JRC Scientific and Technical Reports

RFID Technologies: Emerging Issues, Challenges and Policy Options

Authors: Marc van Lieshout, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij, Claudio Borean.

Editors: Ioannis Maghiros, Paweł Rotter, Marc van Lieshout

EUR 22770 EN - 2007

JRC EUROPEAN COMMISSION

Institute for Prospective Technological Studies

The mission of the IPTS is to provide customer-driven support to the EU policy-making process by researching science-based responses to policy challenges that have both a socio-economic and a scientific or technological dimension.

European Commission
Joint Research Centre
Institute for Prospective Technological Studies

Contact information

Address: Edificio Expo. c/ Inca Garcilaso, s/n. E-41092 Seville (Spain)
E-mail: jrc-ipts-secretariat@ec.europa.eu
Tel.: +34 954488318
Fax: +34 954488300
http://www.jrc.es
http://www.jrc.ec.europa.eu

Legal Notice

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server
http://europa.eu/

JRC PUBSY 6957

EUR 22770 EN
ISBN 978-92-79-05695-6
ISSN 1018-5593

Luxembourg: Office for Official Publications of the European Communities

Printed in Spain

Institute for
Prospective
Technological Studies

RFID Technologies:

Emerging Issues, Challenges and Policy Options

Institute for Prospective
Technological Studies

2007

JRC
EUROPEAN COMMISSION

EUR 22770 EN

Acknowledgements

Editors:

Ioannis Maghiros, European Commission – DG JRC – IPTS
Paweł Rotter, European Commission – DG JRC – IPTS
Marc van Lieshout, TNO

Authors:

Marc van Lieshout, TNO
Luigi Grossi, Telecom Italia
Graziella Spinelli, Telecom Italia
Sandra Helmus, TNO
Linda Kool, TNO
Leo Pennings, TNO
Roel Stap, TNO
Thijs Veugen, TNO
Bram van der Waaij, TNO
Claudio Borean, Telecom Italia

Other Contributors:

Other experts participating in the validation workshop which took place on 3 October 2006 in Amsterdam:

Gaynor Backhouse, Intelligent Content, UK
Ruud Beugelsdijk, College Bescherming Persoonsgegevens, The Netherlands
Massimo Bolchini, INDICOD, Italy
Paula Bruening, Center for Democracy and Technology, USA
Lew Claiborne, RF SAW Inc., USA
Bruno Crispo, Free University Amsterdam, The Netherlands
Florent Frederix, European Commission
Richard Foggie, Department of Trade and Industry, UK
Jeroen van den Hove, Technical University of Delft, The Netherlands
Britta Oertel, Institut for Zukunftstudien und Technologiebewertung, Germany
Bart Schermer, ECP.nl and RFID Platform, The Netherlands
Jeroen Terstegge, Royal Philips BV, The Netherlands
Daniel Tijink, Department of Economic Affairs, The Netherlands

Table of contents

List of figures

List of tables

List of boxes

Executive summary

Radio Frequency Identification (RFID) technology, an enabling technology for automatic identification based on radio waves, will impact the daily lives of European citizens in many different ways. Minuscule devices, called RFID tags are attached to objects and emit information which aptly positioned readers may capture wirelessly. Such tags and readers come in various shapes and forms, have technological capabilities that can open up new application areas and are already in use to improve efficiency and reliability. They also facilitate the coupling of the physical reality to the virtual world, infusing it with digital functionality and triggering the move towards the so called Knowledge Society.

The technology is complex but mature enough for immediate deployment. However, due to its enabling character, it is still under constant evolution – as is evidenced by the increasing number of RFID related patents (65% increase in 2004). The RFID market is still in its infancy with most applications not being large-scale and the forecasted economic benefits (Return-on-Investment) still unclear. However, the technology providers' market for RFID is global and Europe houses a few of the world's strongest RFID suppliers. At the same time the end-user market is specialised in diverse application areas, mainly local and usually dependent on emerging opportunities in the public sector domain. Technology Consultants IDTechEx predict that in 2007 a total of 1.7 billion tags will be sold and that the global RFID market value (including all hardware, systems, integration etc) will be 3.8 billion Euros, rising to 21,3 billion Euros by 2017[1].

Many Europeans already use RFID-equipped cards to access, for instance, their work premises or pay for their public transport fare. The technology is also successfully used for animal tagging, in order to protect the consumers from a host of animal diseases or help them trace their lost pets, and as anti-fraud protection in luxury items. RFID technology is forecasted to spread rapidly over the next decade as soon as tag costs fall enough to allow item-level-tagging. In addition to private sector activities, there are ongoing initiatives both at European and Member State level which demonstrate, on the one hand, an overall comparable activity to that of the US but on the other considerable differences (in magnitude and speed of uptake) among EU countries. Early adopters are expecting to gain considerable experience on which they anticipate commercial profits, while laggards hope to be able to avoid 'teething problems'.

However, the massive adoption of RFID introduces challenges such as concerns over possible eavesdropping over the air interface or over the potential danger of privacy abuses as a result of the ubiquitous, silent and invisible character of the technology. The European Consultation process (over 2000 participants) highlighted the fact that inadequate privacy safeguards will impact acceptance of RFID negatively; trust is thus a major issue. There are also other issues to be addressed at European level: those related to raising consensus on standards, achieving cross-border and cross-sector interoperability and adequate spectrum allocation in order to increase the agility of the market. It is very important for Europe to be prepared for rapid deployment in RFID and also to implement initiatives which will allow European citizens to benefit from this new technology while avoiding the risks it carries.

Objective and scope of the RFID study

A study on "RFID-Technologies: Emerging issues, Challenges and Policy options" was commissioned by the European Commission's DG Joint Research Centre, Institute for Prospective Technological Studies (DG JRC-IPTS) to further investigate RFID technologies and their socio-economic implications. The study looked at technological, market, societal and legal issues so as to identify and analyse barriers and oppor-

[1] Data published at: *http://www.the-infoshop.com/study/ix49177-rfid.html*

tunities for Europe, in order to propose policy options focussing on European citizens' needs. The summary that follows presents the major policy options proposed, a European SWOT analysis, the main issues analysed and the structure of the report that follows.

European SWOT for RFID deployment

The study has identified, mainly through the analysis of the specific application areas, related strengths, weaknesses, threats and opportunities for Europe. Although, it is unlikely that all EU countries will be able to equally benefit from item-level-tagging applications due to the diversity in the structure of their manufacturing sectors, it is expected that they will all be able to profit from human-centred applications. In health, public transport and animal tracking areas, RFID enable the alignment of information processes that allow considerable efficiency gains and improved end-user convenience (e.g. increased safety in the sensitive health area, more efficient supply and use of public transport means, locating animals). Law enforcement is driving RFID take up in animal tracking and more secure travel documents and RFID is expected to have a positive impact on national security and the fight against terrorism. The table below summarises the findings:

Strengths	Weaknesses
- Europe houses part of the big RFID suppliers;	- Many European countries with only marginal attention for RFID;
- High market potential;	- No level-playing field for RFID across countries;
- Leading EU countries with RFID focused attention (UK, France, Germany, The Netherlands, Italy);	- No harmonised frequency policy in the EU;
- Focus of attention comparable to USA.	- Vulnerable image of RFID - Trust issue.

Opportunities	Threats
- Increasing efficiency of production, trade and services;	- High initial and high transition costs;
- Creation of new services, new workplaces;	- Rapid technological evolution may help displace a technology before it is widely adopted;
- Spur for economic development	- High hidden costs (societal and organisational such as for training and education);
- Increased convenience in citizens' everyday life;	- Possible job losses due to wide deployment;
- Increased security, reliability and trust;	- If not implemented properly, RFID may bring a number of threats to privacy and security (Function creep, surveillance capacity).
- Stimulation of research and development of related technologies (enabling, enhancing and concurrent).	

On the other hand, market integration seems to be the first challenge for Europe to tackle while balancing the efficiency gains for businesses with the perceived benefits for citizens emerges as the next challenge. However, Europe's responsibility goes beyond achieving very low cost tags which would enable a future where item-level-tagging is possible; the opportunity comes from developing high-end, added-value market applications promising accurate and actual data-based quality, improved personal safety and security and extensive convenience. The biggest opportunity for Europe in embracing this technology seems to be the realisation of the vision of an integrated physical and virtual world life where RFID technology is the ubiquitous, always-on, seamless bridge to and from both worlds.

Emerging issues and challenges

With RFID out of the laboratory and into the mainstream of business and society, a debate as to the likely and desired implications of the technology on the socio-economic fabric should take place. The study identified a lot of opportunities but also challenges that need to be openly debated. To begin with, the study identified many technical challenges (e.g. in developing advanced RFID tags, linking to wireless networks, merging with sensor devices, improving reliability, setting standards, and testing and certification) and some market ones (e.g. high initial investment costs, uncertainty as to which standards or which technologies will persist, adoption issues as a result of low trust, etc…). Nevertheless, the study would like to draw attention to a number of issues for which consensus will be needed before decisions on the scope and the focus of future initiatives may be taken. Some of them are described below:

1. Currently, a major drawback to wide-spread deployment of RFID systems is the overall attitude of people towards them. In general today, **social acceptance and trust of RFID** is quite low – as a result of insufficient privacy and security safeguards and also the lack of awareness – and may impede take up of RFID technology. However, it is not sufficient to make the technology secure and reliable. The perception of security depends on the individual's reaction to both the risks and the countermeasures adopted. Individuals will need to be appropriately educated if their perceptions are to closely match deployed RFID security reality.

2. **Ethical issues** are also at stake (e.g. over the use of RFID implants) and the development of European good ethical practice is a first step towards addressing them. Due to the complexity of advanced RFID systems, a process needs to be defined which will identify and counter emerging security and privacy threats, prior to the deployment of RFID systems.

3. The foreseen wide-spread use of RFID applications and its enabling capacity raise various **security and privacy concerns**. Most of them are being dealt with through improved technological design, taking into account security and privacy throughout the value chain and also by judging the sensitivity of the case to security and privacy issues. Various initiatives, at EU level, to tackle RFID privacy and security concerns already exist; for example, the Article 29 Working Party has expressed its views on minimising data collection and preventing unauthorised forms of processing through improved use of the technology. However, it is the appropriate mix of self-regulation, through the creation of codes of conduct and of legislation that would need to be enforced that is at the heart of the debate on further initiatives required.

4. The **impact on employment** is not clear and should be monitored. Pessimistic forecasts say that deployment of RFID technology may result in about 4 million job losses (over a 10 year period in the US). However, no major disruption of the labour market is expected, apart from the forecasted shortage of skilled professionals which will impact rapid deployment. Moreover, RFID will create new jobs, related to data processing and service-related jobs and the overall resulting economic growth may also contribute to the creation of additional workplaces. It is clear that training activities will be needed as new kinds of skills will be required both for professional workers (development) and end-users (customisation).

5. High initial costs for setting-up RFID systems, uncertainty on the future of the most promising technologies of today, the lack of well established standards and finally hidden societal, and organizational costs (e.g. training) are well-known **barriers for smaller companies** which are reluctant to adopt the technology.

6. Dependability of RFID information systems, especially in sensitive application areas such as health, signals the need to design appropriate **fallback procedures** in case there are system failures. This obviously adds to the costs of deployment and represents yet another barrier.

7. There is a clear **gap between leaders and followers** in RFID adoption in Europe. This may limit the foreseen benefits of a larger European market and constrain the development of high-end applications which promise to enable a new generation of services for citizens. Moreover, closing the gap has positive growth implications as 'local' European firms will play an important role in the challenging ICT transformation processes that RFID brings.

8. The direction a European harmonized frequency policy should take is still under debate. However, the question as to whether **reserved spectrum bandwidth** in the EU will be sufficiently large for future applications is already important. For comparison purposes, the US administration has reserved bandwidth that is 10 times larger.

9. As a result of the wireless and invisible nature of RFID information exchange enhanced **testing and certification** procedures are needed in order to ensure that, for example, requirements concerning privacy and security are fulfilled (e.g. kill command works according to specification). A vendor-neutral solution to the establishment of certification of providers, approved system integrators, RFID consultants and trainers is needed.

10. Although there are many available technical standards (ISO, EPCGlobal), **semantic interoperability** is also needed so as to allow the structured exchange of information in RFID-based systems as information is application specific. This type of standard would increase usability of information stored on tags and produced by sensor networks. Insufficient semantic interoperability of RFID systems may restrict benefits from their deployment, especially for globally operating systems.

11. RFID systems produce a lot of data locally and collision avoidance is a practical requirement that needs to be addressed. Advanced RFID systems, serving geographically distributed needs, generate **huge amounts of data** which are difficult to manage in real time and which are expected to create a new burden on the global network infrastructure; especially when the system architecture foresees centralised data storage. Moreover, in today's complex business processes where the value chain is composed of different companies, issues related to data ownership, control and liability will need to be addressed.

Proposed policy options

The study looked at a number of RFID issues in general and also focused on the analysis of five selected application areas (animal tagging, healthcare, public transport, identity documents and the ICT sector) where implementation in Europe is well advanced, in order to draw conclusions as to what is at stake for Europe. As technological evolution is continuous, achieving a balance between reaping the benefits and avoiding the pitfalls associated with its implementation is inevitably a moving target. Given the enormous socio-economic potential of this particular technology, a debate on what role Europe should play in this areas has been launched. Whatever the result of this debate, Europe ought to tread a fine line between issues that are considered to be of vital importance for the market players, and the interests of the citizens. Moreover, the EU should take up this opportunity to drive the realisation of the vision of a European Information Society where services integrating the real and the virtual worlds are on offer.

Bearing in mind that there are various intervention instruments (technological, legal, or through stimulation of self-regulation) at the disposal of the policy maker, the study presents the following policy options:

1. Europe will benefit from stimulating cross-border take up of RFID applications primarily through setting-up a harmonised frequency policy and then through stimulating consensus on standards and interoperability issues. Moreover, promotion of best practice, financial support of cross-border pilot and trial programmes, and fostering SME participation in the area will contribute to helping fight market fragmentation and bringing all EU Member States closer to the European Information Society vision.

