Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

27-Feb-2006

English - Or. English

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

RADIO-FREQUENCY IDENTIFICATION (RFID): DRIVERS, CHALLENGES AND PUBLIC POLICY CONSIDERATIONS

JT03204562

DSTI/ICCP(2005)19/FINAL
Unclassified

English - Or. English

FOREWORD

This document is the result of research intended to provide background and facilitate discussions at the OECD ICCP Foresight Forum on RFID, which was held in Paris on 5 October 2005. It has been revised to integrate comments provided to the Secretariat after the Forum by member-countries.

The objectives of the Forum were to provide the venue for an exchange of views and information between governments, experts from the business community and from academia, and civil society; take stock of current and future RFID applications and their potential economic and social benefits; and have a forward-looking policy discussion on critical issues raised by RFID, including infrastructure and standards, as well as security and privacy.

The proceedings of the Forum on RFID, which attracted some 150 participants, have been made available separately.

This report was prepared by Ms. Karine Perset of the OECD's Directorate for Science, Technology and Industry. It is published on the responsibility of the Secretary-General of the OECD.

c OECD / c OCDE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Description of the technology, its economic potential, and applications

Radio Frequency Identification (RFID) is one of several automatic identification sensor-based technologies consisting of three key elements: RFID tags (transponders, typically miniaturised chips); RFID readers (transceivers); and a data collection, distribution, and management system that has the ability to identify or scan information with increased speed and accuracy.

RFID technology is actively being deployed to control manufacturing processes, track assets, enable financial transactions, pay tolls and gas, as well as to allow secure building access and other applications. The developments of standards, technological advancements and end-user mandates have spurred the growth of RFID into retail and consumer good applications. 2004 saw new product releases and, service offerings development at a cautious pace, to include overall market education, and 2005 is seeing much of the same. RFID is poised for growth worldwide, as businesses and governments implement RFID applications to facilitate global commerce and spur innovation and competitiveness. Compared to the bar code system, RFID promises long-term gains, increased reliability and efficiencies in supply chain management, transportation, defence, healthcare, and security and access control, to mention a few. RFID is increasingly used in commercial supply chain applications through aggregate level tagging (*e.g.*, tagging of cases and pallets) and is predicted to produce long-term measurable productivity gains within supply chains and within economies as a whole.

Though it is difficult to predict future uses of RFID technology, it offers promise as the first iteration of intelligent sensor networks. Capable, smaller, cheaper devices such as chips, sensors and actuators are increasingly (inter)connected through radio technology at the edge of IP networks to produce intelligent and innovative applications.

As with the Internet or mobile telephony, RFID is a networking technology – as adoption grows, benefits grow. With time, high costs in the early stages of adoption will give way to cost reductions and growing adoption, leading to benefits and further adoption. As costs fall and the technology gains more prominence, demand should continue to grow based on current assessments of demand drivers, from tens of billions of tags in 2006, to hundreds of billions by 2009, to perhaps trillions later. As prices of RFID hardware and software fall from the current levels[1], many organisations should find valuable uses for RFID in their organisational and logistics operations. Analysts[2] have identified what they consider to be three distinct phases of RFID deployment in economies: initial pilot tests and experimenting with RFID (2003–2005), followed by a supply chain infrastructure phase (2005–2009), then, widespread item-level tagging (2009–2013).

There are significant drivers for industries and governments to develop and rollout RFID solutions throughout value chains. Potential commercial benefits and projected return on investments are significant, as industry and various international standards and specifications-developing organisations, including the International Organization for Standards (ISO) have been developing interoperable standards; large retailers and governmental agencies have mandated RFID labelling for their suppliers; and increasing legislative requirements are driving RFID adoption in certain industries and for certain application areas. Consequently, implementation costs are decreasing rapidly. However, several challenges remain, such as interoperability, current costs of implementation, and privacy and data security issues for certain RFID applications.

Because it is a cross-cutting and enabling technology, RFID contributes to the important role that Information and Communication Technology (ICT) plays to promote innovation, economic growth, and global commerce. Looking toward the future, as the information infrastructures associated with RFID are increasingly accessed across IP networks and contribute to world economies, the OECD is well positioned to discuss with stakeholders how best to create a positive environment for growth, and promote best practices for the implementation and use of RFID.

Critical issues for policy makers

RFID touches on several regulatory and/or policy issues highlighted in this paper. These include international trade, intellectual property rights, standards, spectrum, security, and privacy. These issues are not limited to technical or policy areas, but have potentially wide-ranging social, economic, as well as national security implications. Thus, RFID's benefits and potential pitfalls should be considered within the wider context of its impact on economies and society.

The window of opportunity is now, for policy-makers, industry and consumers to understand and discuss forward-looking public policy issues associated with radio-frequency identification technology and applications, as well as to review existing and proposed associated legislation. It is imperative to understand the technology, its potential, and its policy implications. To achieve the full potential of RFID technology, the inter-related issues of technology diffusion, standards, costs, and privacy and security must be addressed.

Standards work is underway in both standards developing organisations and industry consortia, including the ISO[3] and EPCGlobal[4]. There is an opportunity to examine the merits of encouraging co-operation towards the development of global, interoperable standards, so as to lower costs and have a more uniform approach as the technology continues to emerge in markets. Challenges also remain in harmonising frequency allocation for RFID operations, which vary across regions, and in adopting worldwide interoperable communication protocols.

As RFID migrates to item level tagging in coming years and as governments adopt RFID in various personal identification schemes, it is crucial to address privacy and security issues related to certain types of RFID systems and applications; these issues will play an important role in the wider acceptance of the technology:

- Policies and technological developments that are informed by industry and individual needs, will foster the potential of ICT and facilitate development of emerging technologies such as RFID. Well-crafted policy interventions, such as guidelines around the appropriate use of RFID, may create incentives for the development of technological solutions that address and incorporate smart privacy and security issues early on.
- As with the Internet, promoting consumer education, empowerment of users, disclosure, and choice is the likely most successful road to sustainability and economic benefits.
- A solution set might combine self-regulatory mechanisms, policy guidelines and technological solutions with education and awareness programs.
- Some potential applications of RFID may pose unique privacy and security concerns because people cannot see or sense radio frequencies, and because most RFID tags do not keep a record of when and by whom they have been read.
- RFID is used in a wide range of applications: the impact on personal privacy and data protection varies greatly depending on the specific system and application.

- To safely construct a broad RFID infrastructure, a balance must be achieved between regulation and innovation, whereby private sector innovation is preserved and user benefits are available, whilst legitimate concerns that determine acceptance are identified and addressed.

INTRODUCTION TO RFID

As a sophisticated subset of automatic identification and data capture (AIDC) in the ICT field, Radio-Frequency Identification (RFID) uses radio frequency based communications to allow for contact or contactless reading of identification of entities (products, people or animals), places, times or transactions[5].

Although RFID technologies have been in existence since the 1940's for weapon identification and are already widely used in several areas such as automated toll payments, proximity cards, or theft-detection tags, the improving cost structure and decreased chip size have only recently made it accessible and practical for wide-ranging tracking applications widely across the economy, especially in the industrial, transport, security and consumer goods and service sectors.

Radio-frequency identification (RFID) consists of transponders and readers. Transponders – in the form of either RFID tags or contactless cards – are electronic circuits attached to antennas that communicate data to readers via electromagnetic radio waves using air interface and data protocol as well as many other protocols. RFID tags may be active, with a battery, or passive, which means that they have no internal power supply and harvest power for operation from the reader's electromagnetic field. Passive tags have a shorter range than active tags, and are also passive in their function: readers activate, drive and structure the communication with passive tags, whereas active tags can emit spontaneously.

There are many different types of RFID systems that vary in their exact mode of operation and operating performance. Typically, inexpensive RFID tags used for basic object identification consist of tiny electronic circuit attached to small antennas that are capable of transmitting a unique serial number to a reader. Generally attached to physical objects, they enable these objects to be tracked. Readers located within limited distances communicate with the tags, receive data from the tags, and send this data to an IT system consisting of databases, middleware, and application software for processing.

In the following, an "RFID tag" generally means a device that is generally attached to physical objects or a living being. When one of these objects comes into proximity with a specified RFID reader (either due to motion of the object or the reader) data from the associated tag can be read. The data may be used to identify that specific object or to provide information about it. Applications often use several RFID readers, so that tagged objects can be identified in different locations, for instance, along a production or logistics flow[6]. According to the needs of the application, readers transmit data such as identification and location information and might receive data such as product price, colour, date of purchase and expiration date. For this purpose, the chip consists of a cheap memory and miniaturised radio-frequency circuitry.

Other form-factors of RFID technology are contactless cards, used, for example, for access control, individual identification (passports and electronic ID cards), digital keys (vehicles or motels), or payment. They are essentially sophisticated forms of RFID technology involving additional security features (a microprocessor with embedded processing and cryptographic features)[7].

RFID tags, *i.e.* inexpensive chips with wireless communications ability that attach information to everyday objects and enable their remote identification, can be being combined with sensors, with localisation functions enabled by Global Positioning System (GPS) technology, or with mobile telephony, and (inter) connected to IP networks. Many believe this interlinking constitutes the technological basis for an environment in which everyday objects can communicate. By extension, RFID is considered to be a building block both for the "Internet of things" and for networks of distributed sensors.

