standardisation (ISO) developed several standards in the field of RFID. One example is the ISO 18000 series which defines the air interface for different frequencies, *i.e.* how readers and tags of an RFID system communicate with each other. Furthermore, in 1999, the Auto-ID Center at the Massachusetts Institute of Technology was established with the aim of creating a seamless network with the (Auto-ID Labs, 2004). It was initially funded by the Uniform Code Council, European Article Numbering (EAN) International and industry. By the year 2003, the Center was supported by over 100 user companies, key RFID suppliers and the US Department of Defense and a federation of Auto-ID research institutes was created. Specifications developed by the Auto-ID Center focused on low cost tags for goods with the aim of tracking them along the supply chain. The results of the standardisation activities include two air interface specifications, the Electronic Product Code (EPC) numbering scheme as well as a network architecture (*RFID Journal*, 2007). These specifications were passed to EPCglobal for commercialisation purposes.[2]

Besides standardisation activities, the 1990s were furthermore characterised by an increased commercialisation of RFID systems. According to Landt and Catlin (2001), electronic toll collection systems were widely deployed both in the United States and Europe. For example, different regional toll agencies in the Northeast of the United States developed a regionally compatible toll system. Further important implementation projects included applications such as the tagging of over 3 million rail cars in the United States, access control applications (*e.g.* company badges and ski passes) as well as applications along the supply chains of companies. For example, in the late 1990s, European car manufacturers started RFID projects for asset tracking and tracking of parts along their internal supply chains. In addition, an RFID based immobiliser system for cars was commercialised in the mid-1990s which authenticate car keys and is in wide use. With the broader deployment of these applications, multiple use tags arose *e.g.* for toll collection, access control and gated community access (Landt and Catlin, 2001).

The beginning of the 21st century is marked by *i*) a growing interest of industry, government and the media in RFID technology, *ii*) further technical development, *iii*)

a first round of standards harmonisation, and *iv*) an increasing number of applications.

The impact of RFID is repeatedly discussed in mainstream media, and journals specifically devoted to RFID have been launched such as the *RFID Journal* in 2002. Technological development contributes to smaller tags, a reduction of costs and increased functionality. Concerning standardisation, a first harmonisation was implemented in 2006 when an ISO standard (ISO 18000-6) included the EPC Generation 2 UHF Air Interface Protocol and thus provided a broader technological basis for further RFID implementation in the field of passive, low cost RFID systems. There is a growing interest in RFID applications in different sectors, especially for applications along the supply chain. Important retailers such as Wal-Mart, Metro and Tesco conducted pilot projects and began to implement the technology in 2003 and 2004. Further sectors such as the aviation sector, the logistic sector and the pharmaceutical sector are also moving to wider implementation of RFID technology (*RFID Journal*, 2007). In addition, the public sector has important RFID implementation projects *e.g.* in the areas of defence, health, e-passports and identity cards. Overall, the range of different applications is broadening at a rapid pace and new applications which also integrate other technologies such as sensor technology are emerging. The following section provides an overview of different fields of application.

1.2   Overview of RFID applications

As discussed in the previous section, there is a large number of different RFID applications and the number is growing at a fast pace. To structure this range of applications, eight fields of application are described below.

‹   Asset utilisation:

‹   Mobile assets are tagged for their use along the supply chain. Typical examples are RFID tagged containers which are used at different production stages. Companies rely on RFID technology in order to locate these assets and to monitor which departments use the assets how many times. The aim is to optimise processes and attain a more efficient use of capacity.

‹   Asset monitoring and maintenance:

‹   Mostly fixed and high value assets are tagged to store information, e.g. for maintenance purposes. Examples include tagged machines where the maintenance history and information on replaced parts are stored on the tag. + ¤ ¡ ª ˙ Ÿ Š ° Š ˙ ¥ ¯ ˙ ¯ ° « ® ¡ Ÿ ˙ Ÿ ¥ ® ¡ œ ° ¨ µ ˙ « ª ˙ ° ¤ ¡ ˙ ° Š £ ˙ Š ª tags with high data capacity are needed.

‹   Item flow control in processes:

‹   For item flow control, RFID tags are attached to items which are moving along the supply chain. Often information going beyond a simple ID number is stored on the tag to control production processes. This is, for example, the case in the automotive industry where production information is stored on the tag which can be attached to car bodies or smaller parts. This mainly aims to avoid costly errors during the production process.

‹ Inventory audit:

‹ A prominent application is the use of RFID for inventory audit. Examples include retailer¯ ˙ ³ Š ® ¡ ¤ « ± ¯ ¡ ¯ ˙ ³ ¤ ¡ ® ¡ ˙ ¬ Š ¨ ¨ ¡ ° ¯ ˙ Š ª Ÿ ˙ ¯ « © to improve the speed and efficiency of stock taking. In most cases, only an ID number is stored on the tag to minimise the cost of the tag.

‹ Theft control:

‹ Item level RFID tags are used to prevent theft along the supply chain or at the point of sale. A simple form is electronic article surveillance (EAS) which can be RFID-based. In this case, low-end RFID systems (e.g. 1-bit tags) are used which communicate when consumers leave the shop if they have not been deactivated (Finkenzeller, 2006, pp. 25, 32). Applications for theft control in mail order for high-value products such as mobile phones use more sophisticated tags.

‹ Authentication:

‹ For authentication purposes, RFID is used to provide secure identification mechanisms for persons and objects. Prominent examples of personal authentication are company entry badges, transportation system cards, electronic passports and identity cards. Current fields of application for object authentication include the tagging of drugs in the pharmaceutical sector and high-value goods in the luxury sector to prevent counterfeiting.

‹ Payment systems:

‹ RFID technology is used for payment systems to secure transactions. Safety requirements for tags are very high. The systems are further characterised by very low read ranges to avoid mixing different payment cards.

‹ Automatic display of information:

‹ In the emerging field of automatic display of information, items are tagged to provide additional information on products and services when read. Early applications can be found at the point of sale or in the public sector, for example, in museums.

Table 1 shows the first seven fields of application and gives application examples for the private and the public sector. However, as new applications are developed on a daily basis, the list of examples is non-exhaustive. Further application examples organised by different industry sectors are listed in Table 2 where fields of application and industry sectors are cross-tabulated.