2. The Internet of Things (the billions of tagged objects that will enable access to back-end information systems) will require a service for registering and naming identities, the Object Name Service (ONS), which should be interoperable, open and neutral to particular interests. Europe should position itself in the appropriate international fora to exercise its responsibilities in this area.

The report has also identified the need to establish a debate on RFID in Europe as well as the need for further technological and legal research as primary recommendations for action.

1. European society needs an information campaign on RFID systems to raise awareness as to the likely benefits and possible risks of the wide-spread application of this technology. A debate should also be launched with a view to making the preferred and ethical use of the technology more explicit to all.

2. A closer look at the existing legal framework is deemed essential. Further study is also needed to develop a process for establishing guidelines and best practices which aim to build safeguards against emerging RFID risks.

3. As a result of the enabling character of the technology and its multi-sensor data integrating capabilities, there is a clear need for further technological research to improve efficiency, robustness and security. More research will be needed into:

   a) advanced tag-reader systems;

   b) the enhancing of security and 'privacy by design' for complex applications;

   c) the impacts of almost permanent exposure to very low intensity radio waves produced by ubiquitous always-on RFID devices;

   d) the re-skilling of the professional population to foster market expansion;

   e) how to foster creativity and innovation spirit to help create additional and more advanced links between the physical and the virtual worlds.

Preface

This report is the result of a study on RFID, commissioned by the Institute of Prospective Technology Studies (IPTS), of the Directorate General Joint Research Centre (DG JRC) of the European Commission. The objective of the study is to inform the policy process within the European Union on the socio-economic and technological developments taking place with respect to RFID, analysing prospects and barriers to RFID technologies, and the broader technological, economic, social and legal challenges, to come to a well-founded set of research and policy recommendations. The scope and detailed specification of research has been prepared by IPTS. The study has been performed by two research organisations: TNO (The Netherlands) and Telecom Italia (Italy) in cooperation with IPTS, between December 2005 and January 2007. During this period, the European Commission has organised an open public consultation process on RFID and issued a communication on the subject.

The study has been clustered around a number of research challenges:

- the presentation of a state of the art overview regarding RFID technologies, the relation of RFID technologies with a broader set of ICTs (existing and emerging networks), the analysis of the state-of-the-art concerning frequency allocation and standards, and an analysis of usage typologies of RFID;
- the analysis of market perspectives and socio-economic aspects; the latter were narrowed down to aspects concerning users and trust relations, privacy and security;
- the analysis of the introduction of RFID in a number of application areas; the application areas chosen were: the use of RFID for animal tagging, the use of RFID in the health sector, the use of RFID within the ICT-sector itself, the use of RFID in identity cards, and the use of RFID within public transport systems; this was a deliberate choice, given the surplus of attention for and information about RFID within logistic processes;
- the analysis of the results of the previous steps in terms of policy relevance and the formulation of policy recommendations.

To validate the findings of the project team, a validation workshop has been held on October 2006. The results of the validation workshop have been used to enrich and complement the report.

Many authors have contributed to make this report possible. Marc van Lieshout was overall project leader of the project. More in detail: Marc van Lieshout has written chapters 8, 10, 11 and 16 and together with Sandra Helmus chapter 15; Luigi Grossi has written chapters 4 and 6 and together with Claudio Borean chapters 2 and 3; Graziella Spinelli has written chapters 12 and 13; Leo Pennings has written chapter 14 and together with Linda Kool chapter 7; Thijs Veugen has written chapter 9; and finally chapter 5 was written by Roel Stap and Bram van der Waay.

Structure of the report

The report that follows is composed of four parts. The first part details the technological dimension of RFID systems including the situation on standards and spectrum allocation. The second part presents RFID market parameters and raises socio-economic issues. The third part presents five case studies from different application sectors and draws conclusions as to the specific areas of development as well as for the whole RFID market in Europe. The last part analyses the situation and presents recommendations for further initiatives in Europe. The contents of the first four parts are presented in more detail below:

Part 1: RFID technologies

The state-of-the-art in RFID technology is presented as well as other technologies which: (i) enable RFID usage (e.g. Ethernet or Bluetooth); (ii) enhance it by adding further functionality to basic RFID capabilities (like Near-Field-Communication (NFC) or functionalities offered by middleware); (iii) are competing with it (such technologies are divided into those which enable identification, location or information on state).

The report provides a prospective analysis of alternative tagging technologies, which may replace RFID in the future, like Surface Acoustic Waves, optical tags or DNA tags. It also describes technological limitations of RFID (for example, those resulting from the physical properties of radio waves) and possible solutions to these problems.

The currently available spectrum allocation and frequency regulatory status for using RFID in the EU and world-wide is presented, as well as a description of the most common standards on the market (EPC Global, ISO and ETSI).

The first part ends with a proposal for a typology of RFID applications, which considers business use criteria as well as the sensitivity of application areas in terms of privacy protection. It uses this typology to draw conclusions about the drivers for further development of intelligent applications facilitating global collaboration and automation.

Part 2: Market perspectives and socio-economic issues

The main forces driving the RFID market evolution are presented in an inventory which provides information about the main actors on the global RFID market, such as tag manufacturers, system integrators, software providers and consultants. It also provides web links to their sites. This is followed by an analysis of the RFID market showing that the change of application profile is largely driven by the tag price. Application areas where a relatively high tag price is acceptable (e.g. e-documents, e-payment, access control) have already been developed, and in the next few years the rapid development of applications demanding low-cost tags, (e.g. asset management, supply chain and retail logistics) should be expected.

The pros and cons of RFID usage are analysed from both the retailer's and the user's perspective. Lack of regulation for spectrum allocation in some countries, limitations of technology (e.g. interference of radio signal with metals and water), possible carriers for SMEs (e.g. high initial investment) and forecasts of impact of RFID on employment and likely implications are also presented.

Finally, an exhaustive analysis of privacy and security challenges are also included. Privacy threats, like 'sniffing' the tag information, using tags to track a person, function creep and strategies to counter them are analysed. Threats to security and countermeasures are also discussed as is a methodology of security evaluation, based on the relation between the costs of attack and the cost of countermeasures.

Part 3: Case Studies of RFID implementation

Five application areas were selected to describe state-of-the-art deployment in Europe of RFID technology: animal tagging, healthcare, public transport, identity cards and the ICT sector itself. Analysis in the respective areas is organised around key criteria such as: drivers/barriers, threats/opportunities, role of stakeholders including Member State governments, the technology involved and the likely role for Europe as a whole. The in-depth analysis of such criteria helped determine the drivers and barriers for future RFID usage, the stakeholders' perspectives on the identified drivers and barriers and the perceived European market potential and length of time to adoption. The main issues shaping the policy evaluation include the diversity in stakeholder strategies due to variations in Member State markets and structure of the economy, the perceived EU-wide benefit and the role of the public sector in helping to achieve these benefits.

For each of these application areas conclusions as to future developments of RFID systems are drawn and presented briefly below:

- *Animal tracking* is potentially a huge market segment. The overarching incentive for the introduction of animal ID is that it would enable quick response in animal disease crises (e.g. Foot and Mouth Disease, or Avian influenza). Barriers and opportunities for further development are presented.

- In *healthcare,* RFID may be used to track medicines, prevent patients from taking the wrong drugs or track hospital assets. This would prevent theft and allow optimal usage of equipment. RFID may also be used for patient identification and localisation (e.g. in a crowded environment). In general, RFID can considerably improve performance and reduce costs of healthcare but it also creates new challenges.

- RFID is already used in the area of *public transport*. RFID-based tickets and public transport cards increase efficiency and convenience and are well received by the users. Main barriers are the massive financial investments and the high complexity of such systems leading to costly down-times.

- In the area of *identity cards,* the main driver for RFID use was the need for increased security (e-passport) in the fight against terrorism. Today, both security and privacy concerns drive further technology improvements. Perhaps, the more positive reaction of consumers towards contactless credit cards is a hopeful message indicating future acceptance likelyhood.

- In the *ICT sector,* many companies have started to explore ways to manage and track assets in the ICT department in order to optimize professional personnel work. NFC technology is forecasted to spread widely with its incorporation in mobile devices to be used in contactless payments or contact-less ticketing. No significant barriers to RFID deployment in this sector are foreseen.

Part 4: Policy analysis and recommendations

Finally, the report presents an analysis of all data presented. This leads into conclusions and recommendations which aim to address a number of overarching questions and thus set the basis for a debate in Europe on RFID applications. The impact on EU market integration and what role the public sector plays in stimulating and supporting the realisation of EU-wide benefits is discussed. Research initiatives are also discussed and proposed in this section. In essence, the report proposes a way through which Europe may stimulate initiatives to address the issues presented and thus reap the foreseen benefits of the wide-spread deployment of RFID technology.

Annexes

The report has a number of annexes which present:

1. List of references
2. List of acronyms
3. A word-wide inventory of regulatory status of RFID in the UHF spectrum;
4. A description of selected guidelines and code of practices regarding the implementation and use of RFID technologies;
5. An overview of European activities in e-passports
6. An overview of European activities in other type of e-documents (national ID cards, electronic signature cards, healthcare identity cards, electronic documents for social insurance)
7. RFID in European projects related to public transport
8. Statistics of RFID pilots and trials within the EU and the US divided by application areas.
9. Full table of contents to facilitate reading and procedural and organisational details of this fairly complex process.

Part one

RFID technologies

Institute for Prospective Technological Studies

1. RFID technologies: system features and future technologies

1.1. Introduction

RFID stands for Radio Frequency Identification. The main goal of an RFID system is to carry data on a transponder (tag) that can be retrieved with a transceiver through a wireless connection. The ability to access information through a non-line-of-sight storage in a tag can be utilized for the identification of goods, locations, animals, and even people. Discerning specific information from these tags will have profound impacts on how individuals in commerce and industry keep track of their goods and each other. Early use of this technology concerned the evolution of barcode applications, changing the application scenario perspective (the main differences with barcodes will be investigated in Section 1.2.4).

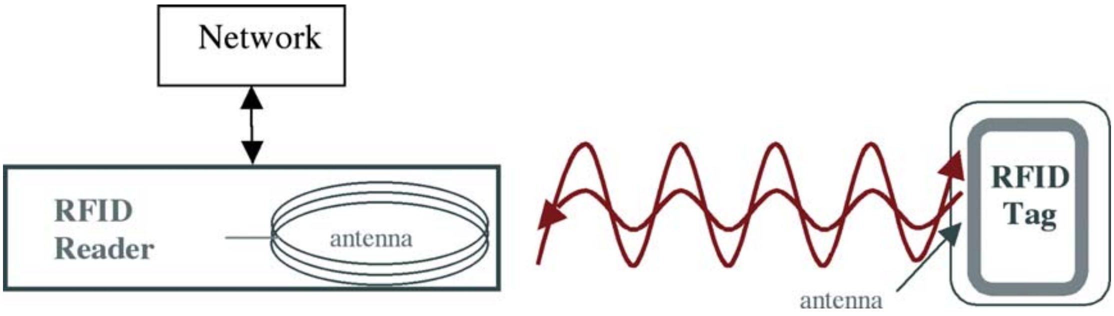
The acronym RFID, Radio Frequency IDentification, encompasses a number of technologies usable to identify objects by means of radio waves. The origin of the technique is the “Identification Friend or Foe” IFF system used in World War II by the Royal Air Force, that was able to get a code back only from “friendly” aircrafts identified with RADAR. Under this very wide umbrella the term is today mainly referring to systems where electronic equipment can “read” information from a multitude of “tags” by means of radio waves. The RFID tag can come in various shapes e.g. as a paper sticker, just as barcode tags are, as a plastic Credit Card, or even as a rugged, chemicals and heat resistant, plastic capsule. The tag might be even powered by a very small battery to support local functions such as storing temperature readings or enhancing the reach of the radio communication.

Although RFID is a mature technology, it took several years for a large scale implementation to occur. The first ones were in the United States. The implementation eventually included supply chain, freeway toll booths, parking areas, vehicle tracking, factory automation, and animal tagging. The most common application of RFID technology today is for tracking goods in the supply chain, tracking assets, and tracking parts from a manufacturing production line. Other application areas include the control of access to buildings, network security, and also payment systems that let customers pay for items without using cash.

Nevertheless some technology related issues still condition the possible applications. As an example, liquids, water especially, absorb radiations while metals reflect it. This means that passive tags applied to bottles of water or to aluminium cans can be hardly read though placed very carefully with respect to the reader antenna and with dielectric support. This is due to the properties of the radiations in relation to their wavelength It is true for HF tags but even more relevant for UHF tags.

The three basic components of a typical RFID system are an antenna or coil, a transceiver (reader with decoder), and a transponder (RFID tag) with electronically programmed information. In an RFID system, an antenna continuously emits radio signals at a given frequency. When a transponder (that is set to detect that specific frequency) comes into contact with these signals, the badge is activated and communicates wirelessly with the reader through the modulation of transmittance frequencies. Through the use of an antenna, the information that is stored on the transponder can be read or written from the transponder. Typically, the antenna is packaged with the transceiver into a larger structure called a reader (interrogator) that is in charge of the system’s data communication and acquisition. The data that is obtained and analyzed by the reader can then be transported to a computer. The general design of a simple RFID system is displayed through the following figure:

Figure 1-1: Diagram describing operation of the RFID system.



A very important feature of the reader is the capacity to avoid collisions among the RFID tags using specific methods. By using collision avoidance a reader can perform multiple readings accelerating the overall reading process in comparison with barcode systems. The performance of collision avoidance systems are evaluated in number of readings per seconds. The typical collision avoidance systems are based on Aloha and slotted Aloha process,[2] well known in literature. The use of an efficient collision avoidance system is essential to calculate the data transmission rate of the reading process.

1.2. RFID system features

1.2.1. Passive, semi-passive, active

RFID tags can be characterized as either active or passive. Traditional passive tags are typically in "sleep" state until awakened by the reader's emitted field. In passive tags, the reader's field acts to charge the capacitor that powers the badge. Due to the strength of the signal that is required, passive tags are most often used for short read-range applications (<1.5 m) and require a high-powered reader with antenna capable of reading the information. Passive tags are often very light, compact, and have unlimited life spans.