DRIVERS AND CHALLENGES TOWARDS ADOPTION

RFID and contactless smart card applications are already widespread in fields such as manufacturing processes, highway toll management, building access badges, mass transit, library check-out, and as an anti-shoplifting device[8]. However, due to cost barriers, performance issues, and lack of accepted standards, the impact on supply chain management has been more modest up to now.

Leveraging opportunities provided by RFID to both private and public sector actors involves understanding the potential applications and the different business cases for the technology and its applications, along with their limitations and current challenges, to develop forward-looking policies.

Drivers of adoption and benefits

RFID deployments have become a strong concern and in some cases a top priority for firms involved in manufacturing and production, logistics, retail, healthcare and for some governmental agencies worldwide. RFID tags are a promising technology enabling its users to efficiently collect and distribute, and potentially store and analyse, information on tracked objects, notably on inventory, location, business processes, security control and numerous other attributes. The Electronic Product Code™ (EPC), the RFID equivalent of the Universal Product Code, provides each product a unique and identifying serial number at the individual item level, which also offers the potential for reducing counterfeiting, and may significantly reduce Intellectual Property Rights (IPR) infractions, and enable pedigree tracking for some applications. The Electronic Product Code™ (EPC) stems mainly from the prominent GS1 consortium.

RFID tags can improve convenience, selection, prices, safety, and security as well as enable a range of new product offerings. In addition to the implications of RFID for supply-chain management in reducing the cost of goods and in saving time through automated checkout, post point-of-sales item-level RFID tagging offers interesting possibilities for item return services and for innovations in smart consumer appliances: *e.g.* RFID-enhanced refrigerators, ovens, washing machines, or personal inventories of CD-ROMs or books – as part of a ubiquitous network.

Putting RFID to Work for Consumers

Some major cell phone manufacturers are preparing the release of communication devices incorporating RFID technology they hope will change the way consumers buy products, services and use their credit cards. Near Field Communication (NFC) technology uses short-range RFID transmissions that provide easy and secure communications between various devices. That means that, for example, purchasing concert tickets, booking hotel rooms and making other types of reservations – and having these transactions charged to a credit card using account information stored in the handheld device or phone, could be as simple as holding a phone close (less than 20 centimetres) to a poster or advertising billboard[9].

In the medium term future, RFID could also be used to create smart products that interact with smart appliances. Merloni Elettrodomestici, an Italian appliance maker, was the first manufacturer to use RFID in its appliances[10]. The company has created a smart washing machine, refrigerator, and an oven. When clothes are dropped into the smart washing machine, an RFID reader in the appliance can read the tags in the clothes (if the clothes have RFID tags) and wash the clothes based on instructions written to the tag. The refrigerator is designed to track each item's expiry date and display information about its nutritional value and can even provide recipes for dishes that can be prepared with the ingredients in the fridge. And the oven will automatically set cooking and baking times and temperatures based on instructions from tags.

Unilever, the Anglo-Dutch consumer products goods company, has created a prototype kitchen of the future in which RFID readers in the pantry read all the tags on products on the shelves. A computer program determines what items can be cooked with what is in the kitchen[11].

Commercial drivers of RFID tags

Commercial drivers for RFID tags in "closed loop" applications

While the supply chain continues to be a major force for the momentum of RFID today, companies are looking to use RFID in more specialised applications where incremental returns on investment may be obtained rapidly. While supply chains tend to be far-ranging and disparate (open loop), focused, localised applications (closed loop) can provide incremental justification for RFID investment. These applications include warehousing, theft detection, asset location/tracking, people location, in-process inventory tracking, repair and maintenance, and luggage tracking. The applications in which companies are currently incorporating RFID are typically closed-loop, can have measurable results in the short term and can be deployed in phases.

Commercial drivers in "open loop" supply chains

RFID tags are expected (and in some instances have already demonstrated their potential) to generate productivity benefits in supply chain management and improved asset allocation, through faster information flow and better inventory management.

- **Speed and accuracy:** RFID has a greater potential of speed than barcodes because applications may require less human intervention, to the extent that appropriate middleware applications and high – capacity data handling software and hardware applications are available and implemented. For example, in several warehousing functions, RFID tags can instantly provide detailed information on exact counts of items, whether at the docking station or within the warehouse inventory. It is noteworthy that performance is heavily depending on the type of material tracked and on the implementation environment, and therefore that experimentation is needed.

- **Visibility:** Supply chain participants can benefit from the ability of RFID tags to hold more information about an item than existing barcode technology such as tracking lot numbers, serial numbers, expiration dates and other pertinent information.

- **Information accrual:** Some RFID tags are writeable, and as they go through various stages of the product life cycle, information can be added to the tag; for example, for food traceability. They may also be equipped with sensors to detect temperature, humidity etc.

The capabilities of RFID stated above should enable productivity gains through automation of receiving, expediting, replenishment, quality control, tracking of lots for recalls or expiration and other supply chain tasks, and also enable better asset allocation with increased fill rates, lower inventory, reduced theft, and better management of products vis-à-vis their expiration dates. It is believed that eventually all supply chain participants –- not just retailers or distributors –- may realise benefits from the use of RFID. It is also believed RFID will affect other facets of business processes, including sales and marketing.

Several studies have found that RFID can lower supply-chain costs by 3 to 5% and increase revenue by 2 to 7%.[12] Retailers in particular may benefit, by reducing out-of-stock items (which represent an average of 9% for retailers worldwide[13] and translate into significant lost sales) and theft (which costs retailers an average 1.7%of gross sales[14]).

Specific mandates for RFID tagging on suppliers, by retailers or governments

Mandates by large retailers and governmental agencies, including the US Department of Defense and Wal-Mart, requiring their top suppliers to use RFID tags, along with technological advances and decreased costs, have spurred the adoption of this technology. Mandates from customers are cited by many manufacturers as their primary reason for deployment of RFID in 2005[15].

- **Retail industry**: In June 2004, Wal-Mart mandated that its top 100 suppliers place tags on pallets and cases of products for shipment to a cluster of supermarkets in northern Texas by early 2005, and its next 200 largest suppliers by early 2006. It is using tags to track goods from when they leave suppliers, through its warehouses/distribution centres, up to the store backrooms and shelves. In the case of Wal-Mart, an early adopter of large-scale, and item-level tagging, the driving force is to efficiently link front-end merchandising and marketing with back-end distribution and purchasing. Suppliers use Wal-Mart's IT systems to automatically track sales of their goods in Wal-Mart stores and co-ordinate replenishment. Other retailers have followed suit, including Tesco, Britain's largest supermarket, and German retailer Metro. Furthermore, Wal-Mart has since extended its RFID roll-out to its top 300 suppliers and to more stores.

- **Governmental agencies**: In the United States, led by the US Department of Defense (DoD), public agencies have been actively implementing RFID solutions. Main applications so far have been in inventory control and in keeping track of expensive items. In October 2004, the DoD mandated that, by January 2005, it would require its suppliers to put tags on cases and pallets shipped to its warehouses. The DoD claims that RFID has enabled it to save in excess of USD 100 million[16], for instance by avoiding reorders in battlefields through accurate information on availability of supplies. The US Social Security Administration has launched a pilot that it claims has generated significant returns, including for administrative applications such as keeping track of inventory or implementing speed passes within its own network of gas stations. In addition, a U.S. RFID Council, comprised of representatives of the entire executive branch and independent agencies, meets twice a year. The RFID Council has four subcommittees on: applications, regulatory issues, standards, and privacy and security. In Europe, the EU Reflection Group on RFID is in the process of drafting a Commission communication on RFID outlining issues associated with RFID (the Reflection Group includes representatives from several DGs, including DG Information Society, DG Enterprise, Taxes and Customs.)

Table 1. Potential RFID benefits for supply chain partners

Manufacturers	Logistics Providers	Retailers
Shorter shipment loading times	More efficient order selection	Better store planning, programming and merchandising with real-time data
Greater shipment accuracy	Better order fill rates	Improved point-of-sale productivity and accuracy at checkout
Better consumer sales data from retailers	Less inventory shrinkage	More accurate returns
Reduced counterfeiting/diversion	Fewer administrative and other human errors	Improved reverse logistics
Improved support for vendor-managed inventory	Lower labour requirements	Greater inventory accuracy and velocity
Easier product safety recalls	Less vendor fraud	Optimised store in-stock levels
More accurate demand planning	More accurate inventory	Reduced internal and external shrinkage
Shorter order lead times	Less time and lower cost for managing inventory	Lower labour requirements
Less need for safety stock	Higher routing efficiency	Automated receiving, vendor payments and shipments to store
Better use of labour	Better security for distributing medical products	Better use of reusable assets (*e.g.* pallets)
Higher sales	Automated receiving, vendor payments and shipments	Lower detention/demurrage charges
Less time and lower cost of cycle counting, receiving, picking and shipping	Increased capacity through more efficient operations	Better grey-market containment
Fewer charge-backs for inaccurate deliveries	Fewer penalties for execution errors	Better ways to measure the execution and effectiveness of display programs

Source: Shutzberg, L. (2004), Radio Frequency Identification (RFID) in the Consumer Goods Supply Chain: Mandated Compliance or Remarkable Innovation? Industry White paper, Rock-Tenn, Norcross GA. p51.