Table 10: Overview of RFID applications in the private and public sectors

	Application examples in the **Private sector**	Application examples in the **Public sector**
Asset utilisation	‹ Container management (*e.g.* small load carriers in the automotive sector) ‹ Loading equipment management (*e.g.* for gears in the automotive supplier sector) ‹ Management of dollies at airports ‹ Fleet management	‹ Waste management: Container management ‹ Health: Location of medical equipment at hospitals
Asset monitoring and maintenance	‹ Machine maintenance ‹ Tool box maintenance (*e.g.* for the maintenance of aircraft) ‹ Maintenance of parts built in aircraft ‹ Smart home applications	
Item flow control in processes	‹ Tagging of parts along the supply chain to correlate information on the tagged item to process steps ‹ Goods movement control ‹ Quality control of goods ‹ Tracing drugs in the pharmaceutical value chain ‹ Tracking finished goods for the purpose of diversion control	‹ Health: Tracking of medication from the pharmacy to the hospitalised patient ‹ Health: Tracing blood bottles ‹ Administration: Document management
Inventory audit	‹ Real-time location systems for finished vehicles in the automotive sector ‹ Automation of warehouse management ‹ Automated sorting and counting of inventory ‹ Checking of ingoing and outgoing goods ‹ Baggage handling at airports ‹ Livestock tagging	‹ Defence: Ammunition management ‹ Education: Lending system in libraries ‹ Exhibition in museums ‹ Science: Tagging animals and plants for research purposes
Theft control	‹ Car keys (immobilisers) ‹ Electronic Article Surveillance (EAS) systems ‹ Tracking products along the supply chain to minimise theft	
Authentication	‹ Persons: o Company badges o Ski passes o Event ticketing o Sports: recording time during a competition ‹ Objects (counterfeiting control): o Proof of authenticity of spare parts (*e.g.* in the aviation sector) o Proof of authenticity of drugs o Proof of authenticity of luxury goods	‹ E-Passports, identity cards ‹ Health: Patient authentication for the monitoring of medication in hospitals ‹ Leisure/sports: recording time during a competition ‹ Traffic: Tolling systems ‹ Traffic: Speed control ‹ Transport: Access control cards for public transport
Payment systems	‹ Tolling systems ‹ Contactless cards for financial transactions	‹ Transport: Payment cards for public transport

Source ˙ ˚ ± ° ¤ « ® ¯ ˙ œ« © ¬ ¥ ¨ š ° ¥ « ª

Table 11: Overview of RFID applications by sector [Note: Includes government applications]

	Asset utilisation	Asset monitoring and maintenance	Item flow control	Inventory audit	Authenti-cation	Theft control	Payment systems
Automotive	‹ Container management ‹ Loading equipment management ‹ Truck control	‹ Machine maintenance	‹ Tagging body parts on the assembly production line ‹ Tagging built-in parts	‹ Finished vehicles real-time location system		‹ Car keys combining automobile immobiliser systems and access control	
Automotive suppliers	‹ Container management ‹ Loading equipment management			‹ Finished products identification ‹ Automation of warehouse management			
Wholesale and retail trade			‹ Goods movement control from store warehouses to the sales area ‹ Freshness control of goods	‹ Goods receipt checking and database entry in the warehouse ‹ Automated sorting and counting of inventory ‹ Checking shipments of outgoing goods		‹ Checking deliveries (in trucks) for theft prevention ‹ Anti-theft systems at the point of sale (EAS)	‹ Contactless payment cards
Consumer goods			‹ Goods tracking along supply chain ‹ Freshness control	‹ Checking outgoing shipments			
Aviation	‹ Container management	‹ Tool box maintenance ‹ Aircraft main-tenance ‹ Tagging built-in parts to avoid errors (wiring harnesses)			‹ Proof of authenticity (*e.g.* for spare parts)		
Airports	‹ Management of dollies	‹ Maintenance of fire shutters	‹ Baggage handling	‹ Equipment check	‹ Border control (e-passport)		
Pharma-ceutical industry			‹ Tracing drugs		‹ Proof of authenticity of drugs		
Agriculture and forestry			‹ Tracing of goods (*e.g.* for freshness monitoring)	‹ Inventory audit in forestry and animal-ID			
Logistics	‹ Container management			‹ Checking of shipments			

	Asset utilisation	Asset monitoring and maintenance	Item flow control	Inventory audit	Authenti-cation	Theft control	Payment systems
Tourism and leisure			‹ Competition time recording (*e.g.* tags in shoes)		‹ Ski passes ‹ Event ticketing		
Financial sector							‹ Contactless payment cards
Luxury goods			‹ Tracking of finished products for diversion control		‹ Proof of authenticity of distri-buted goods	‹ Anti-theft systems at the point of sale ‹ Tracking products from distribution centre to shop to minimise theft	
Public sector Educational institutions				‹ Lending systems in libraries ‹ Exhibitions in museums			
Science				‹ Tagging animals and plants for research			
Public health	‹ Location of medical equipment and patient transport equipment		‹ Tracking medication from pharmacy to patient ‹ Tracing blood bottles		‹ Patient authentica-tion for monitoring medication in hospitals		
Waste				‹ Waste management			
Border control					‹ e-passport		‹ Tolling systems ‹ Public transport access and payment cards

Source ˙ ˚ ± ° ¤ « ® ¯ ˙ œ « © ¬ ¥ ¨ Š ° ¥ « ª

2.   Review of economic impacts

Most RFID applications are still recent and it is very difficult to quantify the impact of the technology. In the recent past, market analysts have published projections on the growing RFID market, and studies are becoming available evaluating the economic impact for specific applications. Section 2.1 compares predictions from different market analysts. Section 2.2 focuses on selected aggregate impact studies for different applications; it does not look at micro-level impact studies.