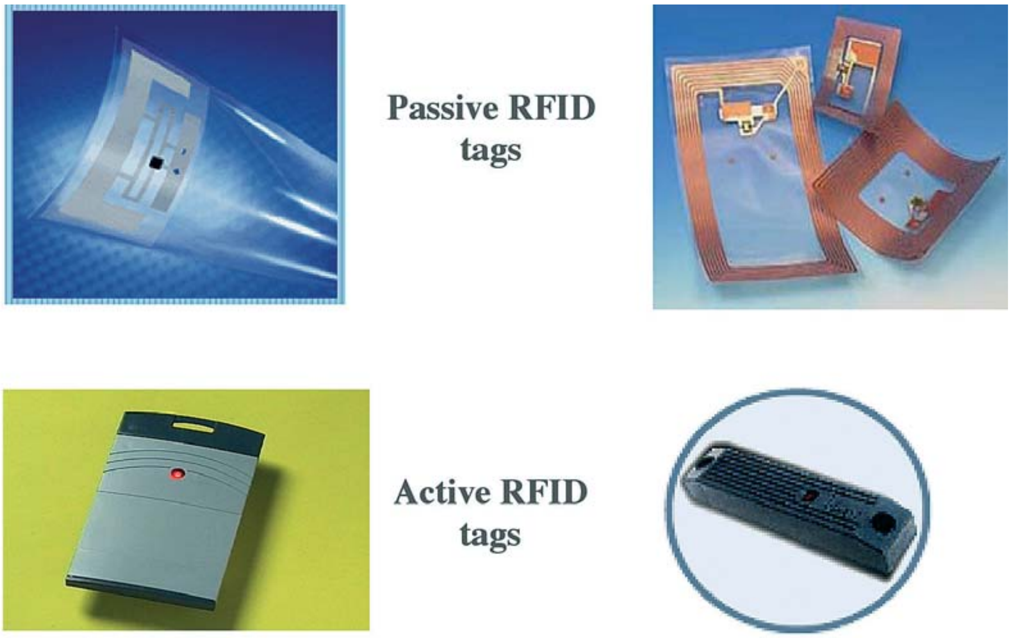
The contactless smartcards, plastic with a credit card size that can be accessed through a radio reader device, are often confused with passive RFID. Although the communication method is quite the same, the contactless smartcards have on-chip processing and memory capability that is not needed on RFID. RFID just holds an identifier while contactless smartcards might hold personal identification data, complex encryption capabilities, or application specific logic.

The active tags are typically powered by an internal battery (that lasts several years but whose duration strictly depends upon the application) and are utilized for long read-range applications up to 100 m. Active badges can continuously emit a detectable signal and are typically read/write with a higher total memory. Due to these increased capabilities, active tags are heavier, more expensive, and have limited life spans.

Another category of tags is commonly referred to as semi-passive (also called semi-active and/or battery assisted RFID). These tags communicate with the reader as if they were passive tags but have a battery on board in order to support specific functions, e.g. to store periodic temperature information from an onboard temperature sensor.

[2] Aloha, developed in the 1970s for a packet radio network by Hawaii University: sender finds out if there is a collision with transmitted data and retransmits data after some time in case there is collision. In case of Slotted Aloha, time is slotted and data can be transmitted at the beginning of one slot so reducing the collision duration.

Figure 1-2: Passive and active RFID tags packages



1.2.2. Frequency

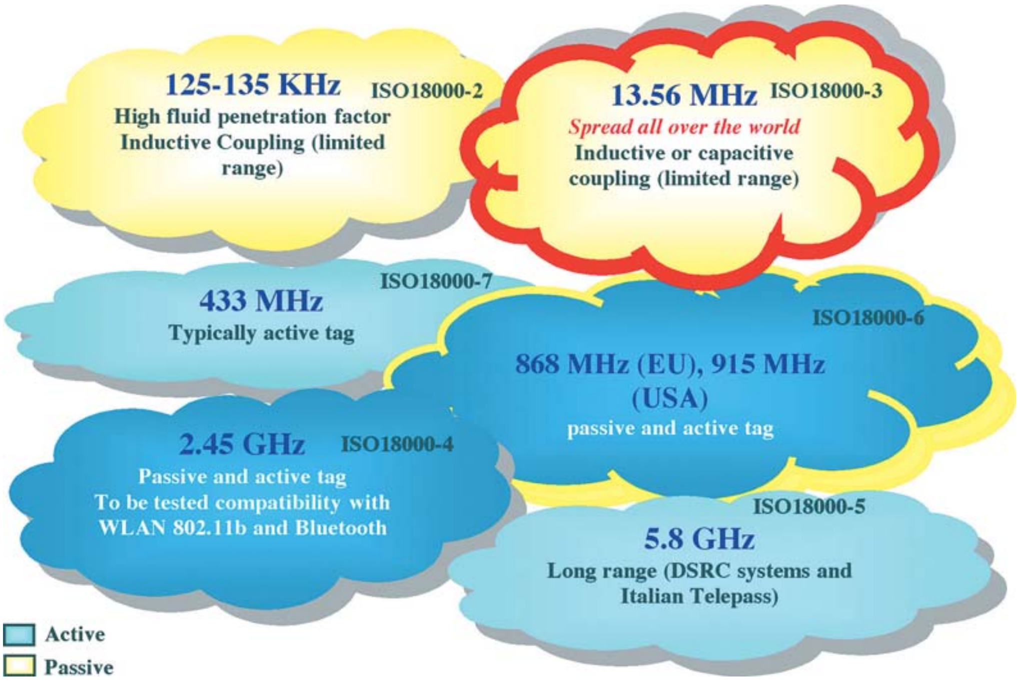
The capabilities of the RFID system are also very dependent on the carrier frequency at which information is transported. Due to government regulation, different parts of the electromagnetic spectrum are assigned for different purposes. This results in a number of frequency bands in use around the world for RFID application. A commonly accepted scheme categorizes these frequencies in four ranges that are summarized in the table hereafter including also typical system characteristics and areas of application.

Table 1-1: Frequency bands and applications

	LF	HF	UHF	Microwave
Frequency Range	< 135 KHz	10 ... 13.56 MHz	860 … 960 MHz	2.4 … 5.8 GHz
Read Range	~10 cm	~1 m	2 ~ 5 m	~100 m
Coupling	Magnetic, Electric	Magnetic, Electric	Electromagnetic	Electromagnetic

Frequency bands used by RFID systems are associated to different part of ISO 18000 standard as described in Section 3.2.1. Different frequencies have to be used for different applications: a rule of thumb for this is that lower frequencies can be used to increase the penetration into materials and water, but give shorter range (inductive coupling). Higher frequencies can increase the range (so called UHF backscattering RFID tags) but become very sensitive to environmental conditions.

Figure 1-3: Frequency used by RFID systems


125-135 KHz ISO18000-2
High fluid penetration factor
Inductive Coupling (limited range)
13.56 MHz ISO18000-3
Spread all over the world
Inductive or capacitive coupling (limited range)
433 MHz ISO18000-7
Typically active tag
ISO18000-6
868 MHz (EU), 915 MHz (USA)
passive and active tag
2.45 GHz ISO18000-4
Passive and active tag
To be tested compatibility with WLAN 802.11b and Bluetooth
ISO18000-5
5.8 GHz
Long range (DSRC systems and Italian Telepass)
Active
Passive

1.2.3. Factors affecting reading capability

It has to be made clear that though the technology promises a number of fancy characteristics, its real application is not straightforward. The possibility of reading RFID tags is conditioned by critical and sometimes rather non-deterministic factors. It is intuitive that if the tag is "too far" from the reader then no reading can take place. On the contrary it might be extremely useful to exactly know how to increase the reading distance up to what is needed by a specific application. Another myth is that anything might be tagged with an RFID, but the truth is that certain materials have characteristics affecting the reading capability.

Trying to put some order in these factors they can be summarized in:

- *Radio technology and reading distance*

  LF and HF passive tag systems use electric and magnetic[3] coupling; this means that the reader yields a magnetic field and the tag is capable of modifying it in a way that the reader can sense. The magnetic field should have enough "intensity" to power the tag circuitry. It can be shown that the intensity of the magnetic field decreases in intensity with distance through a factor that can be approximated to one over the cube of the distance 1/d.[3] This means that doubling the distance, the capability of reading the tag with the same reader is decreased to 1/8. In other words to read a tag at a distance twice the original distance the reader should yield a magnetic field with power eight times the original power used.

  UHF passive tag systems use the so called backscattering: once the tag is activated by the reception of a radio wave, it activates and "sends" back a radio wave with the answer message. In this case the factor that indicates the relation between the power of the reader and the reading distance is one over the square of the distance 1/d.[2] This is why UHF is used where the reading of passive tags is needed at greater distances.

  Active tags are powered by an internal energy source and thus they do not need to extract power from a magnetic or electromagnetic field. They are capable of overcoming the passive tags distance limitations

[3] In the following reference will be made always to magnetic coupling as electric coupling is far less applied.

and support applications with a reading distance of 100 m or even more.

- *Radio frequency and tagged materials*

  Radio waves, as well as light, are absorbed by some materials, notably water, and reflected by others, namely metals, in different ways depending on their frequency. This means that a passive RFID applied on a bottle of water or, worst case, on a beer can, might be hardly read. HF tags might be used to tag bottles of water better than UHF. They can also be used on metal objects by separating them from the metal by some millimetres thick dielectric that allows the magnetic field to transit through the coils of the antenna (not being diverted by the metal of the tagged object).

  UHF passive tags applied to bottles of water can be read only if they are applied on the side of the bottle turned towards the antenna of the reader: if the tag is on the other side then the radio waves are weakened by transiting through the water and the reading is compromised. In the case of metals, appropriate packaging is needed in order to avoid interference of the answer message with the waves reflected by the metal substrate.

- *Reading geometry*

  The magnetic (or electromagnetic) field generated by the reader is somehow oriented by the reader antenna and power is induced in the tag only if the orientation of the tag antenna is appropriate. A tag placed orthogonal to the reader yield field will not be read. This is the reason that guided manufacturers to build circular polarized antenna capable of propagating a field that is alternatively polarized on all planes passing on the diffusion axis. Linear antennas need a more accurate positioning of the tag but can operate at longer distances.

- *Environmental factors*

  The sites where usually RFID are needed are never empty spaces: they are filled up with metal shelves, heating water pipes, moisture, fork lifts moving around, and communication radio equipment. It is very hard to predict what would be the behaviour of a RFID system in such rugged situations. Radio waves are reflected, absorbed and mixed with other radio waves. One RFID technology might work better than the other and this can only be identified through field trials.

  The described factors are the reason for which in most cases prime contractors suggest that after the business case has been stated and the application process has been engineered to benefit most from the RFID application, a limited experiment is implemented in the actual place in order to better identify the technologies to be used.

1.2.4. RFID and barcodes

Although it is often thought that RFID and barcodes are competitive technologies, they are in fact complementary in some aspects. The primary element of differentiation between the two is that RFID does not require line-of-sight technology. Barcodes must be scanned at specific orientations to establish line-of-sight, such as an item in a grocery store, and RFID tags need only be within range of a reader to be read or 'scanned.' Although RFID and barcode technologies offer similar solutions, there are significant advantages to using RFID:

- Tags can be read rapidly in bulk to provide a nearly simultaneous reading of contents, such as items in a stockroom or in a container.

- Tags can be read in no-line-of-sight conditions (e.g. inside packaging or pallet).

- Tags are more durable than barcodes and can withstand chemical and heat environments that would destroy traditional barcode labels. Barcode technology does not work if the label is damaged.

- Tags can potentially contain a greater amount of data compared to barcodes, which commonly contain only static information such as the manufacturer and product identification. Therefore tags can be used to *uniquely* identify an object.

- Tags do not require any human intervention for data transmission.

- Changing the data is possible on some RFID tags

It is easy to see how RFID has become indispensable for a wide range of automated data collection and identification applications. The distinct advantages of RFID technology, however, introduce an inevitably higher cost. RFID and barcode technologies will continue to coexist in response to diverse market needs. RFID, however, will continue to expand in markets for which barcode or similar optical technologies are not as efficient.

1.2.5. Security

Security encryption methods can be embedded onto the tag to ensure that the information on it can only be read or written by authorized users. The creation of encryption specifications for RFID tags by the standards organizations, now in progress, is a vital step for ensuring widespread protection. Security encryption algorithms have already been established for the 13.56 MHz-based ISO/IEC 14443 standard used for automatic fare collection in public transit applications.

In order to create high security RFID systems a defence against the following individual attacks would be needed (see also Chapter 8):

- Unauthorised reading of a data carrier in order to duplicate and/or modify data.
- The placing of a foreign data carrier within the interrogation zone of a reader with the intention of gaining unauthorised access to a building or receiving services without payment.
- Eavesdropping into radio communications and replaying the data, in order to imitate a genuine data carrier (‘replay and fraud’).

When selecting a suitable RFID system, consideration should be given to crypto-logical functions. Applications that do not require a security function (e.g. industrial automation, tool recognition) would be made unnecessarily expensive by the incorporation of cryptological procedures. On the other hand, in high security applications (e.g. ticketing, payment systems) the omission of cryptological procedures can be a very expensive mistake if manipulated transponders are used to gain access to services without authorisation.

1.3. RFID infrastructure elements

Once a tag is placed, the basic components needed to collect the tag information and pass it to the proper application are the readers and the RFID middleware. The readers are the devices capable of activating the tags and having them provide their data. RFID middleware is the software system needed to perform a “sensible” reading, i.e. whenever a contemporary reading of multiple tags is needed it discards duplicates and selects the only data relevant to the application.

1.3.1. RFID readers

Though manufacturers pursue the possibility of a universal reader capable of reading any kind of tag, the current situation is that each type of tag can by read by dedicated equipment. This means that an HF Reader is needed to read an HF tag and a different reader is needed to read a UHF one.