Legislative drivers for RFID display programs

Legislation, particularly relative to product traceability, person tracking, and to national security – such as recycling obligations, requirements to provide country-of-origin labelling, pharmaceutical tracking, food ingredient traceability, techniques to prevent counterfeiting, or cross-border controls – is a catalyst of RFID adoption in certain industries and for certain application areas.

European directives on packing and waste management, including the Waste Electrical and Electronic Equipment (WEEE) Directive, Packaging and Packaging Waste Directives and the Management of End-of-life Vehicles Directive, render producers responsible for waste management. RFID may potentially help in identifying equipment and sub-components that need to be processed, and identify the responsible manufacturer.

Legislation regarding the tracking of medical supplies and food in order to ensure human health and safety is another driver for the adoption of RFID technology. In some cases, existing or proposed legislation requires quite onerous audit trails of such products to be maintained by manufacturers and

retailers. In these cases, while several types of technologies might be used to meet the guidelines, RFID is an obvious choice for cost-effective implementation. In some instances, RFID technology is being explicitly recommended or mandated. For example, the US Food and Drug Administration recommends that drug manufacturers, distributors and retailers adopt RFID technology to combat counterfeiting[17].Additionally, in the food industry, food traceability enabled by RFID is a major topic for discussion[18].

The 2000 Transportation Recall Accountability and Documentation (TREAD) Act, passed in the United States after major recalls involving Firestone/Ford, mandates embedding RFID tags into automobile tires to allow precise tire tracking in the event of a recall[19].

The US Department of Homeland Security has been encouraging the creation of an ISO standard for cargo container electronic seals. Ports and carriers worldwide are waiting for this standard to be finalised before they invest in implementation. The incentive will be fast-track lanes in US ports for carriers that use RFID seals[20]. Initial costs will be high since use of RFID for a large number of containers necessitates infrastructure at every point where cargo status is important, but marginal costs thereafter should be low[21]. Applications of contactless cards for personal identification of citizens (*e.g.* travel documents, identification cards in Belgium and several programmes in Europe), for personal entitlement (*e.g.* the U.K. entitlement card project) are also progressing rapidly[22].

Challenges of RFID

Despite the numerous advantages of RFID technology, realizing its potential requires addressing a number of inter-related technological, economic, standards, privacy, and security issues.

Technological challenges

Technological issues relating to laws of physics must be managed. Although radio waves can pass through most articles, the combination of materials, operating frequencies, associated power and environment can prove to be problematic.

Interference is a main issue. Indeed, there are multiple sources of potential background interference as tags and readers attempt two-way communication. The first source of interference is that data signals of one reader can collide with those of another (reader collision). Furthermore, a proliferation of wireless devices (cordless and mobile phones, personal digital assistants or PDAs, consumer electronics devices, etc.), also creates potential for electromagnetic interference with RFID systems. This might become a significant problem deteriorating the accuracy of RFID systems, since RFID does not have its own dedicated frequency band in most jurisdictions, but rather, operates in bands that are shared with other users. If they are to become widespread, RFID applications will increasingly need to take radio magnetic interference from other devices into account in RFID design and use.

Potential interference of RFID with existing use of radio frequency ranges must be taken into account in RFID design and use. Setting a single global radio standard for RFID systems may not be possible in all frequency ranges considered by Industry. In particular, frequencies assigned for use by RFID are not consistent worldwide in the ultra high-frequency range (UHF: 860 MHz-960 MHz), including throughout different countries in Europe. This limits interoperability of RFID systems, depending on the region or country of the world where the system is used.

Security is yet another technological challenge that RFID faces, since the inclusion of cryptographic features increases cost and may reduce speed.

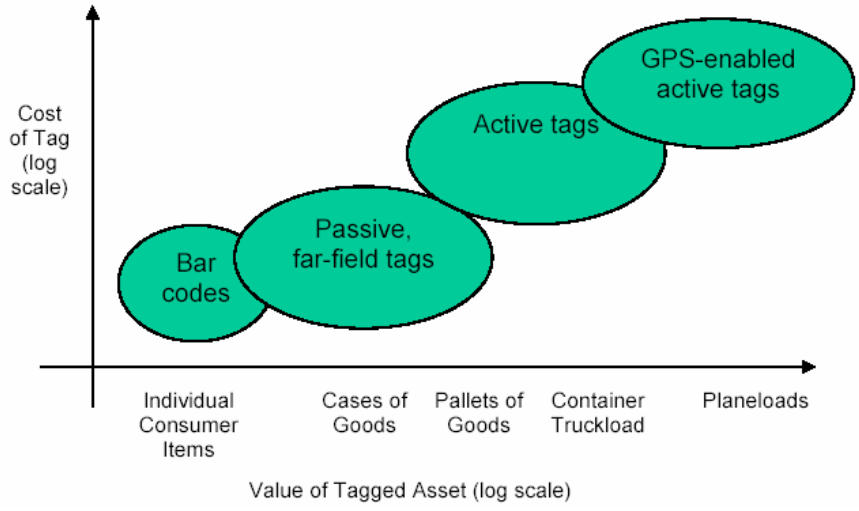
Cost of implementation

Although RFID is already used in many applications today, such as "identification of friend or foe" applications on the battlefield or tracking of vehicles applications which are easy to justify, RFID adoption overall is still in the very early stages. A significant challenge to adoption is that RFID implementation at this stage remains expensive.

If RFID is to gain widespread acceptance, a strong case needs to be made that its return on investment (ROI) exceeds that of current barcode tracking technology. While a plethora of companies claim to have achieved ROI in less than 12-18 months[23], many – in particular those that minimally implement RFID, and SMEs who need to implement RFID to comply with mandates, believe that RFID lacks ROI, according to AMR Research[24]. While the technology offers potential operational cost savings, the investment hurdles are still high: depending on the asset value of the tagged item, the price of the tag can be high as shown in Chart 2. For example, the cost of EPC RFID tags are based on volume, the amount of memory on the tag, and the packaging of the tag, and vary between 20 to 50 U.S. cents. Readers are costly as well: most cost from USD 1 000 to USD 3 000, depending on the features in the device. Companies may also have to buy each antenna separately, which are about USD 250 and up[25]. Database and infrastructure requirements also add to the cost of implementation. Typically, RFID technology costs[26] could be thought of as roughly evenly distributed between hardware, software, and systems integration with existing IT systems. However, as in the case of smartcard and contactless card projects, the major cost factor of RFID tag implementation projects may be in their integration within existing processes, or incurred in process reengineering, rather than in specific hardware or additional network and computing equipment.

Chart 2. The types of tags appropriate for different types of assets

Both the vertical scale of tag cost and the horizontal scale of asset value are logarithmic



Source: National Academies of Science, 2004

Another directly related question is that of who bears the cost of RFID and who reaps the benefits. Resistance has stemmed from (often small and medium sized enterprises) suppliers who claim they are being forced to pay for an investment that saves retailers money. Suppliers will be more likely to consider RFID solutions as a business strategy instead of a compliance issue, when the cost of deployment drops with greater economies of scale, lowering the relative cost of tags, readers and software that make up the RFID system. According to AMR Research[27], 137 Wal-Mart suppliers spent USD 250 million on RFID – *i.e.* USD 1M to USD 3M each, on RFID to meet the minimum requirements for the January 2005

Wal-Mart mandate deadline, to purchase tags, readers, and minimal software. AMR Research also estimated that in order to see significant benefits and ROI, rather than just incurring expenses to meet mandates, each supplier would need to spend USD 13M to USD 23M to integrate RFID into their applications, change existing software and enable large volumes of data to be stored and shared, as appropriate.

Process change

Potential achievements made possible by RFID can be substantial, but, as with other technological advances, they require effective process change. Many organisations have stated that RFID is not a solution or a goal, but an enabling tool to replace current business processes with ones that are more immediate, more precise and less redundant[28]. For RFID to streamline operations, companies must redesign the way they work to exploit it. Business process issues involve enterprise application vendors as well as systems integrators and process change consultancies.

Full benefits of RFID depend on the ability to redirect personnel from tasks such as scanning, searching and verifying product, to higher-value tasks such as providing better customer service[29] or anticipating problems and collaborating on solutions.

IT systems

One of the main stumbling blocks to moving forward with RFID adoption is not the hardware –tags and readers– but the edge-of-network middleware, or RFID middleware, which links RFID hardware to an enterprise's various IT systems. According to ABI Research, per distribution centre, software costs in 2004 ranged from USD 75 000-USD 125 000, excluding integration costs. Furthermore, licenses for retail software ranged from USD 1 500-USD 3 500[30]. These costs have been decreasing significantly with increasing deployments and competitive pressure. Large enterprise resource planning (ERP) providers including SAP, Oracle, IBM and others, are successfully working on applications to manage information flowing from RFID tags and leverage it within existing applications.