2.1   RFID market estimates

In terms of technology application, RFID implementation is still at an early stage. For this reason, it is difficult to obtain market projections and a challenging task to evaluate the RFID market. Table 3 provides an overview of global market ¬ ® « ¦ ¡ œ° ¥ « ª ¯ ˙ › µ ˙ Ÿ ¥ ¢ ¢ ¡ ®¡ ª ° ˙ © š ® § ¡ ° ˙ š ª š ¨ µ ¯ ° ¯ ˙ + ¤ market ˙ ¬ ® « ¦ ¡ œ° ¥ « ª ¯ ˙ ± ¯ ± š ¨ ¨ µ *i.e.* readers, tags, RFID ¡ ˙ & ⁄ Ł ˙ ˙ middleware). Only the study by IDTechEx analysts includes services.

Table 12: Estimates of the RFID global market (USD)

Market analyst	Date of release	2005	2006	2007	2010/ 2011	2015	2017
Gartner	2005	504 million	2.7 billion		3 billion (2010)		
RNCOS	2005	1.9 billion				26.9 billion	
BCC Research	2006	649 million	713.4 million		1.05 billion (2011)		
IDTechEx (Study includes systems and services)	2007			4.96 billion			27.88 billion

Source ˙ ˚ ± ° ¤ « ®¯ ˙ œ« © ¬ ¥ ¨ š ° ¥ « ª

Overall, large differences between market estimates are observed. For example, whereas the market for RFID systems for 2006 was estimated at USD 2.7 billion by Gartner analysts, BCC estimated an RFID market of only USD 713.4 million in the same year.

There are various reasons for these large differences. Two important reasons are the early stage of RFID implementation in both public and private sectors and, as a result, divergent evaluations of the technology in terms of both coverage and

evolution. According to the European e-Business Watch large-scale survey of RFID adoption strategies and impacts in four broad economic sectors,[3] 14% of the European companies interviewed were piloting, using or implementing RFID technology in 2007.[4]

Companies that were using RFID or planning to use RFID expected major effects on: *i*) inventory management (49% of companies using or planning to use RFID), *ii*) control and efficiency of inbound logistics (46%), and *iii*) merchandise management and reduced out-of-stocks (44%). These results correspond to those found in the WPIE qualitative country study for Germany [DSTI/ICCP/IE(2007)6/FINAL]. The major costs for those using or planning to use the technology were seen to be the costs of project implementation and system integration (39% of all companies using or planning to use RFID). Interestingly, for those companies *not* using or planning to use RFID technology, 64% stated that a relevant reason for not using it was the insufficient evidence of a strong return on investment (ROI).[5] To further examine this issue at a more aggregated level, the next section focuses on selected quantitative impact studies.

2.2   Selected studies on the aggregate economic impact of RFID

Whereas section 2.1 deals with market estimates at aggregate level, this section aims at assessing the impact of RFID at a more detailed aggregate level from a user perspective. Apart from studies of toll applications and access control, to date there are very few studies assessing the economic impact of RFID technology in business applications. Of these studies, the majority assess RFID benefits at a qualitative rather than a quantitative level resulting in an even lower number. Of the quantitative studies, we chose two selected impact studies which are based on a well-defined methodology and which outline their assumptions and calculations. The first study deals with global financial impacts in the retail and healthcare sectors. The second study assesses the financial impact of RFID technology at cross-sectoral level in one OECD country.

Ł ª ˙ ° ¤ ¡ ¥ ®˙   ˙ ¯ ° ± Ÿ µ ˙ ˝ š ® ± š   ˙ ! š ª ¥ ˙ š ª Ÿ ˙ + ¤ ¥ ª ¯ ° « ª RFID technology in the retail and the healthcare sectors   ˙ fl ¡ š ¯ ° ¤ ˙ œš ® ¡ ˙ ¯ ¡ œ° « ® ˙ pharmaceutical companies, healthcare distributors and hospitals. They analyse both reduction of costs and the increase of revenues by relying on RFID technology. Calculations are made based on different sources such as case studies of RFID pilot and implementation projects, documents of government and industry associations as well as synthesised results from prior studies. Overall, according to Barua, Mani and Whinston, benefits have already amounted to a global cumulated USD 40 billion in the retail and healthcare sectors.

Out of these estimated USD 40 billion, the retail sector has cumulated benefits of USD 12.05 billion from RFID applications. Total cumulated spending on RFID systems from 2003 to 2006 amounted to USD 2.37 billion according to the authors, resulting in a ROI of about 500%.

This results from both the reduction of costs and increased revenues. On the cost reduction side, economies result from the reduction of labour costs, reduced losses Ÿ ± ® ¥ ª £ ˙ ¬ ® « Ÿ ± œ° ¥ « ª ˙ š ª Ÿ ˙ ¯ ¤ ¥ ¬ ©¡ ª reduced inventory ®¥ ª § š £ ¡ write-offs and non-working inventory. On the revenue side, benefits result from

increased product availability at the point of sale, a faster time to market and ¬ ® « ² ¥ Ÿ ¥ ª £ ˙ ± › ¥ − ± ¥ ° « ± ¯ ˙ š œ œ¡ ¯ ¯ ˙ ˙ ° « Barua, Mani © ¡ ® ¯ ˙ š œ ® and Whinston, 2006). Based on expected adoption rates of pallet tagging (45%) and item-level tagging (25%) in 2011, the authors estimate that benefits will reach USD 68.55 billion in 2011.

Total cumulated benefits in the healthcare sectors have been estimated at USD 27.95 billion. Investments in RFID systems have been USD 2.03 billion, leading to a significantly higher ROI (over 1 300%) compared to the retail sector. According to the authors, this is due to higher RFID adoption rates for the health sectors than for the retail sector.

$ ¤ š ® © š œ¡ ± ° ¥ œš ¨ ˙ œ « © ¬ š ª ¥ ¡ ¯ ˙ ¤ š ²*i*)¡a reduction in¥ ¯ ¡ Ÿ ˙ ° ¤¡ ¯ ¡ counterfeit, shrinkage and parallel trade, *ii*) efficient product recall, *iii*) efficient sample management, *iv*) enhanced inventory turns, and also shorter clinical trial cycles and faster time-to-© š ® § (Barua, Mani and Whinston, 2006). For healthcare distributors, the authors attribute the benefits to enhanced inventory turns on the one hand and a reduction in labour costs at distribution centres on the other hand. Finally, by relying on RFID technology, hospitals have benefited from *i*) better asset utilisation, *ii*) higher inventory turns, *iii*) increased healthcare access and *iv*) higher patient safety because of fewer errors.