A characterization of readers for passive and active tags is presented below:

- Readers of Passive RFID tags:
  - High power emitted (max 4W) in order to activate passive RFID tags
  - High power consumption (rank of Watts)
  - Operating ranges of some meters
  - Passive Readers can read simultaneously a number n of RFID tag with a reading speed of some seconds (n>100)
  - Reader comprises the antenna, anti-collision systems (microprocessor + software + memory), RF transceiver, network interfaces (Ethernet, Wi-Fi, GSM, etc.)
- Readers of Active RFID tags:
  - Low power emissions (10-20 mW)
  - Reduced power consumption (rank of mWatts) that allows integration in handheld devices
  - Long ranges (20-100 m)
  - Active readers can read simultaneously different RFID tags (hundreds of RFID tags) with high reading speed (milliseconds)
  - Readers include an antenna that can be integrated, an anti-collision system (microprocessor + software + memory), a RF

transceiver, network interfaces (Ethernet, Wi-Fi, GSM, etc.)

1.4. RFID middleware

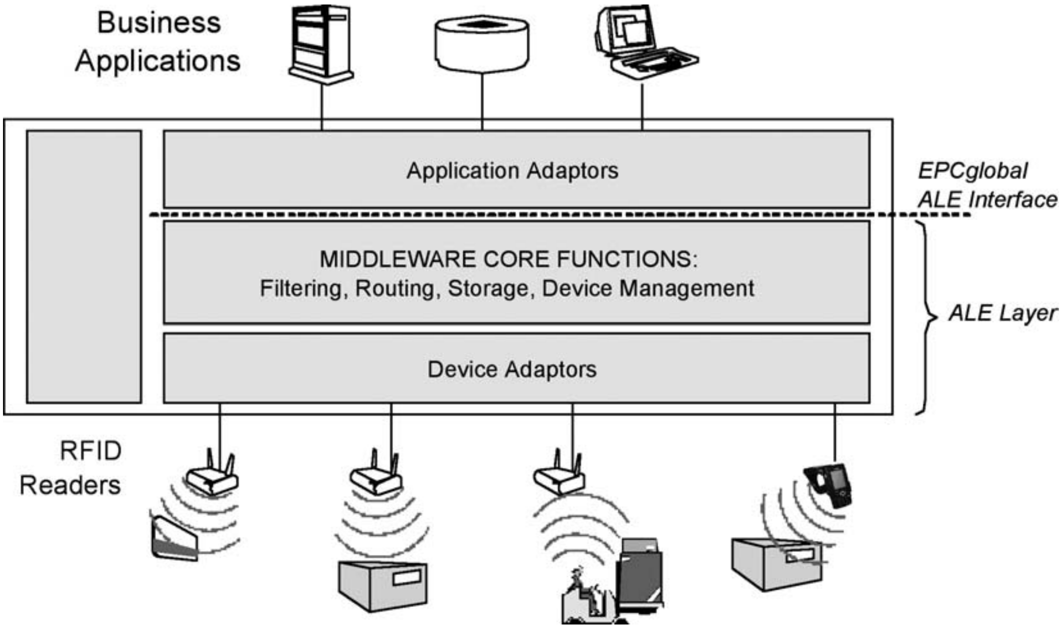
The RFID Middleware is referred to, by software manufacturers (Forrester, 2005) and by EPCglobal (EPCglobal, 2004), as the set of functions in between the pure RFID technology components, in first place the readers, and the business applications capable of exploiting the value of the technology.

These functions can be summarized in:

1. Filtering: thinking of a stream of tag-read events generated by the readers, the filtering functions chooses, on the basis of proper criteria, which ones deserve to be processed by the application layer; as an example, in some cases, when a tag is read twice by the same reader within a few seconds, only one event might have to be reported;

2. Routing: once the tag-read event has been accepted for forwarding by the filtering function, the Routing Function, on the basis of proper criteria, is capable of delivering it to the correct application;

Figure 1-4: RFID middleware – ALE layer as defined by EPCGlobal



3. Data Management: the accepted events are as well recorded on some storage in order to allow for queries on e.g. the history and performance monitoring;

4. Device Management includes the control and management functions of the readers: collects and handles alarms, allows for software download, configuration of frequencies and power emissions, etc.

5. Device Adaptors; at the moment there is no agreement upon the protocol interface (neither official nor industry standard) to make readers work with other systems; the Device Adaptors refer to the software code that has to be provided in order to allow readers be controlled by the other Middleware functions;

6. Application Adaptors: as in point 5 the Application Adaptors allow business applications to interoperate with the RFID Middleware.

On the Middleware subject, a specification activity is being carried out by EPCglobal in order to define the capabilities that have to be supported by the ALE Layer (Application Level Events Layer) in order to allow for the EPCglobal Information and Discovery Services (see Section 3.1). Figure 1-4 depicts the RFID Middleware also with reference to ALE Layer and Interface.

1.5. Organizations developing international standards

As RFID technology continues to expand, the need for establishing global standards is increasing. Many retailers have completed RFID trials within their supplier communities, adding pressure on manufacturers and suppliers to tag products before they are introduced into the supply chain. However, manufacturers cannot cost-effectively manage RFID tagging mandates from disparate retailers until global standards are established. This process requires the creation and acceptance of data standards that apply to all countries, and it requires scanners to operate at compatible frequencies.

1.5.1. EPCglobal

In 1998, researchers at the Massachusetts Institute of Technology (MIT) Auto-ID Center began global research on RFID. The Auto-ID Center focused on:

- Reducing the cost of manufacturing RFID tags.
- Optimizing data networks for storing and delivering large amounts of data.
- Developing open standards for RFID.

The work of the Auto-ID Center has helped make RFID technology economically viable for pallet and carton-level tagging. The Auto-ID Center closed in October 2003, transferring all its RFID technology and information to the EPCglobal organization.

EPCglobal is a member-driven organization of leading firms and industries focused on developing global standards for the electronic product code (EPC) Network to support RFID. The EPC is attached to the RFID tag, and identifies specific events related to the product as it travels between locations. By providing global standards on how to attach information to products, EPC enables organizations share information more effectively. The vision of EPCglobal is to facilitate a worldwide, multi-sector industry adoption of these standards that will achieve increased efficiencies throughout the supply chain—enabling companies to have real-time visibility of their products from anywhere in the world.

The purpose of EPCglobal is to provide the technology to increase efficiency and reduce errors in the supply chain, achieved by the use of low cost RFID tags and a framework for global information exchange (see Section 3.1 for the EPC standards). EPCglobal is a joint venture of GS1 (formerlyEAN International) and GS1 US™ (formerly Uniform Code Council, UCC).

1.5.2. Global data synchronization

Global Data Synchronization (GDS) is an emerging market in Supply Chain Management. It is the foundation for next-generation applications such as RFID-based tracking, and more. GDS is designed to keep supply chain operations synchronized by ensuring that basic product data, such as the description and category stored by one company, matches the data stored by its trading partners. Organizations submit product data in a specific format to data pools around the globe, and the data is then validated against a global data registry.

Standards for GDS are guided by the Global Commerce Initiative (GCI), a collective group of retailers and manufacturers. The standards are being developed by the European Article Numbering Association International and The Uniform Code Council (EAN and UCC). These standards assign attributes to product data that enables manufacturers, suppliers, retailers, and other participants in the supply chain to share product-related data across the globe. For example, manufacturers could have their product catalogue accessible worldwide, and retailers could search for any type of product and take advantage of unlimited global access.

1.5.3. International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is a network of national standards institutes of 148 countries working in partnership with international organizations, governments, industries, and business and consumer representatives. The ISO asserts jurisdiction over the Air Interface (the frequency spectra used for RFID transmission) through standards-in-development ISO 18000-1 through ISO 18000-7. These are represented in the United States by the American National Standards Institute (ANSI) and the Federal Communications Commission (FCC).

The International Organisation for Standardisation (ISO) in collaboration with the International Electrotechnical Committee (IEC) has produced a set of standards for the interface between reader and tag, operating at various radio frequencies. As mentioned, these standards are numbered in the series ISO/IEC 18000-n.

There is strong interest currently in the UHF frequency band between 860 MHz and 960 MHz. The ISO standard, currently being published, is ISO/IEC 18000-6, with options for two differing communications protocols, type A and type B. It is likely that the recently agreed EPCglobal Generation 2 standard will be incorporated into ISO 18000-6 as type C.

Previously, only a relatively small amount of bandwidth at restrictively low power was available in Europe in the newly exploited band around 900 MHz. This is because the frequency range between 902 MHz and 928 MHz as used in North America is assigned to the Global System for Mobile (GSM) services in Europe. The situation has improved immensely following the recent approval by European standards bodies of the use of ten channels at 2 Watts Effective Radiated Power (ERP) in the band from 865.6 MHz to 867.6 MHz, together with five additional lower powered channels. The European Telecommunications Standards Institute (ETSI) has recently produced and approved technical standards to meet these parameters. While the available bandwidth may prove to be a restriction in the long term, the increase of radio frequency (RF) power to 80% of that allowed in North America means that the performance in terms of range will be quite similar in both regions.

1.5.4. AIM Global

AIM Global is the global trade association for the Automatic Identification and Mobility industry that manages the collection and integration of data for information management systems. Serving more than 900 members in 43 countries, AIM Global is dedicated to accelerating the use of automatic identification data collection (AIDC) technologies around the world.

As the leader in developing international RFID standards, AIM Global strives to educate the community. The company is participating as the RFID Association Sponsor for a series of symposiums worldwide to build consensus about standards for using RFID technology on commercial airplanes. Aircraft manufacturers Boeing and Airbus plan to collaborate; both companies are moving toward RFID adoption based on the Air Transport Association (ATA) automated identification and data capture guidelines.

1.5.5. Ubiquitous ID Center

The Ubiquitous ID Center was created to develop technologies such as RFID and others that will enable the automatic recognition of items with the ultimate objective of creating a ubiquitous computing environment. In April 2004, China, Japan, and Korea agreed to participate in Ubiquitous ID-related events, each signing agreements to conduct joint research with the goal of establishing Ubiquitous ID Centers and T-Engine Development centres in each country. T-Engine is the development platform for ubiquitous computing technologies.

1.6. Future tagging technologies

Though radio technology for identification purposes has been a revolution with respect to the proven laser based barcode, future identification technologies will not necessarily be using radio waves. In the following an overview is given of some of the more promising automatic identification technologies currently under study or in very early industrial phase based on radio waves as well as laser readers.

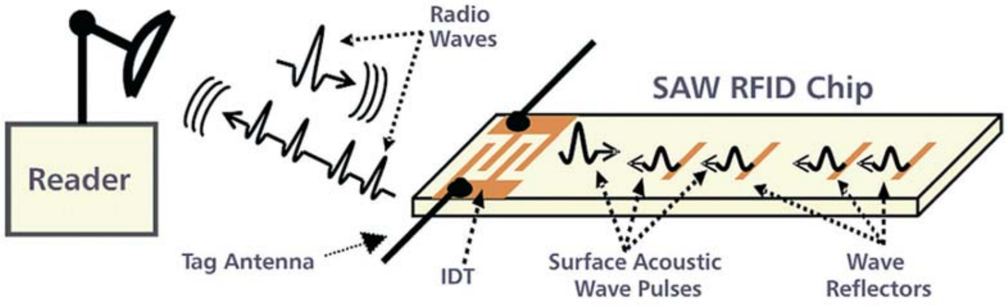
1.6.1. Surface Acoustic Waves (SAW) 4

The promise of the SAW technology is to be able to provide very low cost radio readable tags. The SAW tags are classified as "chipless" tags because there is no need for a real processing chip to operate them. Once the SAW tag receives the radio signal from the reader, a simple transducer translates it into acoustic waves on the surface of

[4] http://www.rfsaw.com

the tag. Metallic structures precisely built on the tag reflect, according to a definable scheme, the acoustic wave back to the transducer that converts it again into a radio signal. The overall effect is very similar to a conventional RFID but, having no need of a processing chip, the cost is dramatically reduced. From experiments it seems that SAW tags perform very well both on metals and water thus overcoming the constraints of HF and UHF RFID. The drawback is that the tag code is hard-coded by the tag manufacturer and is not modifiable. Moreover effective ways to avoid collisions have yet to be identified.

Figure 1-5: Surface Acoustic Wave (SAW) Tags



1.6.2. Embedded tags

Tagging will move from being something attached to an object to become a standard part of the object "fabric". RFID are technologies that can substitute the barcode as soon as 2007 in the mass market. They are already replacing barcode on pallets and in certain market sectors. Their value in the production and distribution chain is very big since they facilitate reading at a distance. There are several flavours of RFID tags, passive, active, rewriteable, etc. For application within the area of *person identification* the ones that fit better are the passive RFID. Being passive there is no need for a battery and the chips can stay "dormant" for tens of years till an appropriate electromagnetic field activates them and read the values stored. Although there are already a number of people who have chosen to be tagged it is still an open question whether it will be a mass-market identification or be restricted to some niches. *Pets and livestock* in many countries are already tagged (in livestock, tags are replacing the branding). It is surely technologically and economically feasible to inject any *newborn baby* with a RFID tag and from that moment on to have a unique electronic signature of the person that can be used through a cross referencing database in a number of ways.

Other identification techniques are at the horizon, based on cellular tagging. The problem here is that cells die and are shed so the tags would need to be replaced continuously. This kind of tagging is likely to be used extensively for *medical treatment*. It may provide tagging for the duration of the cure. Tags are already used in medical treatment to identify cancerous cells, or as a marker for guiding robots during surgical operations. Some leading edge technologies have already demonstrated the possibility of associating nano-antennas to the cell DNA. Nano markers are also under consideration for *medical diagnoses* and they may be used for identification. However the possibility offered by RFID tags, their low cost, easy implantation and reading are shifting the question to the social acceptability rather than on finding alternative technologies. Research in this area is both in basic science and in cross disciplinary approach.[5]

[5] Examples of advanced research areas: a) Underskin Implant of RFID for personal identification, Amal Graafstra, http://www.bmezine.com/news/presenttense/20050330.html b) RFID embedded in cardboard boxes by Beamfetch, http://www.rfidjournal.com/article/articleview/1588/1/72 c) RFID embedded in tires by Michelin, http://www.rfidjournal.com/article/articleview/269/1/1/

1.6.3. UWB tags[6]

UWB (Ultra Wide Band) RFID tags transmit signals over multiple bands of frequencies simultaneously and transmit for a much shorter duration than those used in conventional RFID. This type of tags consumes less power than conventional RF tags and can operate across a broad area of the radio spectrum. UWB tags can be used in close proximity to other RF signals without causing or suffering from interference because of the differences in signal types and radio spectrum used.