Tracking many RFID-enabled objects generates enormous volume of data that will have to be filtered, stored and accessed efficiently. This will require efficient data management, very rapid access and high-capacity storage, and methods of dealing with inaccurate data and ensuring data integrity and data transfer across different systems. One analyst calculated that if Wal-Mart stored every RFID of every tagged item on every shelf, it would generate nearly eight terabytes of data per day[31]. Companies such as Cisco, Nortel and Symbol are looking at how traditional wireless and network management capabilities can translate into more complex active and passive RFID environment management and are already bundling RFID capabilities into existing network provisioning, security and management solutions[32].

Legislative barriers

Additional issues exist regarding health and environmental regulations. For example, in Europe, the Waste Electrical and Electronic Equipment (WEEE) Directive mandates recycling of tags. If RFID tags are embedded into items such as cardboard boxes (rather than attached to the outside packaging of the item, for example), then there may be an issue with subsequently recycling the box since the tags must be removed first.

Consumer and employee privacy concerns as a potential barrier

Privacy is an important issue for RFID implementation, both at a consumer and at a corporate level. In the absence of established rules of practice such as disclosure and transparency, or dedicated technologies to treat data and access adequately, people purchasing goods with tags or working with tagged items may

be unaware of the existence and usage of these tags and, in instances where these tags are used as part of loyalty programmes or charge cards to store identification and other personal information, an individual's personal details could be compromised, or hacked into, if the application is not sufficiently secured. In a similar way, trade unions, privacy advocacy groups and consumer protection entities in some countries have complained that RFID tracking technology may violate employee privacy[33].

There is some opposition to RFID implementation and tracking by consumer groups who worry about the "big brother" aspect of this technology[34]. Without addressing privacy-related issues carefully, appropriately and transparently, including through education, backlash by consumers and citizens is a potential risk that could limit long-term benefits and development. Stakeholder groups such as the Center for Democracy and Technology (CDT) or the Electronic Privacy Information Center (EPIC) are working on constructive dialogues and frameworks, including practical solutions to enhance free expression and privacy in global communications technologies.

MAIN POLICY ISSUES ASSOCIATED WITH RFID

A major advantage of exploring RFID-related issues at this current stage of development, and the primary reason for the ICCP Foresight Forum on RFID, is an opportunity for debate among all stake-holders; including industry, government, civil society, and the technical community; to address policy issues early on and to implement solutions into the actual RFID infrastructure, while respecting OECD economies' needs to balance technology neutrality in their home environments. The issue of legacy infrastructure is vital, as RFID systems designed today may last for decades. Unlike the Internet, where the software by which users connect to the Internet can be updated or patched, the architecture of RFID systems is such that retooling large numbers of small wireless hardware devices could be more expensive. On the other hand, restrictions imposed today could cause the technology to be stifled in its (relative) infancy and prevent it from reaching its vast potential as an economic driver.

Two main policy issues that need to be addressed by all stake-holders and will be discussed at the OECD Forum on RFID are: standards and interoperability, and security and privacy. Standardisation constitutes the main driver for interoperability, which, as mentioned earlier, can also facilitate the adoption of security and privacy requirements. Looking forward, as RFID matures and tag reading capabilities increase, privacy and security issues (in particular unauthorised access, information-sharing leakages and location-tracking concerns) could increase.

Standards and interoperability

With economies increasingly dependent upon the global trading system, the need to explore the benefits and costs of interoperability amongst standards, and harmonisation of standards, has increased. One view is that multiple standards represent large costs for product and technological development and can also represent significant non-tariff trade barriers. Another view is that the ability to develop competing technologies based on alternative standards is the best way to drive innovation and adoption by spurring consumer choice. Successful standards tend to share characteristics of being voluntary, market driven, open, transparent, balanced, and developed in a performance-based system with due process.

Main RFID standards

RFID technology has undergone and is still subject to extensive standardisation activities at the regional and international level through activities in standards developing organisations and consortia, such as ISO and EPCglobal, amongst others. Beyond ISO and EPCGlobal, ongoing RFID standardisation activities are taking place in a number of standardisation bodies, including for example the European Committee for Standardization (CEN), the European Telecommunications Standards Institute (ETSI), the US National Institute of Standards and Technology (NIST), or the Standardization Administration of China (SAC). In addition, it should be noted at the outset that there are opposing views to the EPCGlobal approach, including concerns about intellectual property issues.

There are existing and proposed RFID standards and specifications that specify *i)* the format of data contained in RFID tags (the way data is organised or formatted), *ii)* the air interface protocol for communication between the tags and the readers (frequency, modulation, bit encoding, etc.), *iii)* conformance, ways to test that products meet a standard, *iv)* particular applications, for example how

standards are used for shipping applications, and, *v)* "middleware" protocols, specifying how data and instructions are processed.

One fora of great interest is the ISO, which has created standards for "closed loop" RFID. These include standards for animal identification (ISO 11784 and 11785) and standards for the air interface protocol for RFID tags used in payment systems and contactless smart cards (ISO 14443) and in-vicinity cards (ISO 15693). It also has established standards for testing the conformance of RFID tags and readers to a standard (ISO 18047), and for testing the performance of RFID tags and readers (ISO 18046).

For "open loop" supply chains, where tags are designed to be reused throughout the whole supply chain, applications are relatively newer than the one previously cited, and fewer standards have been finalized. ISO is developing standards for tracking 40-foot shipping containers, pallets, transport units, cases and unique items. These are at various stages in the approval process.

Since 1999, one area of industry-led standardisation efforts has been by EPCGlobal Inc., which has led EPC™ to uniquely identify products and track them through the global supply chain, similar to the Universal Product Code (UPC) on barcodes. EPCGlobal's goal is to make RFID tags as simple as possible, with the aim of driving down the chips' costs below five cents enventually.[35] The EPCGlobal group has produced a taxonomy of tag classes, standard radio frequency signalling protocols between tags and readers, and formats for the storage of identity and data in tags. In addition, the EPC Global Network is creating specifications/standards to interconnect partners' servers containing information related to items identified by EPC numbers. The servers, called EPC Information Services or EPCIS are accessible via the Internet and linked, authorised and accessible via a set of network services, as shown in Chart 3.

In December 2004, EPCglobal ratified a long-awaited ultra high frequency (UHF) Class 1 Generation 2 (EPC Gen2) RFID standard for the air-interface protocol of second generation EPC technologies, which is spurring research and development into applications[36]. The standard calls for 96-bit memory, encryption and an ability to permanently deactivate tags after use. The EPC Gen2 standard removes major user concerns linked to different UHF EPC standards and is being positioned as royalty-free or light-royalty standard (though, technically, using the standard requires joining the EPCGlobal network).

Ongoing RFID standardisation processes

ISO is currently reviewing and balloting the EPC Gen2 specification to ratify into the existing ISO 18000 series, which covers the air interface protocol for major frequencies used in RFID systems around the world for use to track goods in the supply chain. But at present, the EPCGlobal Gen 2 specification has yet to be ratified by the ISO.

In addition, common standards for supply chain, inventory tracking, and asset management have yet to be worked out with China. This will be critical to tagging interoperable cases and pallets overseas, since China, which exports high volumes of goods, is one the world's largest potential RFID markets. EPCglobal has expressed its desire for China to embrace existing EPC. Currently, the Ministry of Science and Technology (MOST) and 13 other Chinese government departments including the Ministry of Information Industry (MII) and the Standardization Administration of China (SAC) are drafting a white paper on RFID in China, which will set the general direction of RFID development in the country. The Standardization Administration of China has charged the National RFID Tags Standards Working Group[37] to help decide which RFID technology standards China will adopt. China has stated that it will adopt standards that are compatible with EPCglobal and ISO standards, but that use its own intellectual property to build a royalty-free standard[38].

Intellectual property rights and competition issues

Intellectual property rights of standards makers, companies and users must be considered. RFID intellectual property issues, in particular Intermec's intellectual property claims[39] on EPC Gen2, caused a standards stalemate, delaying supply chain RFID projects and planning. Recently[40], a group of 20 RFID vendors, without Intermec, formed a "patent pool" consortium to offer easier access to some RFID intellectual property deemed to be "essential patents" by reducing the number of patent negotiations. Companies still need to address Intermec licensing on a one-to-one basis.

Information infrastructures associated with RFID

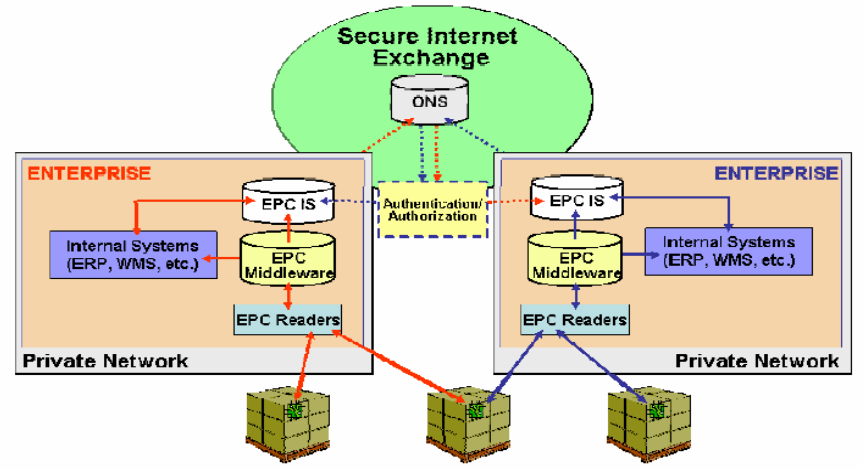
The information infrastructures associated with RFID, in particular with UHF EPC, are and will increasingly be accessed across IP networks, private intranets and the public Internet.