Overall, the report by Barua, Mani and Whinston is one of the first to discuss in detail how RFID benefits can be quantified. This is not an easy task as RFID implementation in these sectors has only taken place recently and the authors admit ° ¤ š ° ˙ ¥ ° ˙ ¥ ¯ ˙ ª « °° ¤ ¡ ¡ ˙ š œ¶ š ¨ ˙ ° « ¡ ˙ ª £ ‡ š ª ° ¢ ¥ ¢ µ ˙ š ˙ ¯ ± œ œ¡ ¯ ¯ ¢ ± Furthermore, benefits are quantified in a rather optimistic way. Calculations are based on current case studies which are in general best practice examples and success stories of leading companies in these sectors. As a consequence, the results of successful projects have been taken to estimate economies and increased sales in a whole sector which may over-state total benefits across firms which are less efficient in implementation.

The study &⁄ Ł ˘ ˙ ¯ $ ˙® ¢ « ® ¡ ˆ ¡ in 2007 focuses on a cross-sectoral analysis of RFID in Germany. Within this analysis, one part is dedicated to sales and productivity effects of RFID technology. Sectors assessed in the study include the consumer goods, retail, logistics and the automotive sector. Macroeconomic effects in Germany in 2010 are derived from sales and productivity effects of each of these sectors. Calculations for all sectors are based on sources such as preliminary case studies of RFID pilot and implementation projects. Overall, according to the study, sales and productivity gains amounted to EUR 3.24 billion in 2004 and are expected to rise to EUR 62.2 billion in 2010.

In **German retailing**, productivity effects are estimated at EUR 8.6 billion in 2010. Estimates are based on total retail sales and the estimation that companies having implemented RFID technology by 2010 will account for 40% of total retail sales. Moreover, the percentage of sales influenced by RFID is estimated at 30% and operational productivity effects (productivity gains from avoiding out-of-stock situations, less shrinkage, etc.) are estimated at 20%. Estimates on productivity gains are based on preliminary studies such as documentation of the Metro future store.

The model calculations for the **German logistics sector** differentiate between logistics and transport services only and auxiliary services in logistics (*e.g.* inventory management, order processing, logistics planning). In the logistics and transport services productivity effects will reach EUR 1.7 billion in 2010 according to the study. In the field of auxiliary services in logistics, RFID use will yield about EUR 4.3 billion in 2010.

Productivity gains in the **German automotive sector** are estimated at EUR 2.4 billion in 2010. Interestingly, these estimates are significantly lower than the estimated gains in the retail sector. This is explained by the estimates of the operational productivity effects directly attributable to adoption of RFID. In the automotive sector, the authors estimate these effects very conservatively at 2% by 2010. In the retail sector, however, these gains are estimated at 20%.

These sector analyses are the starting point for the macroeconomic assessments of RFID technology on the German economy. The calculation is based on the gross value added (*i.e.* the total value of goods generated in the production process minus inputs consumed during production). Industry subcategories were selected which will be influenced by RFID technology in the medium term. Table 4 shows that productivity gains triggered by the use of RFID will increase from EUR 3.24 billion in 2004 to EUR 62.2 billion in 2010.

² ¡ ® š ¨ ¨ ˙ ° ¤ ¡ ˙ ¯ ° ± Ÿ µ ˙ &⁄Ł ˇ ˙ $ ® « ¯ ¬ ¡ œ° ¯ ˙ ¢ « ® ˙ fi ¡ ® © analyses how productivity gains can be calculated for different industry sectors and how they can be aggregated to obtain gains at macroeconomic level. This is a demanding task as RFID implementation has only recently taken place. Furthermore, the authors estimate potential gains in a structured and logical way. However, in their penultimate step, the authors calculate the gains based on a ¬ ¡ ® œ¡ ª ° š £ ¡ ˙ « ¢ ˙ ° ¤ ¡ ˙ ° « ° š ¨ ˙ « ± ° ¬ ± ° ˙ ¥ ª ¢ ¨ ± ¡ ª œ¡ Ÿ ˙ percentage of total (production) cost reduction. As a consequence, estimated gains are high. In addition, as in the report by Barua, Mani and Whinston, calculations are based on current case studies which in general tend to be success stories. This may be another factor leading to a potential overestimation of total benefits.

Table 13.Model calculation: portion of value added due to RFID technology

	Year	Manufacture of transport equipment	Manufacture of textiles and textile products	Manufacture of chemicals and chemical products	Manufacture of machinery and equipment	Commercial agents/wholesaling	Retailing (except motor vehicles)	Transport, storage and communication	Health and social work	TOTAL
Gross value added (EUR, billions)	2004	73.1	37.4	45.6	67.2	89.5	84.0	116.4	141.2	654.4
	2010	71.4	34.4	55.4	85.5	133.5	88.1	148.1	148.1	764.5
Percentage of RFID pioneers	2004	10%	5%	5%	2%	10%	10%	7%	1%	--
	2010	40%	20%	15%	15%	40%	40%	25%	15%	--
&⁄Ł˘˙¬¥« value added (EUR, billions)	2004	7.3	1.9	2.3	1.3	9.0	8.4	8.2	1.4	39.8
	2010	28.6	6.9	8.3	12.8	53.4	35.3	37.0	22.2	204.5
Percentage of output ¥ª₵¨±¡ª RFID	2004	10%	5%	10%	2%	10%	10%	5%	1%	--
	2010	35%	30%	20%	20%	30%	30%	40%	20%	--
Portion of value added ¥ª₵¨±¡ª RFID (EUR billion)	2004	0.7	0.1	0.2	0.03	0.9	0.9	0.4	0.01	**3.24**
	2010	10.0	2.1	1.7	2.6	16.0	10.6	14.8	4.4	**62.2**

Source: OECD based on BMWi (2007).

3. Review of country initiatives

Country initiatives are divided into three main categories: *i)* the use of RFID by the public sector (section 3.1.), *ii)* information, awareness and education programmes (section 3.2), and *iii)* incentives for business R&D and public funding of projects (section 3.3). This categorisation is developed on the basis of literature review and the RFID country study in Germany.