Parco Wireless company has prepared a demo area to show UWB tag advantages. The demo area recreates a hospital environment. By using UWB tag patients can be localised as well as medical and paramedical instruments.

With respect to passive tags, UWB tags do not interfere with electronic equipment used in hospitals. The actual transfer speed (100 kbps) is going to be 24 Mbps within 2 years according to Parco Wireless. Each tag emits its ID signal every second and can be localised by a system of receivers with 5 cm precision. Four antennas are enough to cover an area up to 2000 square meters depending on the building structures in the area.

Today an UWB tag costs about 40 euros.

1.6.4. Optical tags[7]

Optical tags fall in the Physical One Way Function (POWF) class. They have the drawback of needing fairly complex arrangements to be read, namely the extremely precise positioning of the tag with respect to the laser beam of the reader. This makes them not practical for most applications with respect to passive and active tags. A promising characteristic is in the capability to provide different codes to different angled readers thus effectively partitioning information. This might prove useful in several business applications with support for high security.

The prototypes (Massachusetts Institute of Technology) are currently built on an Eurocent sized piece of plastic that has a number of randomly positioned glass micro spheres. When the system is lighted by means of a laser beam it reflects light with a very specific scattering pattern. The pattern is analysed by a system that can precisely identify the single tag instance. The tag can be hardly reverse-engineered: it is practically impossible to build a tag with those micro spheres on the basis of its scattering pattern. Moreover different readers might get different results thus allowing for a robust certification of the identity of the tag. The costs are expected to be comparable to those of the barcode tags when mass produced.

1.6.5. DNA tags[8]

In order to develop anti-counterfeit systems a new technology is being explored: tags which use DNA fragments. There are already companies (such as the American Applied DNA Science) which are developing systems to embed botanic DNA fragments into tags; DNA is among the most resistant code structures: Applied DNA Science guarantees that this type of tagging can be readable for as long as 100 years. It is likely that most benefit will be realised when using this type of tagging directly in passports, bank checks, etc…

1.6.6. Software tags[9]

Software tags are also very promising. The technology of software tags differs considerably from other tags but software tags show great overlap in functionality with other hardware based tags. Software tags will for instance be used in tagging on-line information.

An example of software tags is given by Semapedia.org.[10] Through a Semapedia application it is possible to create a specific picture (resembling a large square filled with little black squares) able to

[6] http://www.rfidjournal.com/article/articleview/1285/1/1/

[7] http://www.sciencedaily.com/releases/2003/11/031113070248.htm
http://web.media.mit.edu/~brecht/papers/02.PapEA.powf.pdf
http://www.trnmag.com/Stories/2002/100202/Plastic_tag_makes_foolproof_ID_100202.html
http://web.media.mit.edu/%7Epappu/htm/res/resPOWF.htm

[8] http://www.csmonitor.com/2004/0318/p14s02-stct.html, http://www.dnatechnologies.com/process/

[9] http://www2.districtadministration.com/viewArticle.aspx?articleid=126

[10] http://www.semapedia.org/

represent, and being associated to, an Internet link (Semapedia links to Wikipedia information). Once the picture is created it must be printed out and placed on a physical object whose internet link is an address. The information about the physical tagged object is then obtained by just taking a picture with a cellular phone and processing it through simple software. By this technique it is possible to place a simple small paper picture close to every monument and then reach the associated information on the Internet by taking a picture of the tag and processing it.

1.7. Potential challenges of RFID implementation

In addition, to choosing the appropriate tag/reader technology in a specific application area, the following list represents potential challenges to consider when implementing an RFID solution:

- *Large volumes of data*–Readers scan each RFID tag several times per second, which generates a high volume of raw data. Although the data is redundant and discarded at the reader level, processing large volumes of data can be difficult.
- *Product information maintenance* – When a high volume of RFID tags are processed by the reader, the attributes of each tagged product must be continually retrieved from a central product catalogue database – a process that results in challenges for large-scale implementations.
- *Configuration and management of readers and devices* – When a large number of readers and related hardware devices are deployed across multiple facilities, configuration and management can be challenging. The implementation of automated devices for these processes is essential.
- *Data integration across multiple facilities* – In an enterprise with multiple facilities that are geographically distributed, it is increasingly difficult to manage data in real time while at the same time aggregating it into the central IT facility—a process that can place a significant burden on the network infrastructure.
- *Data ownership and partner data integration* – When there are different companies involved in business processes, such as commonly found in the Retail supply chain, it can create issues pertaining to the ownership and integration of the data, thereby compromising the integrity of the solution architecture.
- *Data security and privacy* – Depending on the nature of the business application and the solution scenario, security and privacy challenges could have a significant impact on the architecture.

2. Spectrum allocation

The capabilities of the RFID system are very dependent on the carrier frequency at which information is transported. The use of lower frequencies provides larger wavelength and a coupling effect between RFID tag and reader more similar to primary and secondary coupling inside inductors (see also Section 1.2). This causes the range to be shorter in LF (~125 kHz) and HF (~13.56 MHz) bands than in UHF (~900 MHz) and microwave bands (>2.45 GHz): for UHF and microwave as a matter of fact, the coupling between tag and reader is performed by backscattering (the electromagnetic wave is propagated from the reader and reflected by the RFID and modulated according to the specific information of RFID tag). The range that can be achieved using the same radiated power as in case of LF is much higher for UHF and microwave RFID system, depending on propagation conditions as well as on regulatory limits.

Due to government regulation, different parts of the electromagnetic spectrum are assigned to different use purposes. The three frequency ranges that typically distinguish RFID systems are low, intermediate, and high. There are currently four frequency bands in use around the world for RFID applications. Within these bands a number of frequencies are addressed by RFID standards and used by manufacturers in proprietary applications. These frequency ranges and associated information describing typical system characteristics and areas of application are presented through the *Table 2-1*.

Table 2-1: RFID frequency bands and applications

Frequency Band	Characteristics	Typical Applications	Typical Range
Low Frequency 30-300 kHz ITU Band 5	125-135 kHz Short to medium read range Inexpensive Low reading speed	Access control Animal Identification Inventory control Car immobilizer	Few centimetres
High Frequency 3-30 MHz ITU Band 7	13.56 MHz Short to medium read range Potentially inexpensive Medium reading speed	Access control Smart Cards	Few centimetres (could be slightly enhanced using particular antennas)
Ultra High Frequency 300-3000 MHz ITU Band 9	433 MHz 860-960 MHz 2.45 GHz Long read range High reading speed Line of sight required for micro-wave backscattering systems Expensive	Railroad car monitoring Toll collection systems	Under 10 meters
Super High Frequency 3-30 GHz ITU Band 10	5.8 GHz Line of sight required for micro-wave backscattering systems Expensive	Toll collection systems UWB Localization	100 m and over

Frequency bands used by RFID systems are associated to different parts of ISO 18000 standard as described in Section 3.2.1. Different frequencies have to be used for different applications: a rule of thumb for this can be associated to the fact that lower frequencies can be used to increase the penetration into materials and water, but give shorter range (inductive coupling). Higher frequencies can increase the range (so called UHF backscattering RFID tags) but become very sensitive to environmental conditions.

2.1. Regulatory status for using RFID

Frequency bands are defined through national regulation: any RF equipment is allowed to be powered only if complying with these regulations. This applies also to RFID applications in various ways. LF band is basically unregulated and thus LF RFID are freely used (e.g. electronic car key, automatic coffee machines, etc.).The 13.56 MHz, 433 MHz, 2.45 GHz frequencies were originally allocated globally for Industrial, Scientific and Medical (ISM) non-commercial applications and, not considering possible local regulations, are license-free.[11]

The UHF frequency range needed for EPC-global compliance (860-960 MHz) that is not a license-free band has a different status. In this case each country has taken up the responsibility of making the frequencies available for RFID applications. This process is well underway worldwide.

Table 2-2 presents UHF spectrum allocation characteristics concerning the 27 EU Member States of the European Community and *Table 2-3* presents the spectrum allocation characteristics of selected remaining countries in Europe. The status code “IP” means that no regulations are available at the moment but work is in progress, while the code “NA” stands for no information available. In the EU25 area it can be seen that issues in most countries should be solved during the year 2006, except in Italy and Hungary where some decisions still have to be taken. It should be noted that the unavailability of UHF frequencies in some countries might heavily undermine their capacity in the future to keep the pace with international commerce.

Table 2-2: EU27 UHF spectrum allocation

Country	Status	Frequency	Power	Protocol	Comments
Austria	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since 2 February 2006
Belgium	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Bulgaria	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Cyprus	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Czech Republic	OK	865.6-867.6 MHz	2 W erp	LBT	
Denmark	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since January 2005
Estonia	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006. License possible.
Finland	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since 3 February 2005
France	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be implemented in July 2006
Germany	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since 22 December 2004
Greece	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Hungary	IP	865.6-867.6 MHz	2 W erp	LBT	Implementation is in progress
Ireland	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Italy	IP	865.6-867.6 MHz	2 W erp	LBT	Conflict with band allocated to tactical relays military application. Temporary licenses available.
Latvia	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Lithuania	IP	865.6-867.6 MHz	2 W erp	LBT	Individual license required. New regulations should be in place in 2006
Luxembourg	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Malta	IP	865.6-867.6 MHz	2 W erp	LBT	Individual license required. New regulations should be in place in 2006

[11] To check the ISM Bands reference can be made to “European Radiocommunications Committee (ERC) within the European Conference of Postal and Telecommunications Administrations (CEPT)” at http://www.ero.dk/eca-change .

Country	Status	Frequency	Power	Protocol	Comments
Netherlands	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations will be in place since 27 February 2006
Poland	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since October 24th 2005
Portugal	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Romania	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since April 7, 2006
Slovak Republic	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place
Slovenia	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Spain	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations will be in place by January 2007
					Temporary licenses available.
Sweden	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations approved 13 Dec 2005. In the law since 1 Jan 2006
United Kingdom	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place as of 31 January 2006

Table 2-3: UHF spectrum allocation in other European countries

Country	Status	Frequency	Power	Protocol	Comments
Bosnia Herzegovina	NA				
Croatia	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Iceland	OK	865.6-867.6 MHz	2 W erp	LBT	
Macedonia, FYR	NA				
Norway	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations will be in place in 2006
Serbia	NA				
Montenegro	NA				
Switzerland	OK	865.6-867.6 MHz	2 W erp	LBT	
Turkey	IP	865.6-867.6 MHz	2 W erp	LBT	Conflict with band allocated to tactical relays military applications

2.2. Efficient use of spectrum allocation (RFID, WiFi, ZigBee)

The selection of the technology to be used according to the application scenario is a hard issue to solve because it has to take care of several factors that rely upon the application requirements but also upon the availability of spectrum resources. By using passive RFID systems (tags and readers) the tags do not need batteries but the overall power emission radiating from the reader has to be much higher than battery operated active RFID systems (where the power source of the tags itself can be used to send a response from an interrogation without waiting for an electromagnetic field coming from the reader in order to enable the passive RFID). Considering this, it can be assumed that the emitted power of active RFID systems (tags and readers) is significantly lower than the emitted power related to passive RFID systems. The disadvantages connected to spectrum occupancy are related to the use of passive RFID for bands that can be used by other wireless system because a passive reader may occupy a significant portion of the spectrum not allowing other systems to work properly.

An example of this is the 2.45 GHz ISM band where technologies like WiFi, Bluetooth and ZigBee coexist (see Section 4.2 for information about these technologies). If active RFID tag technology is used, the effect can be considered similar to having multiple ZigBee networks situated in a limited area: in that case the spectrum can be crowded but the power level can be maintained low enough to guarantee the correct functionality of the networks. If a 2.45 GHz passive RFID system is placed inside a WiFi network, it can seriously affect the WiFi performance. So attention has be paid into the combined use of active and passive RFID technologies and the frequency band choice because the application behaviour can be affected by it.

In general the choice of the frequency band has to take into account the following points that are strictly connected to application requirements and cost of the final solution:

- Application requirements:
  - Range of readings;
  - Number of simultaneous readings per second;
  - Frequency of readings (it can discourage the use of active RFID tags);
  - Types of material of the tagged objects (problems with fluids)
  - Operational environment (propagation environment can significantly change its effect according to the frequency range)
- Cost:
  - Referred to the RFID tags;
  - Referred to the RFID readers;
  - Referred to the RFID system (middleware and network infrastructure).

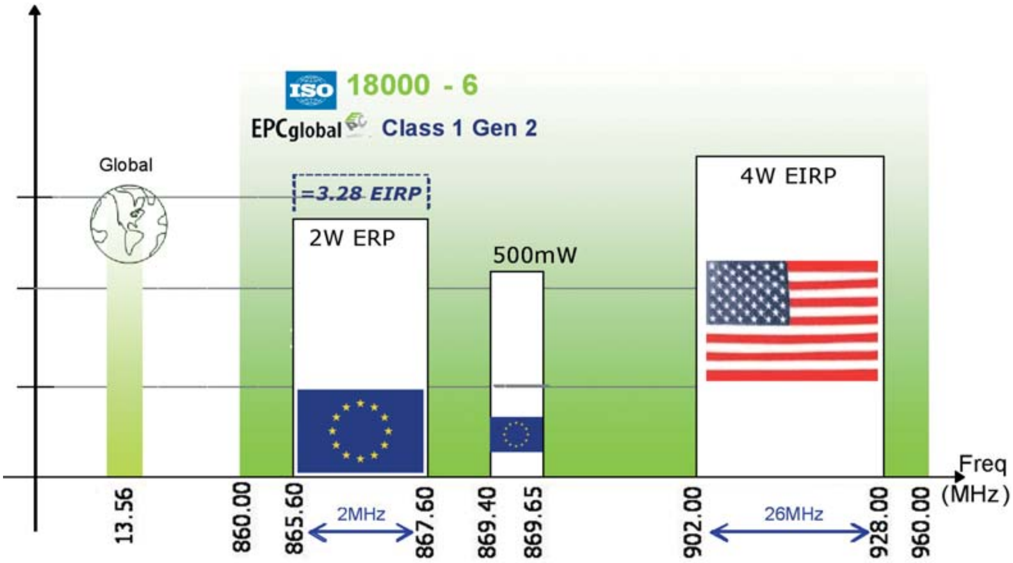
Therefore, in order to guarantee multiple radio solutions in a limited area, attention has to be paid to the choice among the passive RFID tag solutions; the trade-off with active tags can be found considering the cost of the active RFID tags and the fact that battery operated systems could require replacement (it strictly depends upon application requirements and frequency of readings).

