For Official Use **DSTI/ICCP/IE/REG(2007)1/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **07-Apr-2008**

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/IE/REG(2007)1/FINAL
For Official Use

Cancels & replaces the same document of 25 March 2008

Working Party on the Information Economy
Working Party on Information Security and Privacy

OECD POLICY GUIDANCE ON RADIO FREQUENCY IDENTIFICATION (RFID)

www.oecd.org/sti/security-privacy
www.oecd.org/sti/information-economy

JT03243729

English - Or. English

FOREWORD

This OECD Policy Guidance on Radio Frequency Identification has been developed by the OECD Committee for Information, Computer and Communications Policy (ICCP), through its Working Party on the Information Economy (WPIE) and Working Party on Information Security and Privacy (WPISP). It has been developed as a contribution to the 2008 Seoul Ministerial Meeting on the Future of the Internet Economy and draws on policy discussions and analytical studies on RFID carried out by the OECD from 2005 to 2007.

It was declassified by the ICCP Committee at its 54th Session on 5-7 March 2008. It is published under the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

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 tags to the organisation's information infrastructure where it is processed and 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 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

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-Frequency Identification: a Focus on Security and Privacy" (2008) [DSTI/ICCP/REG(2007)9/FINAL], "Radio Frequency Identification Implementation in Germany: Challenges and Benefits" (2007) [DSTI/ICCP/IE(2007)6/FINAL], "Radio-Frequency Identification: Drivers, Challenges and Public Policy Considerations" (2006) [DSTI/ICCP(2005)19/FINAL], "Proceedings of the OECD Foresight Forum on Radio Frequency Identification Applications and Public Policy Considerations" (2005) [DSTI/ICCP(2006)7].

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 or object. Tags' data depends on their use contexts. For example, in a supply 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 data ("skimming"). While not all uses of RFID implicate privacy concerns, RFID 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.

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

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

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).

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; technical measures to protect security and privacy; individuals' 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).

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 information

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 stage of the system's life (planning, deployment, operation, 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, each stage of the system's life, and each component of the system.

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 information, or in which it would not be in the individuals' best interest to disable 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, individuals' knowledge and consent, and transparency. Extending the dialogue to 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.