3.1 The use of RFID by the public sector

The public sector is an important user of RFID technology in addition to rapidly increasing use of RFID in the private sector. Examples which are contributing to widespread use of the technology include using RFID technology in electronic passports (e-passports), and for tracking assets and items in the area of defence and equipment of hospitals.

Seven main application areas in the public sector are listed below:

‹ **E-passports and identity credentials**
E-passports combine the traditional paper document with an RFID tag where the critical information is stored. The RFID tag often contains biometric data such as data for facial recognition and fingerprints. The format of the biometric data and communication protocols is defined in a standard adopted by the International Civil Aviation Organization to ensure international inter-operability. The RFID tag runs on the standardised ISO/IEC 14443 communication protocol (Finkenzeller, 2006, p. 404). RFID technologies are also planned for national identity credentials or other official documents such as driving licences, residence permits, social security cards, etc.

‹ **Public services (***e.g.* **waste management/waste control)**
Public services include services such as the management of parking facilities and waste management. In waste management RFID is used for two main purposes: for tracking (hazardous) waste to protect the environment and to allocate costs according to the amount of waste. Currently applications can, for example be found in Korea where pilot projects in the field of hazardous waste tracking were conducted as well as in Germany where costs of waste are œš ¨ œ± ¨ š ° ¡ Ÿ ˙ š œœ« ® Ÿ ¥ ª £ ˙ ° « ˙ ° ¤ ¡ ˙ 3 š ¯ ° ¡ ¯ ˙ 2 « ¨ ± © ¡ ˙

‹ **Health (***e.g.* **applications in hospitals)**
A significant number of public sector RFID projects are implemented in healthcare. One area where multiple projects are already at the implementation stage is the hospital sector. RFID is used to track assets such as beds or containers, to identify patients for medication control and to track babies and dementia patients to increase their security. Other applications include health insurance cards which have already been introduced in Mexico, for example. Information such as username and prescribed drugs are stored on the embedded RFID chip.

‹ **Document administration/postal services**
The public sector also uses RFID technology for the administration of documents. In this field, RFID tags are attached to documents to improve the location of documents and thus to increase process efficiency and quality. RFID is also used for postal services in distribution centres to facilitate the sorting of mail items.

‹ **Defence**
RFID technology in the area of defence is mainly used to streamline supply-chains and procurement processes. The most prominent example of a department relying intensively on RFID technology is the US Department of Defense. Both active and passive tags are attached to inbound and outgoing shipments at the case and pallet level.

‹ **Education/Cultural institutions/Science**
The public sector also relies on RFID at its cultural institutions. Examples include lending systems at libraries and newer applications can be found in museums where artworks are presented via RFID technology via automatic display of information.

‹ **Logistics/Transport (***e.g.* **toll collect systems)**
Finally, RFID is used by the public sector in the fields of logistics and public transports. Toll collect systems were early applications of RFID technology. Newer applications are access cards for public transport, RFID-based bus schedules as well as particular location-based services.

Table 5 gives a non-exhaustive overview of RFID applications used by OECD countries indicating that applications are very diverse. Many projects in the fields of e-passports, health, transport and defence are already at the implementation stage. Newer applications can be mainly found in the fields of public services and education.

Overall, governments are currently developing and using RFID in a variety of different areas. To be an important user of RFID technology has a number of important effects both for further RFID suppliers and users. On the supply side, government projects can have significant effects. Pilot projects contribute to further development and testing of different components of RFID systems, and are seen as an important means to spur innovation. Moreover, important implementation projects support the formation of an RFID market at national and international level. These effects on the supplier side enhance a more reliable and sophisticated supply of different components of RFID systems.

On the user side, pilot projects conducted by governments provide pilot experiences for new RFID applications. Both the public and the private sector profit from technology feasibility studies and testing results. A further characteristic of government projects is their ability to generate valuable experience and robust results « ª ˙ š ˙ ¨ š ® £ ¡ ˙ ¯ œš ¨ ¡ ˙ ˙ ⁄ ± ® ° ¤ ¡ ® © « ® ¡ ˙ © š ª µ ˙ « ¢ ˙ ° ¤ ¡ ˙ £ « wider applications.

Government projects are usually designed to disseminate results widely. A wide range of stakeholders involved in RFID technology benefit from these projects and results are usually made broadly available. If this process is organised in a highly efficient way, spill-over benefits of public sector RFID projects can be considerable.

Table 14: Selected RFID applications in the public sector in OECD countries

Country	Project category	Project description
Austria	Health	Tests by the municipal administration of Vienna on the applicability of RFID in the health care system
	Public services	Tests in the Viennese parking facility management
Denmark	Education	Lending systems in libraries
	E-passport	E-passport available since mid-2006; biometric passport relying on RFID embedded fingerprint technology to be introduced mid-2009
Germany	E-passport	E-passport (available since the end of 2005), electronic ID card (to be introduced at the end of 2009)
	Public services	Waste management in different communities
	Education	Lending systems in libraries
Japan	Logistics/Transport	Set-± ¬ ˙ « ¢ ˙ ° ¤ ¡ ˙ ⁄ ® ¡ ¡ ˙ ! « › ¥ ¨ ˙ based on ubiquitous network technology including RFID tags, to provide information for seamless movement (*e.g.* transfer routes and transport modes)
Korea	Public services, health, defence, logistics/transport	Pilot projects in the fields of procurement, baggage handling, container management, ammunition management, tracking hazardous waste, museums, air cargo, etc.
Mexico	Health	Health insurance card: RFID technology ¥ ˉ ˙ ¥ ª ° ¡ £ ® š ° ¡ Ÿ ˙ ¥ ª insurance" card where the username, information on doctors as well as prescribed drugs are stored
Netherlands	E-passport	E-passport
	Health	RFID technology used in hospitals
	Education	Libraries
	Logistics/Transport	Payment cards for public transport
Portugal	E-passport	E-passport and e-passport control systems at Portuguese airports (*e.g.* Lisbon, Faro)
Spain	Document administration/ postal services	The Spanish postal service uses RFID technology in 15 distribution centres in different locations in Spain (*e.g.* Madrid, Barcelona)
United Kingdom	E-passport	Biometric passport relying on RFID technology
United States	Defence	Use of passive and active RFID tags for inbound and outgoing shipments along the supply chain
Singapore	Logistics/Transport	Nationwide Electronic Road Pricing (ERP) system to control and manage traffic volume; payment of road usage charges. The ERP is applied to all of ˙ ¥ ª £ š ¬ « ®00 vehicles
	Public services	RFID tags replace paper season parking tickets at car parks in public housing estates
	Education	Lending systems in all national and community libraries

Source: Compiled from replies to the IT Outlook Policy Questionnaire 2008 and case studies.