3. RFID standards

As RFID technology continues to expand, the need for establishing global standards is increasing. Many retailers have completed RFID trials within their supplier communities, adding pressure on manufacturers and suppliers to tag products before they are introduced into the supply chain. However, manufacturers cannot cost-effectively manage RFID tagging mandates from disparate retailers until global standards are established. This process requires the creation and acceptance of data standards that apply to all countries, and it requires scanners to operate at compatible frequencies.

Figure 3-1 provides an overview of the relevant RFID standards and their relationships with special reference to EPCglobal standards. It has to be noted that the electromagnetic power that is radiated by the reader in order to read the tags has a relevant impact on the maximum distance between the reader and the tag: increasing power enables increasing the read distance and the technology exploitation potential. The radiated power can be measured in different ways. As an example US standards allows a maximum radiated power of 4W EIRP (Equivalent Isotropic Radiated Power) while European standards allow for 2W ERP (Effective Radiated Power). If the power radiation characteristics have to be compared then it should be noted that 2W ERP is equivalent to 3.28W EIRP thus comparable to the US 4W.

Figure 3-1: RFID frequencies and relevant standards



3.1. EPCglobal[12]

EPCglobal is a member-driven organization of leading firms and industries focused on developing global standards for the electronic product code (EPC) Network to support RFID (see also Section 1.5.1) The EPC is attached to the RFID tag, and identifies specific events related to the product as it travels between locations. By providing global standards on how to attach information to products, EPC enables organizations to share information more effectively. The vision of EPCglobal is to facilitate a worldwide, multi-sector industry adoption of these standards that will achieve increased efficiencies throughout the supply chain—enabling companies to have real-time visibility of their products from anywhere in the world.

[12] EPCglobal ratified Standards can be downloaded at: http://www.epcglobalinc.org/standards_technology/ratifiedStandards.html

The Board Of Governors of EPCglobal is composed by the following enterprises: P&G, GS1, Sony, Lockheed Martin, Wal*Mart, DHL, HP, Metro, Cisco, Novartis, Johnson&Johnson, OAT Systems, USA DoD. It is composed by leader companies (20% user and 80% technology) that are using RFID, most notably the giant U.S. based Wal*Mart supermarket chain, and houses very few technology providers. This distribution mimics the intentions of EPCglobal in order to ensure that supply chain process requirements, settled by user companies, lead the standardization process: RFID should be kept functional to supply chain purposes. In this situation the US do not have a dominant position with respect to Asia or Europe: supply chain requirements are the same all over the world. On the other hand, probably in virtue of the nationwide availability of UHF frequencies, the US appears to be in front of the others in terms of trials and operational RFID automated installations. Whereas Wal*Mart and the DoD play the star role in the US, in Europe METRO and TESCO run short behind.[13]

In *Table 3-1* an overview of the different EPC protocols is summarized: the recent EPCglobal Generation 2 protocol (chosen by Wal-Mart for its RFID adoption) is reported as Class 1 Version 2 according to EPC Protocol naming.

Table 3-1: EPCglobal Protocol[14]

Protocol	Frequency	Description
Class 0	UHF	Read-Only – Manufacturer pre-programming
Class 0 Plus	UHF	Read-Write
Class 1	HF/UHF	Write-once, Read-Many (WORM)
Class 1 Ver. 2	UHF	WORM
Class 2	UHF	Read-Write Tag

With reference to the EPCglobal framework the relevance of the specification activity being carried out to define the framework architecture should be noted. This activity has the objective to allow for the worldwide retrieval of information, from manufacturing to retail, regarding some product item. Each organization involved in the manufacturing and distribution of some product might publish, by means of the “Information Service” component, information regarding the local treatment of the product item. During the whole process down to the actual exploitation of the product item, this information can be made available to consumers too, by means of the “Discovery Service” and the “Object Naming Service” (ONS) through a system similar to the Domain Name Service-DNS of the Internet.

The recent EPCglobal Generation 2 protocol (chosen by Wal-Mart for its RFID adoption) is one of the most discussed in the last year because it promises good range and performances.

As a general consideration it should be said that the currently relevant EPCglobal specifications are the low level technology, i.e. the tag radio interface, and the coding, i.e. the Electronic Product Code –EPC. The first one is critical to allow the possibility of reading worldwide the EPC tags and the second one allows the possibility of having a unique worldwide way of coding the tags. The other published specification, namely ALE, is to be considered as more manufacturer related in order to foster the independent development of supply chain applications and RFID infrastructure. Still under development is the other relevant and probably even more impacting EPC Information Services (EPC-IS) interface. When available this will allow the automation of supply chains among different companies.

[13] The organization has set itself tough targets in developing standards and interfaces for most of the elements of an RFID system, as follows: a) The Electronic Product Code (EPC), b) The standards for the ID System describing the functions, interfaces and communications protocols for the reader and tag, c) EPC Middleware that will sit between RFID readers and enterprise applications, ensuring that erroneous, duplicated and redundant information is filtered out, d) The Object Name Service (ONS) that will be operated by Verisign under contract to EPCglobal, e) The EPC Information Service (EPC-IS) that will store, host and provide access to serial number specific information about products as they pass along a supply chain, f) The EPC Discovery Service providing subscribers to EPCglobal and EPC-IS with additional information about individual items for tracking and tracing purposes.

[14] The latest protocol is highlighted

3.2. International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is a network of national standards institutes of 148 countries working in partnership with international organizations, governments, industries, and business and consumer representatives. The ISO asserts jurisdiction over the Air Interface (the frequency spectra used for RFID transmission) through standards-in-development ISO 18000-1 through ISO 18000-7. Members[15] of ISO are worldwide national organizations for standardization. For example the United States are members through American National Standards Institute (ANSI), France through Association Française de Normalisation (AFNOR), Italy through Ente Italiano di Unificazione (UNI).

International Organization for Standardization (ISO) in collaboration with the International Electrotechnical Committee (IEC) has produced a set of standards for the interface between reader and tag, operating at various radio frequencies. As mentioned, these standards are numbered in the series ISO/IEC 18000-n and detailed in the following.

3.2.1. ISO/IEC 18000 information technology AIDC techniques - RFID for item management - air interface

- 18000-1 Part 1 – Generic Parameters for the Air Interface for Globally Accepted Frequencies
- 18000-2 Part 2 – Parameters for Air Interface Communications below 135 kHz
- 18000-3 Part 3 – Parameters for Air Interface Communications at 13.56 MHz
- 18000-4 Part 4 – Parameters for Air Interface Communications at 2.45 GHz
- 18000-5 Part 5 – Parameters for Air Interface Communications at 5.8 GHz (Withdrawn)
- 18000-6 Part 6 – Parameters for Air Interface Communications at 860 to 960 MHz
- 18000-7 Part 7 – Parameters for Air Interface Communications at 433 MHz

The first part is the defining document that explains how the standard works and the rest are divided by frequency. A revision to all the parts of 18000 will include fixes to the standards based on actual issues discovered during the use of the standards along with the addition of the capabilities to use batteries and sensors with the existing technologies. Work has started on this area at the end of 2005.

3.2.2. 18000-1 Part 1 – generic parameters for the air interface for globally accepted frequencies[16]

ISO/IEC 18000-1:2004 defines the parameters to be determined in any Standardized Air Interface Definition in the ISO/IEC 18000 series. The subsequent parts of ISO/IEC 18000 provide the specific values for definition of the Air Interface Parameters for a particular frequency or type of air interface, from which compliance (or non compliance) with ISO/IEC 18000-1:2004 can be established. ISO/IEC 18000-1:2004 also provides description of example conceptual architectures in which these air interfaces are often utilized.

ISO/IEC 18000-1:2004 limits its scope to transactions and data exchanges across the air interface at Reference Point Delta. The means of generating and managing such transactions, other than a requirement to achieve the transactional performance determined within ISO/IEC 18000-1:2004, are outside its scope, as is the definition or specification of any supporting hardware, firmware, software or associated equipment.

ISO/IEC 18000-1:2004 is an enabling standard that supports and promotes several RFID implementations without making conclusions about the relative technical merits of any available option for any possible application.

[15] The complete list of ISO members is available at: http://www.iso.org/iso/en/aboutiso/isomembers/index.html

[16] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=34112

3.2.3. 18000-2 Part 2 – parameters for air interface communications below 135 kHz[17]

ISO/IEC 18000-2:2004 defines the air interface for radio-frequency identification (RFID) devices operating below 135 kHz used in item management applications. Its purpose is to provide a common technical specification for RFID devices to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. ISO/IEC 18000-2:2004 defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order. It further defines the communications protocol used in the air interface.

ISO/IEC 18000-2:2004 specifies:

- the physical layer that is used for communication between the interrogator and the tag;
- the protocol and the commands;
- the method to detect and communicate with one tag among several tags ("anti-collision").

It specifies two types of tags: Type A (FDX) and Type B (HDX). These two types differ only by their physical layer. Both types support the same anti-collision and protocol. FDX tags are permanently powered by the interrogator, including during the tag-to-interrogator transmission. They operate at 125 kHz. HDX tags are powered by the interrogator, except during the tag-to-interrogator transmission. They operate at 134.2 kHz. An alternative operating frequency is described.

An optional anti-collision mechanism is also described.

3.2.4. 18000-3 Part 3 – parameters for air interface communications at 13.56 MHz[18]

18000-3 ISO/IEC 18000-3:2004 provides physical layer, collision management system and protocol values for RFID systems for item identification in accordance with the requirements of ISO 18000-1. It relates solely to systems operating at 13.56 MHz.

ISO/IEC 18000-3:2004 has two modes of operation, intended to address different applications. The modes, whilst not interoperable, are non-interfering:

- Mode 1 is based on 15693 with additions/changes to better suit the Item management market and improve the compatibility between vendors;
  - The Interrogator to Tag data rate is 1.65 kbps (fc/8192) or 26.48 kbps (fc/512);
  - The Tag to Interrogator data rate is 26.48 kbps (fc/512). The protocol extension has a precursor data rate ~ 52.97 kbps (fc/256) and a main reply data rate ~105.94 kbps (fc/128).
- Mode 2 is a high speed interface.
  - The Interrogator to Tag data rate is 423.75 kbps;
  - The Tag to Interrogator data rate is 105.9375 kbps on each of 8 channels.

Both of the MODES require a license from the owner of the Intellectual Property, which shall be available on terms in accordance with ISO Policy.

3.2.5. 18000-4 Part 4 – parameters for air interface communications at 2.45 GHz[19]

ISO/IEC 18000-4:2004 defines the air interface for radio-frequency identification (RFID) devices operating in the 2.45 GHz Industrial, Scientific, and Medical (ISM) band used in item management applications. Its purpose is to provide a common technical specification for RFID devices that may be used by ISO committees developing RFID application standards. ISO/IEC 18000-4:2004 is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. ISO/IEC 18000-4:2004 defines the

[17] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=34113

[18] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=34114&ICS1=35&ICS2=40&ICS3

[19] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=34115

forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum EIRP, spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order, and where appropriate operating channels, frequency hop rate, hop sequence, spreading sequence, and chip rate. It further defines the communications protocol used in the air interface.

ISO/IEC 18000-4:2004 contains two modes. The first is a passive tag operating as an interrogator talks first while the second is a battery assisted tag operating as a tag talks first.

Mode 1: Passive backscatter RFID system - The FHSS backscatter option or the narrow band operation RFID system shall include an interrogator that runs the FHSS backscatter option 1 RFID protocol or in narrow band operation, as well as one or more tags within the interrogation zone

Mode 2: Long range high data rate RFID system - This clause describes a RFID system, offering a gross data rate up to 384 kbps at the air interface in case of Read/Write (R/W) tag. In case of Read Only (R/O) tag the data rate is 76.8 kbps. The tag is battery assisted but back scattering. By using of battery powered tags such a system is well designed for long-range RFID applications.

This air interface description does not explicit claim for battery assistance in the tag, also real passive tags or tags for mixed operation are conceivable.

3.2.6. 18000-5 Part 5 – parameters for air interface communications at 5.8 GHz

This part has been withdrawn at the final voting in 2003. No ISO 18000-5 standard is thus available and it will not become a standard unless an ISO member puts forward a new proposal and starts the lengthy standards process all over again It is here mentioned for completeness. The lack of this standard will cause the emergence of non-interoperable proprietary solutions but this might not be a problem as the applications for active tag systems are mostly localized. Other related standards, as those for DSRC[20] (Dedicated Short Range Communications), might take over ISO.

3.2.7. 18000-6 Part 6 – parameters for air interface communications at 860 to 930 MHz[21]

ISO/IEC 18000-6:2004 defines the air interface for radio-frequency identification (RFID) devices operating in the 860 MHz to 960 MHz Industrial, Scientific, and Medical (ISM) band used in item management applications. Its purpose is to provide common technical specifications for RFID devices that may be used by ISO committees developing RFID application standards. ISO/IEC 18000-6:2004 is intended to allow for compatibility and to encourage interoperability of products for the growing RFID market in the international marketplace. ISO/IEC 18000-6:2004 defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum EIRP, spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order, and where appropriate operating channels, frequency hop rate, hop sequence, spreading sequence, and chip rate. It further defines the communications protocol used in the air interface.

ISO/IEC 18000-6:2004 contains one mode with two types. Both types use a common return link and are reader talks first. Type A uses Pulse Interval Encoding (PIE) in the forward link, and an adaptive ALOHA collision arbitration algorithm. Type B uses Manchester in the forward link and an adaptive binary tree collision arbitration algorithm.