The political economy of RFID identifiers is similar to the coordination of name and number spaces in other media: fundamentally, identifiers must be unique and this uniqueness requires coordination. The Object Name Service (ONS) is an important part of the RFID-System developed by EPCGlobal for its implementation. Since the RFID tag only stores the Electronic Product Code of an object, the Object Name Service (ONS) interlinks this EPC with information about the specific item identified by the RFID tag. The ONS establishes the connection between a physical resource (identified through RFID tags that transmit EPCs) and the related information (which is formatted via Physical Mark-up Language or PML), via the Internet [41]. Information on a product can consist of detailed product information, order data, or details of the origin and history of goods.

This Object Name Service (ONS) is very similar to the Internet's Domain Name Service, an automated networking service that connects an address called a URL (Uniform Resource Locator) to an IP-address (a number), i.e. a computer which contains data. The ONS handles the allocation between EPC and a URL. Verisign, that also manages the root zone file of the DNS system on Internet, was selected by EPCGlobal to develop the ONS and operate the authoritative root for the EPC network for RFID and provide the security framework for authentication, data protection, and access control.

Additional initiatives for better connecting objects to information are under way. For example, the Digital Object Identifier (DOI) for electronic identification of documents and EPCGlobal are conducting a joint study regarding collaboration and possible convergence of DOIs and EPCs.

Chart 3. A graphic representation of the EPCGlobal network infrastructure



Source: EPCGlobal.

Spectrum and power limitations

RFID uses radio waves at different frequencies, meaning that radio-frequency systems integrate the specific band in which they operate in their design from the early conception. Radio frequency is regulated in countries either by a telecommunication regulator or a specific agency responsible for radio frequency. Some of the main bodies governing frequency allocation for RFID are described in Annex 3, Table 3. Radio frequency power emission is limited in most countries. This means that RFID readers can only emit a given amount of radio power, in general up to 2 Watt, limiting their range.

In general the frequency used by RFID applications is not subject to licensing. RFID uses both low-frequency (LF: 125 – 134.2 kHz and 140 – 148.5 kHz) and high-frequency (HF: 13.56 MHz). Low frequency is used for applications such as animal tracking, while high frequency is widely utilised in identification badges and building access controls, library book tracking, airline baggage tracking, apparel item tracking and pallet tracking.

However, there is no one single global standard for the ultra high-frequency (UHF: 850 MHz-950 MHz) bands that are viewed as key for "open circuit" supply chain management applications. In North America, UHF can be used unlicensed for 902 - 928 MHz, but restrictions exist for emitted radio power (by readers). In Europe, the European Telecommunications Standards Institute (ETSI) has published ETSI EN 302 208 on "Radio Frequency Identification Equipment operating in the 865 MHz to 868 MHz band, with power levels up to 2 Watts. However, some European countries have not yet implemented regulations as recommended by CEPT for RFID systems in the 865 – 868 MHz band, due to incompatibility with existing radio systems. For China, there is no regulation for the use of UHF. Each application for UHF in these countries needs a site license, which needs to be applied for from the local authorities. For Australia and New Zealand, 918 – 926 MHz are unlicensed, but restrictions exist for transmission power.

Though there is no one single global standard for UHF, "agile readers" are emerging which are able to read multiple tag protocols.

Box 1. RFID Frequency Bands and Standards

The most common RFID frequency bands and the standards associated with their usage:

Low Frequency: 25 kHz HF –- Near field, all passive	– ISO 18000-2
High Frequency (HF): 13.56 MHz HF –- Near field, mostly passive	– ISO 18000-3 Mode 1, Mode 2
	– ISO 14443 Type 1, Type B
	– ISO 15693
	– EPCglobal Class-1 HF
Ultra High Frequency: 900 MHz UHF –- Far field, some active	– EPCglobal Gen2
	– ISO 18000-6 Type A, Type B
Microwave: 2.5 GHz UHF –- Far field, some active	– ISO 18000-4 Mode 1, Mode 2

Source: based on U.S. National Academy of Science, 2005

Security and privacy by design

According to several security researchers[42], the privacy and security issues that RFID raises must be considered before standards are set and widely implemented. In their view, technology safeguards integrated in standards, whether as options or as requirements, can help maintain the balance between those concerned about business efficiency and those concerned about privacy. This "privacy-by-design" approach might prove to be more efficient in the long-run.

A working document by the European Commission (EC)'s Working Party of Member State Data Protection Authorities ("Article 29 Data Protection Working Party") investigating RFID and privacy, also

states that the way RFID standards and technology products are developed may have a great impact in ensuring the effective implementation of the data protection rights[43] that are recognised by Article 12 of the EC data protection Directive 95/46.

In many of the RFID standardisation initiatives, it may be possible to include enhanced levels of data protection features into technical specifications. For example, it was proposed by academics in 2004[44] to modify the standard of the reader-to-tag protocol developed by ISO, in order to implement, at the technical level, provisions of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Also at the standards-setting level, vulnerability studies conducted by working groups can assess the security of data on various types of RFID systems. For example, the electronic seal standard at ISO is being delayed by such concerns. Furthermore, data protection features of a standard may permit data encryption when necessary, as in the previously cited example of the electronic seal.

Security and privacy issues related to the use of RFID

The collection and use of personally identifiable information through RFID technologies, represents a public policy challenge, and a lack of privacy protection or sufficient security may hinder the deployment and use of RFID technologies. With RFID moving closer to item-level tagging in the next few years and also being used or considered by governments for authentication/identification applications such as identity cards, passports or license plates, issues relating to privacy and security of individuals come to the forefront. It is indeed likely that personal data will increasingly be obtained through RFID. At the same time, RFID security and privacy issues may vary widely according to the type of RFID system and how the RFID system is deployed within current legal frameworks.

Currently however, most privacy and security concerns around certain commercial applications of RFID involve the collection, use, and storage of the RFID-generated data at the individual customer level, at or after the point of sale. For instance, some concerns revolve around whether and what type of notice might be given to customers when RFID is used at the item level; whether options are provided to customers to disable the tag; what data is collected and how it is used or shared; and how long and for what purpose the data is retained. Some privacy advocates are concerned that RFID tags remain active after a purchase and that third-party groups might be able to access tag information or track item movements, unnoticed by the tag holder. To briefly summarise – the issue is when, by whom and how tags can be switched off, and what happens to the data on the tag or collected from the tag. Privacy concerns aside, it should also be noted that consumers, for various reasons, may wish to keep the tags active, for example in order to track their supply of medicine.

Inter-relationship of security and privacy issues

Security and privacy issues are closely inter-related and one RFID application may involve both types of issues. Security risks include infrastructure threats, as well as unauthorized access to **sensitive** personal information. Privacy risks stem from the possibility to use RFID to locate or track people. Additional privacy concerns stem from the fact that even RFID tags which do not contain personally identifiable information (*e.g.* a product code) could be associated with a person's identity.

- *Infrastructure threat:* Though not specific to RFID, corporate infrastructures dependant on RFID as a mission-critical element of corporate infrastructure could become increasingly vulnerable, *e.g.* to new forms of denial-of-service attacks through jamming radio frequency signals.
- *Skimming and eavesdropping:* Skimming occurs when information from an RFID chip is surreptitiously gathered by an unauthorised party. Possible scenarios include the use of RFID

readers by criminals to determine the contents of an individual's bag. Eavesdropping occurs when data is intercepted while it is being read by an authorised RFID reader.

- *Illicit tracking*: A primary security concern surrounding RFID use by governments or by companies is the illicit tracking of RFID tags, whereby, in addition to personal location privacy, corporate or military security may be violated if tags can be read arbitrarily. This may also give rise to the potential for corporate espionage inside the supply chain.

- *Cloning and ID theft:* Another security concern is that of unauthorized duplication, or cloning of RFID tags: some RFID tags can be scanned at a distance and without the tag-holder's knowledge. This is an issue for RFID tags in building access cards or contactless payment systems, as well as for RFID passports, ID cards, or even objects.

- Risks to privacy

  - The potential invisibility of RFID tags as well as readers is considered to be one of the major privacy concerns with RFID. Hence, there may be a possibility to collect information about a certain product, and – depending on the circumstances – also about the person carrying the product, without the knowledge or consent of the individual carrying the product.

  - An RFID application could collect large amounts of data. If a tagged item is for example paid for by credit card or in conjunction with use of a loyalty card, then it could be possible to tie the unique ID of that item to the identity of the purchaser. Personal data, obtained through RFID, could be used to create a profile of a person. Such a profile could then be used for various purposes, for example to evaluate a consumer's worth to a company.

  - In theory, RFID applications make it possible to track people through the RFID tags they carry with or on them. This will become more relevant if different RFID applications are integrated into a larger system. For example, the EPC Global system of tags creates globally unique identifiers for each tagged product.