3.2   Information, awareness and education activities

Apart from being a user of RFID technology, another important role for the public sector is in providing and sharing information and in the education of stakeholders. Information and education activities include for example:

‹   Conferences on RFID technology and its impacts.

‹   Discussion forums and online dialogue platforms.

‹   Information (*e.g.* studies providing an introduction to RFID, its benefits and barriers and assessing current and future RFID markets).

‹   Publication of guidelines (*e.g.* how the private sector could assure data protection).

‹   Demonstration projects.

Table 6 illustrates different information, education and awareness activities in OECD countries. Activities in this category primarily focus on the publication of studies and demonstration projects. Most of the studies are either directed at consumers or companies. In the first case, studies are published aiming at increasing public awareness. One of the challenges of studies directed at consumers is a balanced presentation of potential benefits and potential risks as potential risks vary greatly according to specific RFID applications. Another major challenge is to distinguish between applications which do not have an impact on consumers and users and where privacy is not an issue (*e.g.* supply chain applications), and applications which directly concern consumers and where privacy is an issue. In the first case, studies provide an introduction to RFID technology and information on fields of application and benefits and challenges in technology implementation.

A significant number of these studies focus on small and medium-sized enterprises (SMEs). These companies often face important transaction costs, especially in the case of new RFID applications where few off-the-shelf solutions exist and where different technology providers supply different parts of the RFID system. Further, SMEs often lack the necessary R&D budget, economic capacity and time to take large risks with new technologies. As SMEs are potentially important users of RFID systems, information and awareness on prospective applications as well as showcases are important for diffusion of RFID technology and reducing unnecessary risk. Publications on best practices can further facilitate RFID diffusion among SMEs.

Some OECD countries (*e.g.* Finland and Korea) have provided showcases and demonstration projects which include demonstrations in application centres and implemented projects, for example in the field of baggage handling.

Overall, as RFID implementation projects are still at an early stage, lack of knowledge potentially hampers further development and implementation. Governments are experienced in raising awareness of and disseminating information on new ICT technologies and fields of application, often in collaboration with other stakeholders, and can help devise collaborative mechanisms to improve diffusion and uptake in generic technologies. Projects are usually characterised by being developed in close collaboration with other stakeholder groups including industry groups and academics and they try to give a comprehensive overview of the technology. In fi ¡ ® © š ª µ ˙ ¢ « ® ˙ ¡ ´ š © ¬ ¨ ¡ Security Aspects and Prospective & ⁄ Ł ˇ ˙

thus helping German companies to reduce transaction costs by reducing the time spent searching for information on RFID technology. Further activities aiming at discussing different facets of RFID implementation and the broad dissemination of these activities could contribute to better understanding of RFID technology and applications and thus foster its broader acceptance and diffusion.

Table 15: Selected RFID information and education activities in OECD countries

Country	Project category	Project description
Australia	Information (guide)	starting guide to radio identification for SMEs[6]
	Information (event)	build awareness of opportunities and challenges presented by RFID technology
Canada	Information (study)	update discussing RFID technology, pilots and deployment in Canada, consumer concerns and policy developments[7]
Denmark	Information (study)	study, published by the Independent Technology Council[8]
Finland	Demonstration projects (application centre)	Partly publicly funded RFID application centre providing information and piloting facilities[9]
Germany	Conference	organised by the Federal Ministry of Economics and Technology[10]
	Discussion forums	activities and initiatives both administrated by the government and industry
		trust
	Information (online portal)	Commerce Ne... part on RFID technology including studies and checklists
	Information (studies)	A number of studies issued by the government such as eine Chance für kleine und mittlere Unternehmen (RFID guide an opportunity for small and medium-... Security Aspects and [11][12]
Italy	Information (study)	is working on a study evaluating the use of RFID in public administration[13]
Japan	Guidelines	technological changes and usage in order to improve dissemination conditions of RFID
Korea	Information (studies, guidelines)	RFID technology feasibility studies, guides for companies based on conducted pilot projects (see Part 3.1)
Netherlands	Information	...information on RFID directed at SMEs via generic ICT awareness and educational programmes

Country	Project category	Project description
Switzerland	Discussion forum	Risk dialogue foundation[14] (dialogue between stakeholders from industry, science, public sector, consumer protection, data security amongst others)
	Information (study)	(¤ ¡ ´ ¬ ® ¡ œš ± ° ¥ « ª Š ® µ ´ ¬ ® ¥ ª œ¥ ¬ ¨
European Commission	Information (communication)	Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and (¤ ¡ ´ ¸ « © © ¥ ° ° ¡ ¡ ´ « ¢ ´ ° ¤ ¡ Frequency Identification (RFID) in Europe - steps towards a ¬ « ¨ ¥ œµ ´ ¢ ®š © ¡ ³ « ® §
Singapore	Information (knowledge base)	Creation of a knowledge base by the National RFID Centre to shorten learning curves and deployment times across industries
	Discussion forum	Creation of an RFID focus interest group with linkages to a network of local and overseas RFID labs by the National RFID Centre
	Demonstration projects	Demonstration of novel RFID technologies and solutions at the National RFID Centre

Source: Compiled from replies to the IT Outlook Policy Questionnaire 2008 and case studies.

3.3   Incentives for business R&D and public sector project funding

Public sector project funding (either wholly or in part) is a third category of country initiatives . They include *i)* projects funded and conducted by the public sector for business sector applications, *ii)* funding of mostly collaborative projects between business, research and public groups, and *iii)* funding projects conducted by the private sector. Some of these funding schemes are specifically focused on RFID, in other cases R&D and new applications as well as the development of standards are funded via general national technology development and support funding mechanisms.[17] It should be further noted that RFID R&D and investment can benefit from general R&D tax incentives and investment incentives, but that there are no reported RFID-specific R&D or other tax incentives for their development in OECD countries.