ISO/IEC 18000-6:2004 has been updated to include the EPCglobal Generation 2 specification as Type C as well as fix issues in relation to Types A and B. This is published as an Amendment to the standard.[22]

[20] More details are available at http://grouper.ieee.org/groups/scc32/dsrc/worldwide/inde.html

[21] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=34117

[22] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=43923

3.2.8. 18000-7 Part 7 – parameters for air interface communications at 433 MHz[23]

ISO/IEC 18000-7:2004 defines the air interface for radio-frequency identification (RFID) devices operating as an active RF Tag in the 433 MHz band used in item management applications. Its purpose is to provide a common technical specification for RFID devices that may be used by ISO committees developing RFID application standards. This standard is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. ISO/IEC 18000-7:2004 defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum power, spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order, and where appropriate operating channels, frequency hop rate, hop sequence, spreading sequence, and chip rate. ISO/IEC 18000-7:2004 further defines the communications protocol used in the air interface.

3.3. ISO/IEC 14443[24]

ISO 14443 defines a proximity card used for identification that usually uses the standard credit card form factor defined by ISO 7810 ID-1. Other form factors also are possible. The RFID reader uses an embedded microcontroller (including its own microprocessor and several types of memory) and a magnetic loop antenna that operates at 13.56 MHz.

The standard consists of four parts and describes two types of cards: type A and type B. The main differences between these types concern modulation methods, coding schemes (part 2) and protocol initialization procedures (part 3). Both type A and type B cards use the same high-level protocol (so called T=CL) described in part 4. The T=CL protocol specifies data block exchange and related mechanisms. The diffused MIFARE cards comply with ISO14443 part 1, 2 and 3 type A.

Part 1: Physical characteristics

Part 2: Radio frequency power and signal interface
Amd 1:2005 Bit rates of fc/64, fc/32 and fc/16

Part 3: Initialization and anti-collision
Amd 1:2005 — Bit rates of fc/64, fc/32 and fc/16
Amd 3:2006 Handling of reserved fields and values

Part 4: Transmission protocol
Amd 1:2006 Handling of reserved fields and values

3.4. European Telecommunications Standardization Institute – ETSI

In the following details are given for the most relevant ETSI standards with relationship to RFID. Among them, EN 302 208 has been approved in 2005 and is relevant to EPCglobal Class 1 Gen 2 specifications.

3.4.1. EN 300 330

EN 300 330: Radio Equipment and Systems - Short range devices, Technical characteristics and test methods for radio equipment to be used in the 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz.

This standard defines the characteristics of RFID systems operating at LF and HF.

Part 1: Technical characteristics and test methods[25]

Part 2: Harmonized EN under article 3.2 of the R&TTE Directive[26]

3.4.2. EN 300 220

EN 300 220: Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the

[23] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=37978

[24] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=28728

[25] http://webapp.etsi.org/action/V/V20060324/en_30033001v010501v.pdf

[26] http://webapp.etsi.org/action/V/V20060324/en_30033002v010301v.pdf

25 MHz to 1000 MHz frequency range with power levels ranging up to 500 mW;

The standard is relevant to UHF (433 MHz and 860-960 MHz) RFID. Nevertheless the power limitation to 500mW allows only for a limited read range (<1m).

Part 1: Technical characteristics and test methods[27]

Part 2: Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive[28]

3.4.3. EN 302 208

EN 302 208: Electromagnetic compatibility and Radio spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W;

The standard is relevant to UHF 860-960 MHz RFID. These UHF channel allocations for ETSI countries allow 2W (ERP) operation. The standard will permit operation in Europe of product built in compliance with ISO 18000-6. EN 302 208 provides for the operation of RFID at UHF frequencies. It should be noted that this has not yet been endorsed by all EU countries.

Part 1: Technical requirements and methods of measurement[29]

Part 2: Harmonized EN under article 3.2 of the R&TTE Directive[30]

3.4.4. EN 300 440

EN 300 440: Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range;

Part 1: Technical characteristics and test methods[31]

Part 2: Harmonized EN under article 3.2 of the R&TTE Directive[32]

3.4.5. EN 300 328[33]

EN 300 328: Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

The standard is relevant to microwave (2.45 GHz) RFID.

3.4.6. EN 300 674[34]

EN 300 674: Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5.8 GHz Industrial, Scientific and Medical (ISM) band;

Dedicated Short Range Communication (DSRC) at 5.8 GHz - ElectroMagnetic Compatibility and Radio Spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Technical characteristics and test methods for DSRC transmission equipment (500 kbit/s /250 kbit/s) operating in the 5.8 GHz Industrial, Scientific and Medical (ISM) band.

Part 2: Harmonized EN under article 3.2 of the R&TTE Directive

Sub-part 2: Requirements for the On-Board Units (OBU)

[27] http://webapp.etsi.org/action/PE/PE20050805/en_30022001v020101c.pdf

[28] http://webapp.etsi.org/action/V/V20060324/en_30022002v020101v.pdf

[29] http://webapp.etsi.org/action/OP/OP20060714/en_30220801v010102o.pdf

[30] http://webapp.etsi.org/action%5CV/V20040903/en_30220802v010101v.pdf

[31] http://webapp.etsi.org/action/V/V20010907/en_30044001v010301v.pdf

[32] http://webapp.etsi.org/action/V/V20010907/en_30044002v010101v.pdf

[33] http://webapp.etsi.org/action/OP/OP20060922/en_300328v010701o.pdf

[34] http://webapp.etsi.org/action/PU/20040810/en_3006740202v010101p.pdf

3.5. Conformance testing

EPCglobal has given to a company named MET[35] the mandate to organize the so called EPCglobal inc. Hardware and Performance Testing Programs. **Only this centralized lab** is allowed to certify the compliance to EPCglobal standards. This applies only to manufacturers that want their equipment to be marked as EPCglobal compliant.

Would manufacturers want to sell their equipment in Europe, they should be as well certified by ETSI accredited labs. But this should be also completed by compliance to other directives as those concerning Electro Magnetic Compatibility (EMC).

As far as the testing equipment, it probably could be said that there is no special need: probably any telecommunication conformance testing lab should be already skilled enough to certify the compliance of some RFID equipments to the ETSI standards and to the different national and European directives.

It should be noted that conformance testing of RFID equipment is mainly relevant for the extended supply chain, namely the one where the same tag is companion to a product from its manufacturer premises down to the consumer home. In the case of the so-called "closed loop" supply chain, where the tags are applied on the containers which are used to move goods inside the company and never exit, then compliance is much less relevant: all that is needed is that the tag can be read by the readers and in these cases this is ensured by using technology of a single manufacturer.

3.6. Interoperability issues

Standards are generally critical where there is the need to ensure interoperability among systems developed by different manufacturers and, in more general terms, where the development of a product market requires fostering. For RFID a number of application examples is hereafter reported, discussing interoperability issues.

Integrated Logistics – Standards are clearly needed as tagged items can be shipped worldwide and tags applied in EU should be readable in Asia and the US, and vice versa. Poor standardization might cancel any benefit of the technology.

Asset Management – This means that assets (i.e. valuable equipment as well as containers of spare parts) within a company are tagged e.g. for a better production process control. In this case, while standards are useful in order to develop a product market, they are not essential: as the technology operates inside each company, a single vendor solution can fit the requirements and allow for the development of innovative solutions.

People and animal identification – While proprietary solutions might be acceptable in a first phase, in the long term standard approaches will be mandatory in order to exploit the technology. An RFID identity card should eventually be globally readable by means of devices complying with a global standard. The same criteria apply to animal identification in order to allow for the tracking across borders.

E-payment – This case is similar to the previous one also in terms of the technology. The banking sector might have enough power to develop their own solutions and impose them to manufacturers.

Toll payment – Highway toll payment should also be standardized to support "roaming" like services across different operators and/or countries.

Access Management – This refers to solutions deployed inside a company or an organization in more general terms. Each employee holds a personal RFID badge that (included in an access control system using identifiers such as biometrics) allows the entrance in protected areas. Though this application does not require a global standard, RFID standards for people identification are desired.

Car keys – Each car manufacturer might install proprietary solutions as each key should just work with the reader installed inside the car. Manufacturers' de-facto standards are emerging.

[35] *http://www.metlabs.com/pages/RFID.html*

4. RFID technologies: RFID system features

In Section 4.1 we scope RFID to some basic components and define two distinguishing usage scenarios which we will use throughout the rest of this deliverable.

Section 4.2 focuses on the key technologies for future RFID implementation. Based on the classification of technologies around RFID we present here a schematic overview of technologies and their capabilities in relation to RFID.

In Section 4.3 a view is presented on the RFID tag lifecycle process and the states in the lifecycle. Finally, a future development of the technology is presented.

In Section 4.4 a typology on RFID usage is presented. Based on a three layered viewpoint model and a usage domain model, the RFID usage typology is described. In this chapter different usage domains are positioned against RFID related aspects.

4.1. The RFID-systems perspective

The main capability RFID offers is to link events from the real world, actual movement of objects, to business control software. In other words RFID helps to virtualise some of the real world around us. This Section presents a vision how to use RFID in the most optimal manner.

4.1.1. RFID definition and positioning

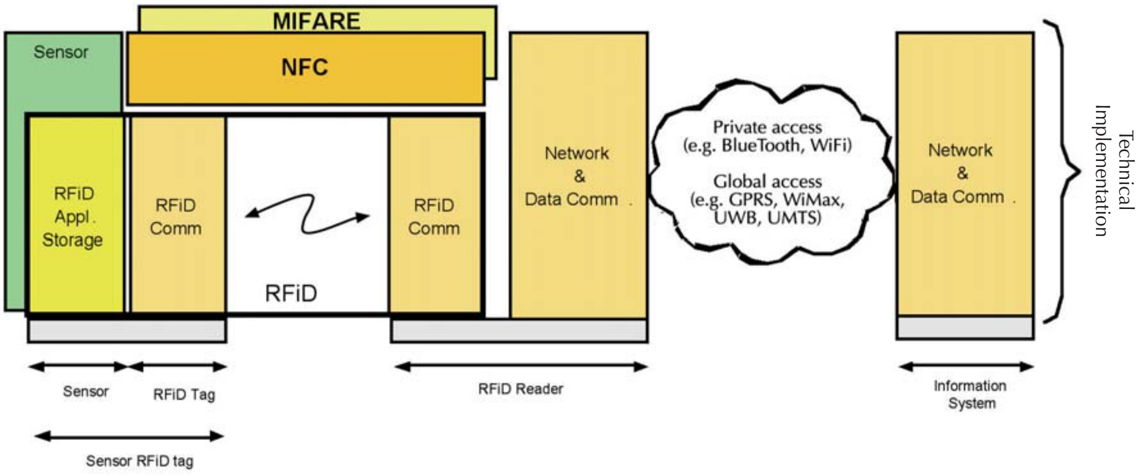
In order to be able to position RFID in relation with other technologies, to place it in a context, we use the view presented in Figure 4-1. This view contains readers as well as tags. It shows that RFID provides functionality to exchange RFID data (RFID Comm) and to store application data on the tag. However, the application data itself is not part of the RFID definition, but can be used e.g. by a sensor application.

The figure shows RFID technology, consisting of readers and tags. When it is complemented with storage and/or sensors a more advanced (sensor) tag can be constructed.

In order to interpret information on tags, the reader must be connected to some information processing system. This connection can be made via different wired or wireless network technologies (Network & Data Comm).

The figure shows also that there are other technologies which are based upon (part of) RFID and extend them. Near Field Communication (NFC) and Mifare are such technologies.

Figure 4-1: Positioning of RFID-system



4.1.2. Two views on using RFID

Two perspectives (or abstract usage domains) can be discerned when looking at how RFID can be used in present and future environments:

- RFID for business process automation
  In this perspective RFID is used to automate a single business process. This can be a very large business process, but the focus is on the internals of this business process and how to automate them.
- RFID for business domain computerization
  In this perspective RFID is used in an entire business domain. Therefore we speak about computerization; entire processes will change due to the use of RFID within the domain.

The main capability RFID offers is to link events from the real world, for instance the actual movement of objects, with business control software. The next paragraph discusses this in more detail.

4.1.3. Aspects for object virtualization

In order to virtualize an object into the computer three aspects are important:

- *Identification*
  An object in the real world must be identifiable in order to uniquely collect information about that object and, if desirable, change it.
- *Location*
  Each identifiable object in the real world has, at a specific point in time, a specific location.
- *State*
  The state of an object is the determination of specific characteristics of that object, other then its identity and its location, e.g. its colour, temperature, etc. Movement and speed of the object is also dimension of state.

RFID is not the only technology which can be used to collect these aspects. A number of other technologies are available that offer similar functionality. Notwithstanding the differentiation in technology, the features of virtualisation (identification, location and state) will remain the same. Certain technologies are specifically designed for one of these aspects, e.g. a temperature sensor to collect the temperature state of an object. Others offer information about two or all three aspects.

RFID is designed for identification, but offers also limited location information. After all, at the moment the RFID tag is scanned by the RFID reader, the location of the tag is also known. Therefore also the location of the object the tag is attached to is known

RFID can also be used to collect state information. Some tags have memory which can be used freely, for instance to store specific context information about the object.

This all turns RFID into a promising technology for implementation in a (sensor based) network.

4.2. RFID system perspective

This section presents an overview of the relationship of RFID with network technologies. To enable a fruitful comparison, we will introduce a typology to indicate the relation between RFID and network technologies: they enable each other, they enhance each other, or they are concurrent to each other.