Consumer and citizen perceptions and reactions

From the perspective of privacy and individual liberty, the previously-mentioned potential scenarios are undesirable. But firms and governments will have to handle privacy issues delicately. Privacy advocates, such as the Electronic Privacy Information Center (EPIC) or Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) are concerned that details of what consumers buy and how they buy it, may be held in databases and potentially used for detrimental purposes. Several well-known public campaigns such as those against Benetton, Gillette and TESCO were effective at halting the companies' RFID trials[45]. Constructive dialogues and discussions on lessons learnt are increasingly taking place between all stake-holders involved in order to achieve a balance between the needs of industry, governments, and civil society.

Legislative solutions

Applicability of existing privacy legislation

A question is whether current regulatory frameworks, *e.g.* legislation and self-regulatory mechanisms for the protection of personal data, are applicable, adequate and efficient to address issues associated with RFID. In most cases, existing privacy legislation, when it is technology neutral, is applicable.

Within Europe, laws implement Directive 95/46/EC, and are considered applicable to the gathering and processing of personal data by means of RFID. Directive 2002/58/EC is considered to be applicable in special cases where RFID is used in combination with mobile phone handsets. On 19 January 2005, The European Commission's (EC) Working Party of Member State Data Protection Authorities published a working document on data protection issues[46]. The working document is aimed at *i)* providing guidance to companies deploying RFID on the application of the basic principles set out in EC Directives[47], and *ii)* providing guidance to manufacturers of the technology as well as RFID standardization bodies on their responsibility towards designing privacy compliant technology.

In the United States, the Federal Trade Commission protects consumer information through enforcement of Section 5 of the FTC Act, which prohibits unfair or deceptive acts in or affecting commerce. The FTC has used Section 5 to enforce privacy and security promises made by companies that collect consumer information.

Processing personal data through RFID technology is also subject to the principles contained in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (cf. Box 2 below). The Guidelines have formed the basis for many of today's privacy laws, such as the EU Directive 95/46/EC, the Privacy Framework of the Asia Pacific Economic Cooperation (APEC) Group, and underpin much of the U.S. privacy law.

However, various definitions of personal information exist and these subtleties can make a difference when applied to RFID[48]. In addition, while in most cases existing EU privacy legislation is applicable when RFID technology is used to store and process personal data, the situation has to be nuanced when an RFID tag contains information that is in itself not related to an individual. For example, a product code contained in a tag that is attached to a product does not constitute personal information as long as the item is handled in the supply chain or stays in the realm of the seller. Existing EU privacy legislation would thus not apply. If, however, an individual purchases the product, and at or after the point of sale, the identity of this individual is revealed, the product code on the tag may itself become indirect personal information, and privacy legislation could be applicable. In addition, any information relating to an individual that may in the first place be collected through RFID technology without knowledge of the individuals identity, may become personal information when the individual's identity is linked to these data at a later stage.

The requirements that flow from the applicability of data protection and privacy legislation or principles include, inter alia, notification to individuals of the use of RFID technology, data collected, purpose of processing, identity of the data controller[49], and measures to enable individuals to exercise their right to access to their data, and to have data erased, rectified, completed or amended, as applicable. Data controllers would also need to limit the collection of personal data to that necessary for fulfilling the purpose of the application, ensure that the use of the data is consistent with the specified purposes, and implement security safeguards to prevent loss, unauthorised access, destruction, use, modification or disclosure of personal data processed in RFID applications.

In addition, the OECD has developed guidelines for the Security of Information Systems and Networks that apply to all participants in the new information society. These suggest the need for a greater awareness and understanding of security issues, including the need to develop a "culture of security" - that is, a focus on security in the development of information systems and networks, and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks. The guidelines constitute a foundation for work towards a culture of security throughout society.

Box 2. 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980, continue to represent international consensus on general guidance concerning the collection and management of personal information. By setting out core principles, the guidelines play a major role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to transborder data flows, both on and off line.

The Guidelines contain the following eight principles:

1. **Collection limitation**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data quality**: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. **Purpose specification**: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use limitation**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except a) with the consent of the data subject; or b) by the authority of law.

5. **Security safeguards**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. **Openness**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual participation**: An individual should have the right a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him (within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him); c) to be given reasons if a request made under subparagraphs a) and b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. **Accountability**: A data controller should be accountable for complying with measures which give effect to the principles.

Box 3. 2002 OECD Guidelines for the Security of Information Systems and Networks

The Security Guidelines should be read in conjunction with complementary recommendations concerning privacy (see Box 2) and cryptography (see Annex 2).

The Security Guidelines contain the following nine principles:

1. **Awareness**: Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

2. **Responsibility**: All participants are responsible for the security of information systems and networks.

3. **Response**: Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

4. **Ethics**: Participants should respect the legitimate interests of others.

5. **Democracy**: The security of information systems and networks should be compatible with essential values of a democratic society including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6. **Risk assessment**: Participants should conduct risk assessments to identify threats and vulnerabilities and should be sufficiently broad-based and allow determination of the acceptable level of risk.

7. **Security design and implementation**: Participants should incorporate security as an essential element of information systems and networks.

8. **Security management**: Participants should adopt a comprehensive and forward-looking approach to security management, based on risk assessment and dynamic; encompassing all levels of participants' activities and all aspects of their operations.

9. **Reassessment**: Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

Enacting specific provisions on RFID

Some countries, including Japan[50], Italy[51], Korea, and the United States (at the individual state level)[52] have proposed or are considering proposing specific guidelines or regulations on RFID.

Other countries, such as the Netherlands, have come to tentative conclusions that additional RFID specific legislation is not necessary at this stage of RFID development. They also believe that premature legislation will most likely delay and frustrate further development and application of RFID, while not necessarily contributing to better protection of privacy and individual freedom. In some cases, expanding legal protection of privacy may be less necessary than increasing the transparency of the existing regimen and strengthening enforcement of the legal regime.

Industry self-regulation

One example of a self-regulatory approach is the currently published (2005) EPCglobal guidelines[53] for EPC usage follow the basic privacy tenets of notice, choice, and security – and also include consumer education. *Notice* involves marking RFID-tagged objects with an industry-standard label on the product or packaging. *Educating* consumers to recognise products with EPC tags will take time. According to some industry players, this will require a multimedia campaign similar to what was done with ingredient labels[54].

Choice means that consumers will be informed of the choices that are available to discard or remove or disable EPC tags from the products they acquire. On *record use, retention, and security*, the guidelines state that "the Electronic Product Code does not contain, collect or store any personally identifiable information". However, for future consumer applications that require linking EPC numbers with personally identifiable information, new forms of notice may be required.

Out of these guidelines, the issue of choice is currently complex, unless tags are on packaging which can be discarded. While EPC tag *protocols* allow the tags to be "killed", RFID readers that can both read and deactivate tags are expensive and are reportedly not 100 percent effective. One two-way reader in 2004 cost several thousand dollars[55]- multiplied by the number of checkout counters in a store across a country, this may translate into a prohibitively expensive option for some firms, and may therefore limit achieving the objective of using RFID to optimize the supply chain.

Proposed technological solutions for privacy and security

For some applications, communication protocols need to be secure; hence encryption capability is required on the transmission device. For example, through air interface encryption and mutual authentication, smart card-based wireless ID applications can be secured from ID theft or tracking[56]. However, this level of security requires more financial and managerial resources.

But most low-cost RFID devices do not have the computational resources necessary to use standard cryptographic techniques. Without encryption of data or transmission, an RFID tag transmits its unique ID number in a way that can be intercepted. Because the unique ID tends to be a random number that only points to a field in a database, this information itself may be of little value unless it is linked to other relevant information.

To address the problem of consumer privacy, some RFID vendors and users have participated in EPCglobal's development of the Gen 2 EPC tags so that they can be "killed", meaning tags can be rendered permanently inoperative at the point of sale. However, while addressing privacy concerns, "killing tags" may limit potential beneficial RFID applications for consumers, limit RFID technology diffusion and the development of innovative solutions that benefit consumers. Hence, ways of delivering both privacy and utility must be found. A significant amount of research into the area of technological solutions is going on in various fora, including the EICAR RFID Task Force[57] or research laboratories.

A number of technological solutions have been proposed aimed at balancing privacy and utility by creating means for restricting emission or processing of information[58]. Examples include the "privacy bit"[59] developed by RSA Labs, which aims to supplement the current EPC Gen 2 standard as an option for developers of technology.

Researchers with the Auto-ID Lab at the University of St. Gallen and ETH Zurich have enunciated ideas similar in spirit to the privacy bit, and have investigated both enforcement via audit devices and the relationship of their ideas to the OECD's guidelines for protecting personal information.

Another solution proposed for EPC tags is the introduction of a disable/enable mechanism that would disable all tags by default as part of the shopping check-out process and provide consumers with a password enabling them to re-enable their objects' tags if needed[60].

The approach to the RFID privacy problem proposed by Engberg, Harning and Jensen uses zero-knowledge protocols and consumer control of keys, and claims to ensure consumer privacy needs without reducing corporate value from utilising the potential of RFID[61]. This approach would allow for limiting communication of tag data to authorised readers, without revealing tag data to other parties.