Table 7 provides an overview of funding projects in selected OECD countries. Further projects with important funding volumes are conducted by the European Commission within the 6th framework programme (see Box 1). Overall, projects range from RFID projects in specific fields of application, the funding of selected projects between different stakeholder groups, to a wide range of tax expenditures via general tax incentives.

Table 16: Selected RFID funding projects in OECD countries

Country	Project	Description	Stakeholders
Australia	National EPC Demonstrator Project (2006/2007)	Funding two phases of the National EPC Demonstrator Project: RFID in (open circulation) supply chains; interoperability and integration requirements	Government and industry
Austria	FIT-IT Programme line ¡ ©› ¡ Ÿ Ÿ ¡ Ÿ ‾ µ ‾ ° ¡ ©‾	Ministry for Transport, Innovation and Technology. RFID projects funded in the ¬ ® « £ ® š © © ¡ ˙ ¡ ©› ¡ Ÿ Ÿ ¡ Ÿ	Government, industry, academics. Funding cooperative industry/academic research projects
	Competition: Development and Application of RFID Technology	\$ ® « ¦ ¡ œ° ˙³ ¥ ° ¤ ¥ ª ˙ ° ¤ ¡ ¦ œ« ª « © µ Ł ¸ (˙ ⁄ ± ª Ÿ ¥ projects. Total funding volume provided by the Federal Ministry of Economics and Labour: EUR 400 000	Government, industry and academics
	\$ & # ˙ ¸ (˙ initiative	Joint private-public initiative by the university of Graz and NXP (former Philips Semiconductors) for RFID R&D	Public sector and industry
Canada	McMaster RFID Applications Lab (MRAL)	Creation of an RFID lab at McMaster University in joint public-private initiative. Hub for RFID applications promoting RFID research, social and economic impact and policy issues	Industry and public sector
Denmark	Train travel card	Test of RFID technology based e-ticket by major Danish train operator	Government and industry
	BroBizz (Bridge toll)	Use of RFID technology for commuters for the toll system on the bridge between Denmark and Sweden, as well as toll on bridges in Denmark	Government
	Mail delivery and registration	Implementation of smart phones to combine road planning, RFID scans, payment and postal registration by the major Danish mail operator in 2007	Government and industry
Finland	GIGA[18]- Converging networks	TEKES (main government body for funding R&D programmes). Programme focus areas: wireless access (including RFID), seamless networking, network support, telecommunication business	The programme is a combination of research and industrial projects
Germany	-	Targeted support of projects developing pioneering RFID activities and producing show-cases	Government and industry
Korea	Airline Baggage Tracking and Control System	RFID tags attached to baggage of domestic flight passengers and RFID readers deployed in destination airports to secure baggage traceability	Jeju, Busan, Daegu, Gwangju and Chungju airports
Mexico	PROSOFT[19] fund	Programme for development of the software industry (PROSOFT), supports RFID-related projects. About one third of funding from the Ministry of the Economy	Government, industry and academics
Spain	Interference tests	Interference tests in several Spanish towns (*e.g.* Madrid) to test the compatibility of RFID with radio links	Government
Turkey	RFID Research and Test Centre	Established by Istanbul Technical University. Research projects RFID use, especially logistics and manufacturing	Public sector and industry

Country	Project	Description	Stakeholders
Singapore	National RFID Centre (September 2006)	Funding RFID industry pilot projects	Government and industry
		Training for potential solutions for companies and end users	Government and industry

Source: Compiled from replies to the IT Outlook Policy Questionnaire 2008 and case studies.

Government support promotes RFID technology on both supplier and user sides. The funding of projects with a wider scope (*e.g.* the Finnish GIGA project) has the particular advantage that these projects have the potential to trigger wider and future applications. Finally, funding of long-term projects allows development and testing of more future-oriented applications such as applications combining RFID technology with other promising technologies (*e.g.* sensor technology). At all funding stages, collaboration with different stakeholders and intense information exchange are crucial and help to maximise benefits.

Besides the projects described above, the public sector may also need to address environmental and recycling issues related to RFID technology. The technology can very effectively track, minimise and assist efficient waste and pollutant disposal. But in addition, environmental impacts associated with the technology itself will need to be addressed. As the number of RFID tags continues to rise, they will have to be separated from other materials during recycling processes. Government support could encourage research on the impact of RFID technology on the environment and especially on recycling issues.

Box 2: Selected RFID funding projects in the 6th Framework Programme

BRIDGE (Building Radio frequency IDentification solutions for the Global Environment):

o Three year RFID application research and development project. Funding: EUR 7.5 million.

o Objective: to resolve barriers to the implementation of RFID and EPCglobal technologies (solutions for network(s), application software, security, hardware, …

SMART

o 30-month project.

o Objective: … based on effective and efficient information/knowledge sharing and collaboration across supply chain partners, capitalizing on the fact that products are uniquely identified with the use of smart tagging technology …

StoP

o 30-month project

o Objective: … based and network-oriented systems for the …

Indisputable Key

o Objective: resource optimisation in the timber industry.

CE RFID (Coordinating European Efforts for Promoting the European RFID Value Chain)

o Objective: CE RFID aims at improving the conditions of competition for RFID technology and its further development in Europe and at reinforcing the political environment of RFID at European …

Source …

REFERENCES

Auto-ID Labs (2006), Auto-ID Lab St. Gallen   About, www.autoidlabs.org/the-labs/stgallen/about/page.html, accessed 19 April 2007.

Barua, A., D. Mani and A. Whinston (2006), *Assessing the Financial Impacts of RFID Technologies on the Retail and Healthcare Sectors*, University of Texas at Austin, Austin.

Bundesministerium für Wirtschaft und Technologie (BMWi) (2007, editor), *RFID: Prospects for Germany, The State of Radio Frequency Identification -based Applications and their Outlook in National and International Markets*, Berlin.