To prevent consumers from unwanted scanning of RFID tags attached to items they may be carrying or wearing, several privacy-enhancing technologies (PETs) have been proposed. "Selective blocking", such as the RSA® Blocker Tag by RSA Laboratories, involves using a cheap passive RFID device that locally jams RFID signals by interrupting a standard collision avoidance protocol, allowing the user to prevent identification if desired. Other PETs include shielding RFID tags from scrutiny using what is known as a Faraday Cage—a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies) as well as active jamming of RF signals[62].

Several low strength cryptographic solutions, such hash-locks, backward-channel XORing, third-party privacy agents, and LPN authentication, have been proposed[63].

Others, such as the founders of Matrics, have proposed altogether alternative approaches to EPC Gen 2 for achieving robust RFID security. In their view, the key to RFID security being simplicity and a fundamentally secure foundation, they propose to store a random number in a read-only memory as the tag ID[64].

ANNEX 1. SOURCES

POLICY PAPERS:

US Federal Trade Commission (FTC), 2005, "RFID: Applications and Implications for Consumers. A Workshop Report from the Staff of the FTC", March– http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf

US Department of Commerce, 2005, "Radio Frequency Identification – Opportunities and Challenges in Implementation", Washington, April– www.technology.gov/reports

OECD, 2004, Digital Delivery in Distribution and Logistics, April, DSTI/ICCP/IE(2004)17/FINAL– www.oecd.org/dataoecd/19/8/34884379.pdf

OECD, 2004, Information Technology Outlook, pp. 272-274 – www1.oecd.org/publications/e-book/9304021E.pdf

OECD, 2004, The Security Economy, Chapter 4. RFID: The Concept and the Impact, OECD International Futures Programme.

European Commission Article 29 Data Protection Working Party, 2005, Working document on data protection issues related to RFID technology, January, 10107/05/EN WP 105 http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

OTHER:

National Academy of Sciences, 2004, Radio Frequency Identification Technologies: A Workshop Summary www.nap.edu/catalog/11189.html

Industry and civil society best practices.

ANNEX 2. RELEVANT OECD GUIDELINES

Box 4. Other relevant OECD Guidelines

1997 OECD Guidelines on Cryptography (selected text)

The OECD Guidelines on Cryptography outline eight interdependent principles, each of which addresses an important policy concern, which should be implemented as a whole so as to balance the various interests at stake:

1. Trust in cryptographic methods: Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.

2. Choice of cryptographic methods: Users should have a right to choose any cryptographic method, subject to applicable law.

3. Market driven development of cryptographic methods: Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.

4. Standards for cryptographic methods: Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.

5. Protection of privacy and personal data: The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods. The OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data provide general guidance concerning the collection and management of personal information, and should be applied in concert with relevant national law when implementing cryptographic methods.

6. Lawful access: National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.

7. Liability: Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.

8. International co-operation: Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

Ministerial Declaration On The Protection Of Privacy On Global Networks, 1998 (selected text)

The Governments of OECD Member Countries declare that:

They will take the necessary steps, within the framework of their respective laws and practices, to ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks, and in particular:

- Encourage the adoption of privacy policies, whether implemented by legal, self-regulatory, administrative or technological means.
- Encourage the online notification of privacy policies to users.
- Ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress.
- Promote user education and awareness about online privacy issues and the means at their disposal for protecting privacy on global networks.
- Encourage the use of privacy-enhancing technologies, and
- Encourage the use of contractual solutions and the development of model contractual solutions for online transborder data flows.

ANNEX 3. COUNTRY EXAMPLES OF NATIONAL RFID POLICIES

Table 2. Selected examples of privacy and data protection specific safeguards to the use of RFID

Italy	Provision of March 9 2005 by the Italian Garante on Safeguards applying to the use of RFID-devices: The provision requires both public and private data controllers to comply with the data protection principles set forth in the law, i.e. data minimisation; information notice; consent; purpose specification. The Italian Garante also lays down specific provisions concerning the use of RFID devices in the employment context and underskin RFID implants.
Japan	On March 30, 2004, the "Research and Study Group on the Advanced Use and Application of Electronic Tags in the Ubiquitous Network Era" of the Japanese MIC (previously MPHPT) compiled the "Guideline structure for the protection of privacy in the use of RFID tags" in the "Efforts towards the Advanced Use and Application of RFID" (final report). On March 16, 2004, the Ministry of Economy, Trade and Industry (METI) developed the "guidelines to protect privacy concerning RFID tags." Subsequently, the above-cited two ministries, MPHPT and METI, jointly compiled "Guidelines for Privacy Protection with Regard to RFID Tags" within the scope of consensus among stakeholders, including service providers and consumer groups. These guidelines were published on 8 June 2004 and have come into force, but are non-binding. The guidelines are recommended to be applied to all business activities which handle RFID tags and products with RFID tags. The two ministries will carry out awareness campaigns on the guidelines toward relevant organizations, consumers.
Korea	The Korean "RFID Privacy Protection Guideline" was finalised and published by the Ministry of Information & Communication (MIC) on 7 July 2005, but was not in force yet as of 19 September 2005. The Guideline is not mandatory but, if there are the needs for the enactment of the Guideline, the Korean Government will create legislation reflecting the Guideline. The Guideline is applicable to both the public and private sector because it is not in force. However, if it is enacted as an Act, there may be some exceptions for the public sector.

Table 3. Selected examples of spectrum regulators and main regulations for ultra high frequency (UHF) RFID

China	The frequency within the UHF band that the next-generation Gen 2 global standard will operate on (which is the 860-MHz to 960-MHz frequency) is heavily occupied by GMS and CDMA telecommunications devices. China's radio-frequency management authority is testing a number of frequencies and offering temporary licenses in the UHF band[65].
European Union	ERO, CEPT, ETSI. National administrations must ratify the usage of a specific frequency before it can be used. The European Telecommunications Standards Institute (ETSI) has published a technical standard for RFID equipment (EN 302 208) ETSI 300 328 Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with emitted radio power (by readers) of up to 2 Watt. The European Conference of Postal and Telecommunications and Administrations (CEPT) has recommended that RFID be allocated the 865-868MHz spectrum licence-free in its recommendation on Short Range Devices (CEPT/ERC/Rec 70-03).
Japan	The Ministry of Internal Affairs and Communications (MIC), the regulator in charge of spectrum management, institutionalized the high-power passive tag system using 952-954 MHz band in April 2005, and is planning to institutionalize the low-power passive tag system using 952-955 MHz band and the enhanced high-power passive tag system around February 2006.
United Kingdom	The U.K.'s Ofcom, the regulator in charge of spectrum, published on 9 August 2005 draft regulations[66] covering RFID, recommending that RFID equipment in the 865-868 MHz band be exempt from wireless telegraphy licensing. These are open to public comment until 12 September 2005.
United States	The Federal Communications Commission (FCC) authorises the 902-928 MHz frequency bands for unlicensed Industrial-Scientific-Medical (ISM) devices. Requirements specify the maximum power output.

GLOSSARY

AIDC	Automatic Identification and Data Capture
Auto-ID Labs	Auto-ID Center was a non-profit collaboration between private companies and academia that pioneered the development of an Internet-like infrastructure for tracking goods globally through the use of RFID tags carrying Electronic Product Codes. The center closed its doors in September 2003. EPCglobal was set up to continue the work of commercializing EPC technology, and the center's research work is carried on by Auto-ID Labs at universities around the world.
CEPT	European Conference of Postal and Telecommunications Administrations
CRM	Customer Relationship Management
DHS	U.S. Department of Homeland Security
DNS	Domain Name System
DOI	Digital Object Identifier
DoD	U.S. Department of Defense
EAN	European Article Number
EAN International	The European bar code standards body
EPC	Electronic Product Code
EPCGlobal	A non-profit organization set up the Uniform Code Council and EAN International, the two organizations that maintain barcode standards, to commercialize EPC technology. EPCglobal is made up of chapters in different countries and regions. It is commercializing the technology originally developed by the Auto-ID Center.
ERO	European Radiocommunications Office
ERP	Enterprise Resource Planning
ERP	Emitted Radio Power
ESTI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communication
HF	High Frequency
IANA	Internet Assigned Numbers Authority
ICT	Information and Communications Technologies
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
NFC	Near Field Communication
ONS	Object Name System
PDA	Personal Digital Assistant
PET	Privacy Enhancing Technologies

GLOSSARY
(Cont'd)

PML	Physical Markup Language
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
ROI	Return On Investment
TCP	Transmission Control Protocol
UID	Unique Identifier/Identification
UCC	Uniform Code Council
UHF	Ultra-high frequency: from 300 MHz to 3 GHz (typically, RFID tags that operate between 866 MHz to 960 MHz)
UPC	Universal Product Code
URL	Uniform Resource Locator
WAN	Wide area network
WEEE	Waste Electrical and Electronic Equipment Directive
WLAN	Wireless Local Area Network

NOTES

1 Passive tags generally range from 20 cents when purchased in high volume to several dollars when embedded in key fob or plastic housing for protection. Active tags range from USD 10 to USD 50 or more, depending on the size of the battery, the amount of memory on the microchip and the packaging around the transponder. UHF readers range in price from USD 500 to USD 3 000, depending on their functionality. http://www.rfidjournal.com/article/articleview/1336/1/129/

2 Research and Markets, RFID Industry— A Market Update, June 2005, http://www.researchandmarkets.com/reports/c20329

3 International Organization for Standardization.

4 EPC global is a joint venture between EAN International and the Uniform Code Council. Industry-led, its members include Gillette, METRO AG, Novartis Pharma AG, Proctor and Gamble, Unilever, Target, Carrefour, Tesco, Kimberly Clark, Cisco Systems, Hewlett-Packard among others, and universities, such as the Massachusetts Institute of Technology.