Danish Board of Technology (2006), RFID from Production to Consumption   Risks and Opportunities from RFID Technology in the Value Chain, www.tekno.dk/pdf/projekter/p06_rapport_RFID.pdf, accessed 1 February 2008.

EC Ruhr (2007), *RFID   Eine Chance für kleinere und mittlere Unternehmen*, http://www.ec-net.de/EC-Net/Redaktion/Pdf/RFID/rfid-leitfaden-mittelstand,property=pdf, accessed 1 February 2008.

European Commission, DG Enterprise and Industry (2007), Sectoral e-Business Watch, Chart Report 2007, http://www.ebusiness-watch.org/statistics/table_chart_reports.htm, accessed 6 April 2008.

I ± ® « ¬ ¡ Š ª ˙ ¸ « © © ¥ ¯adio Frequency Identification (RFID) in Europe: ¯ ° ¡ ¬ ¯ ˙ ° « ³ Š ® Ÿ ¯ ˙ Š ˙ ¬ « ¨ ¥ œµ ˙ ¢ ® š © ¡ ³ « ® § ˙ ¸ « © © ± ª ¥ œŠ European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions (COM(2007)96), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:EN:PDF, accessed 6 February 2008.

Federal Office for Information Security (Germany) (2004), Security Aspects and Prospective Applications of RFID Systems, http://www.bsi.bund.de/fachthem/rfid/RIKCHA_englisch_Layout.pdf, accessed 1 February 2008.

Finkenzeller, K. (2006), *RFID Handbuch*, 4th edition, Hanser, Munich.

Garfinkel, S. and B. Rosenberg (Eds.) (2005), *RFID: Applications, Security, and Privacy*, Addison-Wesley Professional, Upper Saddle River.

Hodges, S. and D. McFarlane (2005), *Radio Frequency Identification: Technology, Applications and Impact*, Whitepaper, Auto-ID Labs, Cambridge.

Industry Canada (2008), *RFID Technologies and Consumers in the retail marketplace*, www.ic.gc.ca/epic/site/oca-bc.nsf/en/ca02287e.html, accessed 1 February 2008.

AIM Global (The Association for Automatic Identification and Data Capture Technologies),
www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf.

www.oecd.org/
dataoecd/19/23/39693586.pdf, accessed 1 February 2008.

IEEE Security and Privacy, Nov./Dec., pp. 85-89.

RFID Journal,
http://www.rfidjournal.com/article/articleview/1338/1/129/, accessed
19 April 2007.

TA-SWISS Zentrum für Technologiefolgen-Abschätzung (2003), *Das Vorsorgeprinzip in der Informationsgesellschaft - Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt*, http://www.ta-swiss.ch/a/info_perv/2003_46_pervasivecomputing_d.pdf, accessed 1 February 2008.

NOTES

1 For a discussion of different frequency ranges and further characteristics of RFID systems see the OECD RFID country study for Germany [DSTI/ICCP/IE(2007)6/FINAL].

2 EPCglobal Inc. is an industry standards group which establishes industry-driven standards in the field of supply chain management (see also http://www.epcglobalinc.org/about/).

3 European Commission, DG Enterprise and Industry: Sectoral e-Business Watch, Chart Report 2007. The final study by the Sectoral e-Business Watch is expected in June 2008. The e-Business Watch studies aim at analysing the impact of ICT and e-business on enterprises, industries and the economy in general.

4 The survey sample consisted of 434 enterprises from 4 sectors (manufacturing, retail distribution, transportation, hospital activities) and 7 EU countries (France, Germany, Ireland, Italy, Poland, Spain, and the United Kingdom). Quantitative interviews were conducted by phone relying on computer-assisted telephone interviews (CATI).

5 The survey question was stated as follows: "Please tell me for each of the following items whether or not this is a relevant barrier for an RFID project. Is ° ¤ ¥ ¯ ˙ Š ˙ ®¡ ˙ ¡ ² Š ª ° ˙ › Š ®®¥¡ ® ˙ ¢ « ® ˙ Š ª ˙ & ∕ Ł ˇ ˙ ¬ ® « ¦ ¡ œ° ˙ ¡ ² ¥ Ÿ ¡ ª œ¡ ˙ « ¢ ˙ Š ˙ ¯ ° ® « ª £ ˙ ®¡ ° ± ®ª ˙ « ª ˙ ¥ ª ² ¡ ¯ ° © ¡ ª ° ˙ &

6 Small and medium-sized enterprises.

7 http://www.ic.gc.ca/epic/site/oca-bc.nsf/en/ca02287e.html.

8 English summary: http://www.tekno.dk/pdf/projekter/p06_rapport_RFID.pdf.

9 http://www.rfidlab.fi/?1;2;1200;1200;14.html.

10 http://www.nextgenerationmedia.de/Nextgenerationmedia/Navigation/en/rfid-conference.html.

11 http://www.ec-net.de/EC-Net/Redaktion/Pdf/RFID/rfid-leitfaden-mittelstand,property=pdf,bereich=ec__net,sprache=de,rwb=true.pdf (in German).

12 http://www.bsi.bund.de/fachthem/rfid/RIKCHA_en.htm.

13 http://www.osservatori.dig.polimi.it/dettaglioOsservatorio.php (in Italian).

14 http://www.risiko-dialog.ch/Themen/Kommunikationstechnologien/263 (in German).

15 http://www.ta-swiss.ch/a/info_perv/2003_46_pervasivecomputing_d.pdf (in German).

16 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:EN:PDF.

[17]   See for example the National Science Foundation (NSF)
(http://www.nsf.gov/eng/iip/iucrc/directory/celdi.jsp) and the National
Institute for Standards and Technology (NIST)
(http://www.nist.gov/public_affairs/techbeat/tb2006_0330.htm#rfid;
http://csrc.nist.gov/staff/Kuhn/phillips-karygiannis-kuhn05.pdf) for the United
States.

[18]   www.tekes.fi/giga.

[19]   http://www.software.net.mx/en/prosoftp4p.htm.

[20]   http://www.bridge-project.eu/.

[21]   http://www.smart-rfid.eu/page.php?3.

[22]   http://www.stop-project.eu/PROJECT/tabid/57/Default.aspx.

[23]   http://www.rfid-in-action.eu/public/.