5 OECD, 2004, Information Technology Outlook 2004, pp. 272-274.

6 OECD, 2004, The Security Economy, Chapter 4. RFID: The Concept and the Impact, OECD International Futures Programme.

7 However, a distinction is often made between RFID and contactless smart cards, see http://www.smartcardalliance.org/pdf/alliance_activities/rfidvscontactless_final_121704.pdf for example.

8 Electronic Article Surveillance – EAS, a system applied in shops in many countries since the 1960s.

9 http://www.vnunet.com/vnunet/news/2124563/nokia-brings-rfid-mobile-phones

10 Merloni Unveils RFID Appliances, April 4, 2003, http://www.rfidjournal.com/article/view/369/1/1/

11 http://www.rfidjournal.com/article/articleview/1332/1/129/

12 Toensmeier, Patrick, Plastics Engineering, February 2005, As RFID Applications Increase, Suppliers Look To Lower Its Cost

13 http://www.reed-electronics.com/electronicnews/article/CA6261023.html?industryid=21376

14 Toensmeier, Patrick, Plastics Engineering, February 2005, As RFID Applications Increase, Suppliers Look To Lower Its Cost.

15 Report by AMR Research and ABI Research.

16 Elizabeth Board, EPCGlobal, conversation of 25 July 2005.

17 http://www.fda.gov/bbs/topics/news/2004/NEW01133.html

18 http://www.nal.usda.gov/fsrio/research/fsheets/fsheet12.htm

19 Product Recalls Pushing RFID, E-week, August 16, 2004, http://www.eweek.com/article2/0,1895,1636342,00.asp

20 Customs-Trade Partnership Against Terrorism (C-TPAT) run by U.S. Customs and Border Protection, a DHS component.

21 ABI Research, 2004, Electronic Container Tracking White Paper.

22 ABI Research, 2004, Electronic Container Tracking White Paper.

23 Roberti, Mark, RFID's Case of Schizophrenia, 1 August 2005 http://www.rfidjournal.com/article/articleview/1762/1/128/

24 Gaughan, Dennis, "RFID Technology Assessment 2005-2007: Where Is the ROI?", July 20, 2005

25 http://www.rfidjournal.com/article/articleview/219#Anchor-Won't-6296

26 National Academies of Science, 2005, Radio Frequency Identification Technologies: A Workshop Summary, January.

27 http://www.amrresearch.com/Content/View.asp?pmillid=17856&docid=12118

28 http://www.rfidjournal.com/article/articleview/1684/1/82/

29 Garfinkel, S. and Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, Chapter 27, P&G: RFID AND PRIVACY IN THE SUPPLY CHAIN, Sandy Hughes.

30 ABI Research, 2004, RFID Middleware Market Competition Heats Up, February.

31 Jim Crawford, an analyst at Retail Forward in Columbus, Ohio, http://www.dmreview.com/article_sub.cfm?articleId=1035524

32 ABI Research, 2005, Multi-Site Active & Passive RFID Deployments Drive Demand for Better Network Management Solutions, 28 April -- http://www.abiresearch.com/products/insight/Multi-Site_Active_and_Passive_RFID_Deployments_Drive_Demand

33 http://www.rfidgazette.org/2005/07/union_wants_eur.html

34 For instance Katherine Albrecht, a vocal opponent to RFID, Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID, forthcoming.

35 Garfinkel, S.L.; Juels, A.; Pappu, R., RFID privacy: an overview of problems and proposed solutions, Security & Privacy Magazine, IEEE, May-June 2005, pp 34- 43.

36 The aim was to create a single, global standard that would be more closely aligned with ISO standards.

37 Garfinkel, S. and Rosenberg B., 2005, RFID Applications, Security, and Privacy, Chapter 31: Asia: Billions Wake Up to RFID, Bimal Sareen.

38 http://www.informationweek.com/story/showArticle.jhtml?articleID=60405010&tid=5978 and http://www.bdachina.com/content/en/features/analyses/B1122966499/

39 Intermec holds some 140 critical patents related to RFID technology.

40 Week of 15 August 2005.

41 PML simplifies the exchange of data between companies.

42 Including Burt Kaliski from RSA Security, http://www.theregister.co.uk/2005/02/18/rsa_rfid/

43 Namely, access, rectification and deletion.

44 Christian Floerkemeier, Roland Schneider, Marc Langheinrich, 2004, Scanning with a Purpose - Supporting the Fair Information Principles in RFID protocols, Institute for Pervasive Computing, ETH Zurich, Switzerland.

45 http://www.nap.edu/books/0309095433/html/21.html

46 http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf. The public consultation was closed end of March, 2005.

47 In particular the data protection Directive (Directive 95/46/EC of 24 October 1995) and the Directive on privacy and electronic communications (Directive 2002/58/EC of 12 July 2002).

48 Garfinkel, S. and Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, Chapter 4, RFID and Global Privacy Policy, Stephanie Perrin.

49 The term "data controller" is defined in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as 1. a) "data controller" means a party who, according to domestic law, 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"

50 Cf. table 1 in annex 3.

51 Cf. table 1 in annex 3.

52 "Maryland, Utah, and Virginia have introduced bills designed to study the issue in more depth and to provide recommendations for future legislation. Missouri and Utah have introduced legislation that would require all products containing RFID tags, to be appropriately labelled. Utah has introduced another bill that requires instructions to be provided on how to disable the RFID tag, or a notice that the tag will remain active after purchase. New York, Virginia and Washington also have introduced bills that make personally identifiable information collected by automatic toll systems (like EZ-Pass) confidential. In California, proposed legislation regulating the use of RFID technology required businesses using RFID systems to 1) tell customers it is using an RFID system, 2) get express consent before collecting information, and 3) detach or destroy RFID tags attached to products before customers leave the store." None of these proposals has been passed into law yet. Source: Department of Commerce: "Radio Frequency Identification – Opportunities and challenges in implementation", Washington D.C, April 2005, p. 36 – www.technology.gov/reports/. Legislation proposed by Senator Joe Simitian on RFID may be enacted in California in September 2005. Simitian's bill, SB682 (http://www.etopiamedia.net/empnn/pdfs/sb682-1.pdf) would set standards for use of RFID technology by public agencies in California.

53 http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html

54 Garfinkel, S. and Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, Chapter 27, P&G: RFID AND PRIVACY IN THE SUPPLY CHAIN, Sandy Hughes.

55 Garfinkel, S. and Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, Chapter 27, P&G: RFID AND PRIVACY IN THE SUPPLY CHAIN, Sandy Hughes.

56 Cf. e.g. the ICAO "Basic Access Control" scheme foreseen as an option for the use of RFID technology in machine-readable passports, which is meant to prevent skimming (i.e. electronically reading the document without the person that has control over the document noticing) as well as eavesdropping on the communication between an RFID chip in a passport and an authorized reading device (through encrypting the data during transmission), in: Machine readable travel documents – Technical Report – PKI for Machine Readable Travel Documents offering ICC read-only access, ICAO-NTWG PKI Task Force, Version 1.1, 1 October 2004, http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf

57 http://www.eicar.org/rfid/information_material.htm

58 Garfinkel, S.L.; Juels, A.; Pappu, R., RFID privacy: an overview of problems and proposed solutions, Security & Privacy Magazine, IEEE, May-June 2005, pp 34- 43.

59 http://www.rsasecurity.com/rsalabs/node.asp?id=2115, Research Papers from RSA Labs

60 Cf. Spiekermann, S., Berthold O.: Maintaining privacy in RFID enabled environments - Proposal for a disable-model, in: Robinson, Philip; Vogt, Harald; Wagealla, Waleed (Eds.): Privacy, Security and Trust within the Context of Pervasive Computing. Series: The International Series in Engineering and Computer Science, Vol. 780 http://www.wiwi.hu-berlin.de/~sspiek/SPPC_spiekermann-edited.pdf

61 Cf. Stephan J. Engberg, Morten B. Harning, Christian Damsgaard Jensen: Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience. http://www.obivision.com/Papers/PST2004_RFID_ed.pdf

62 Three instances of "smart RFID-tag" approach, that have been proposed, are the hash-lock method, the re-encryption method (in several forms), and silent tree-walking. For more information, see Garfinkel, S. and Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, Part IV Technical Solutions.

63 Including hash-locks, backward-channel XORing, third-party privacy agents, and LPN authentication.

64 Garfinkel, S. and Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, Chapter 22, Randomization; Another Approach to Robust RFID Security, Michael Arneson, William Brandy.

65 http://www.informationweek.com/story/showArticle.jhtml?articleID=60405010

66 http://www.ofcom.org.uk/consult/condocs/wireless865_868/wireless865_868.pdf