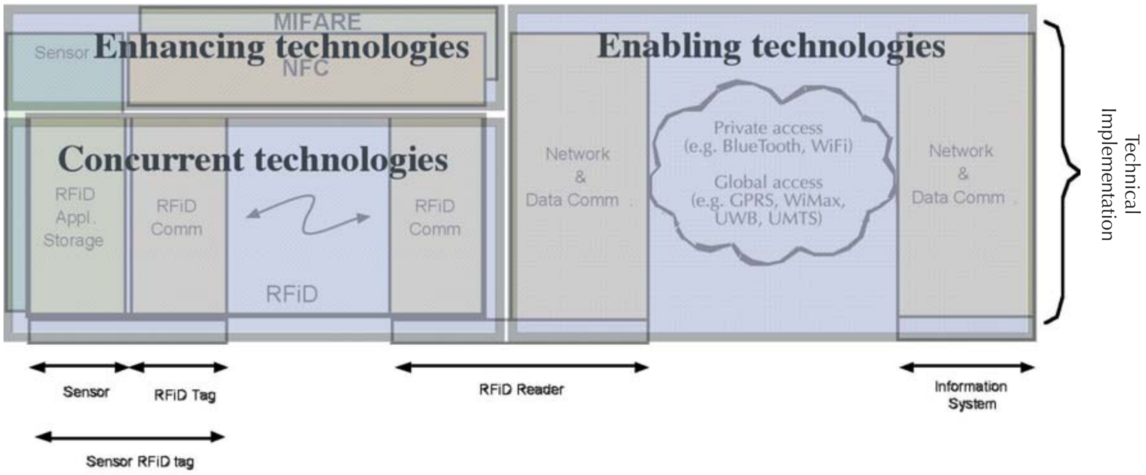
4.2.1. Classification of technologies around RFID

We identify three classes to order the relation between RFID and network technologies:

- Enabling technology
- Enhancing technology
- Concurrent technology

In *Figure 4-2* these classes are mapped onto the RFID positioning figure from section 4.1 and will be used to characterize the different technologies.

Figure 4-2: Classification of technologies around RFID



On top of the RFID model introduced in the previous section, the three classes are drawn, each pinpointing to distinct aspects of RFID: the enabling class on top of the network, the enhancing class on top of the RFID extensions and the concurrent class on top of the basic RFID functionality. Each of these classes represents a different way to compare RFID with other technologies.

We do not imply that network technologies are uniquely positioned towards one of the identified aspects of RFID. A technology such as Zigbee can be placed in more than one class. Zigbee can be seen as a LAN technology, connecting RFID readers in a larger network. But Zigbee is also part of the concurrent class because it can compete with active RFID in offering a solution for identification and location.

4.2.2. Enabling technologies

The enabling technology class is about communication technologies which enable the use of RFID and increase the application area of RFID. As shown in Figure 4-1, this class is about connecting the RFID readers with the back-end of RFID systems. Without a network only local RFID solutions are possible, for instance a standalone PC or PDA with a RFID reader. Due to enabling technologies it is possible to distribute RFID readers around a larger area.

Examples of often used communication technologies to connect RFID readers onto a network are listed below. Note this paragraph is about the enabling technologies. They make a remote and or mobile RFID reader possible.

- *Local Area Networks (LAN)*

  LAN networks can be used to distribute the RFID readers over a remote location within a building or premises. Some of them are wireless, others are wired. Note that in each case the RFID reader must be equipped with the appropriate interface, or an adapter device must be added. Note that most RFID readers on the market today still have only a serial (RS232/RS485) interface.

  - *Ethernet / UTP (IEEE 802.3)*

    A cable technology very widely used to connect computers to a network, Internet or intranet. The network topology are stars (connecting local computers), connected to each other possibly forming a very large network.
    Speeds between 10 Mbits/s and 1 Gbits/s are common, the current standard is 100 MBits.s.

  - *UWB (IEEE 802.15)*

    UWB stands for Ultra Wide Band, a wireless technology still in development. UWB does not have its own single frequency; it uses existing frequencies of other technologies. By using very low transmission power it stays within the background noise of the other technologies, so there is no interference. Depending on the range, with UWB speeds ranging between 1Mpbs (100m) and 400Mbps (4m) this technology is expected to hit the mass market by 2008.

- *Wifi / WLAN (IEEE 802.11)*
  A wireless network technology, often used as a wireless version of Ethernet. Speeds between 11Mbits/s and 54Mbits/s are commonly used.
- *ZigBee (IEEE 802.15.4)*
  This network is especially designed for low power, mesh networks. Therefore it is very suitable to connect sensors and RFID readers. It will last a long period of time with one battery, typically 3 years. It can easily adapt to changes in network topologies if sensors are moved around, added or removed.
  ZigBee can only transfer limited amounts of data, several 100kbits/s within the entire ZigBee network, so individual elements can only transmit a portion of that per time-period.
  In general such mesh networks are called Wireless Sensor Networks (WSN). These networks are self organizing, enabling a dynamic multi hop infrastructure. This means that the network topology can continuously change while the network keeps its functionality and each node can communicate with all the other nodes. Topology changes can occur due to failure of one of the nodes or because the nodes are mobile and move, constantly changing the wireless nodes in reach.

- *Wide Area Networks (WAN)*

  WAN networks are used when the RFID readers must be distributed over a much larger area compared to LAN technologies or when a user does not have access to the local LAN networks.

  - *GPRS*
    GPRS stands for General Packet Radio Server. It is an addition on GSM (Global System for Mobile Communications), a network which many countries use for their mobile phone infrastructure. Depending on the used local network operator, mobile phone coverage over the entire country is not exceptional.
    GSM/GPRS can operate in three different frequencies: 900 Mhz, 1800 Mhz and 1900 Mhz. GPRS can reach speeds up to 52 kBits/s
  - *UMTS*
    The Universal Mobile Telecommunications System is introduced as the successor of GSM/GPRS. Therefore it is called a third generation (3G) mobile communication technology. Speeds of 384Kbits/s are possible and in theory even 2Mbits/s. At this moment it starts to become available, but is still expensive to use.
  - WiMAX
    The Worldwide interoperability for Microwave Access is an emerging standard which will come to the market in the next couple of years. First field trials are already taking place. In theory ranges up to 50km are possible and speeds up to 80Mbit/s at short distances. WiMAX is seen as an alternative for GSM and UMTS, but also for ADSL or cable connections. At this moment it is too early to predict the future of WiMAX.

- *Personal Area Networks (PAN)*

  PAN networks are used when the RFID reader are located at very close distance (up to a few meters) to the person operating them. In most cases the RFID reader will be mobile and connected to or integrated with a PDA or mobile phone.

  - *Bluetooth*
    Has been developed for replacing the local wires around a computer, some people call it therefore a wireless wire. It is described in the IEEE 802.15.1 standard. Speeds are between 1 and 10Mbits/s and it has a range of 1-100 meters depending on the class.
    Bluetooth starts to become standard in most laptops and mobile phones, enabling easy wireless access to a number of devices. A drawback of Bluetooth is that it needs relatively much power, so battery based devices like mobile phones have to be recharged more often.

Pencil-like RFID readers with a Bluetooth interface to a mobile phone or PDA start to become available.

4.2.3. Enhancing technologies

The enhancing technology class is about technologies which extend the usage of RFID, they *enhance* RFID. By adding extra functionality upon the basic RFID capabilities on the tag, new applications become possible. Some of these additions fit perfectly in the passive RFID tag model, they do not need a power source of their own. Others need an additional battery on the tag. They also want to perform tasks when the tag is not within the field of a reader, therefore a more predictable energy source is needed like a battery. Note that some extensions are made just on the tag (memory), other extensions need changes both on the tag and in the reader (security) while some extensions take place outside the direct scope of RFID (service platform).

In the next three subsections different enhancing technologies will be discussed. We will look at powerless extensions, battery based extensions and devices that combine the reader and tag functionality.

Powerless extensions

The two most important powerless extensions of a RFID tag are adding:

- Memory
- Security

Additional memory is a very common extension; most RFID tags are capable of storing additional data. This is a necessity if a specific ID must be stored on the tag, next to the factory UID (Universal IDentifier). The factory UID is determined during the production process of the tag and each tag has memory to store the UID.

Other use of additional memory is storing information about the object it is related to. For instance colour, size or maintenance track record of the object, etc. Also biometrical data can be stored in the memory of the tag, for instance in your passport. Biometrical devices can scan your fingerprint or eye and compare it with the data on the passport to check if you are who you say you are. At this moment there are no tags which allow changing the program of the tag itself to change its behaviour. Only configuration parameters which control the behaviour of the tag can be stored in memory. Think about starting or stopping a sensor log, etc. In most cases the additional memory on a tag is used to store just static data which can be updated from time to time.

RFID in itself is not a very secure technology. Tags can easily be read using a reader and the wireless communication can be monitored by others. For situations where more security is needed, for instance access control to buildings, special *security* extensions are developed. They make it possible to communicate, in a secure manner, secrets between the tag and the reader. The two most important standards which make this possible are the smartcard standards of Philips: Mifare and Sony: Felica. Most commonly they are used in company cards to unlock doors, logon to computers, etc.

Battery-based extensions

A battery is needed to make additional functionality of the RFID tag possible. Therefore, a major factor in extending RFID is the development of small, powerful, flexible batteries. By combining a RFID tag and such a battery, a device is created with the form factor of a credit card. The battery offers a constant power supply on the tag, even if the tag is not within the field generated by the reader.

To save energy most tags are active only during very short periods of time. The active periods are controlled by timers, e.g. tag is activated to take a measurement once a minute. For this type of tags lifetime of 3-7 years is possible.

There are three main purposes to add a battery to a RFID tag:

- To add functionality on the RFID tag, in most cases sensors.
- To boost the communication range between the tag and the reader.
- When the tag has a boosted communication range, it becomes possible to let the RFID tag initiate an event by itself, instead of waiting until it gets interrogated by a reader.

Additional functionality

Adding a battery to an RFID tag opens a whole new range of possibilities: adding sensors to the tag, measuring an external aspect in the real world. For instance, temperature, humidity, a toxic substance, movement, etc. Measurement information can be stored on the tags' memory and can be read via a RFID reader. Measurements can be taken at certain intervals, for instance every minute. But also event based measurement is possible, when the temperature raises above a certain threshold for instance, the timestamp of that event is logged.

Using this mechanism, it becomes possible to pinpoint to specific events, for instance the moment an object was undesirably defrosted. Imagine the situation when deep frozen fish food was moved from a cooling container into a cooling truck and was left for 2 hours in the sun. Afterwards it was frozen in again within the truck. Using temperature logging tags these fluctuations in temperature can be traced and reported back to responsible parties.

Communication range boost

RFID tags which use a battery to boost its communication range, are called "active RFID" tags. They use a different frequency than passive RFID, but they work in the same way as passive RFID tags. Most active RFID systems can cover an area within range of maximum 200m in an ideal situation. In reality physical obstacles such as walls, metal (cars), water, etc have a significant influence.

Because an active RFID tag transmits a signal of its own, special signal strength algorithms can be used to determine more precisely the location of the object. In contrast, passive RFID-systems, which have typically a read range of about between 0.1 and 0.5m, can give an accurate (0.1 - 0.5m tolerance) location of the tag if it is in the field of the reader. At the moment the tag has left the reader field, the location becomes unknown.

Tag event initiation

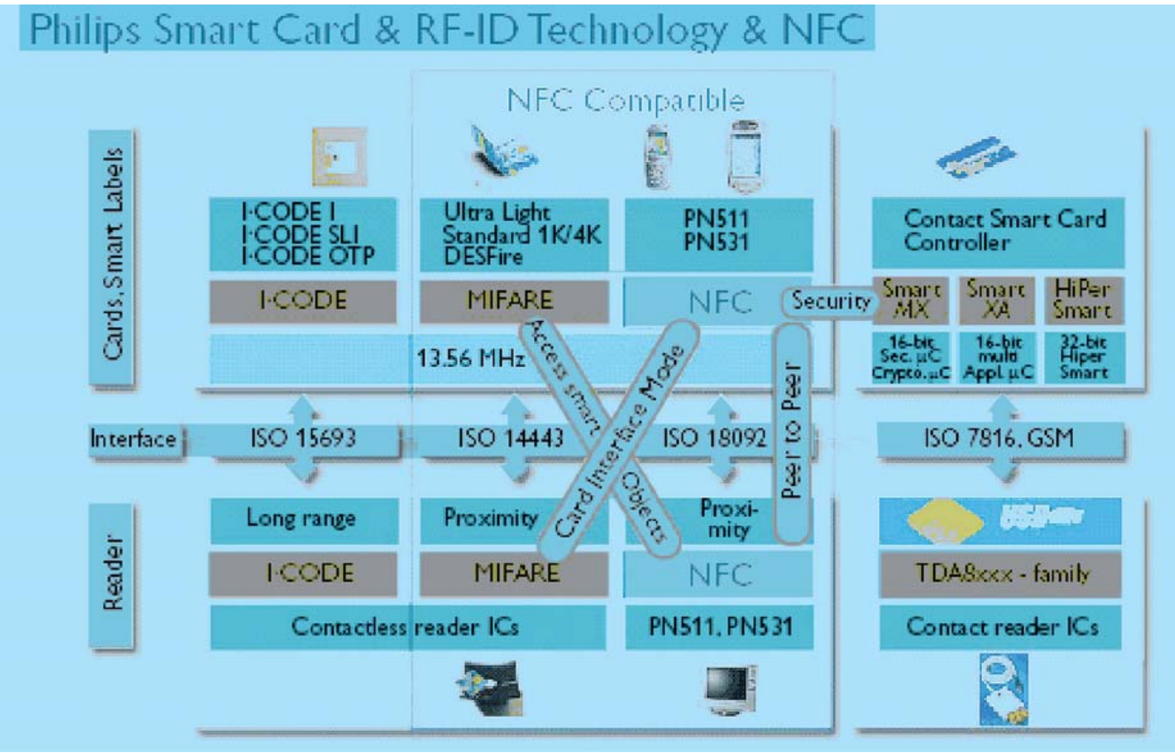
Active RFID tags have the opportunity to initiate an event by themselves. Because the communication range is in most cases large enough to cover the entire desired area, tags have the opportunity to communicate data to readers at all times. In combination with a sensor this provides a powerful tag. For instance, by putting a movement sensor on an active RFID tag, a surveillance monitor system for a museum can be build. Putting an active movement tag on the back of each painting, these paintings can be monitored at all times. When a painting is removed from its place, this event can directly be reported to the surveillance system. The very moment someone, thief or personnel, is moving the painting, the sensor on the tag will trigger an event and the tag will emit a signal. If the painting is scheduled to move, the alert will be notified but nothing will happen. But if the painting is not scheduled to move, the alert may alarm security officers. In fully automated (i.e. virtualized) systems, it will become possible to integrate the various planning and alert systems, leading to fully automated alarms when something is occurring which has not been foreseen by the integrated system. But even with less sophisticated systems, the thief can be tracked by the paintings-tag within the museum using the location algorithms of the active RFID solution.

Combination of reader and tag in one device

Besides adding power and functionality, there is a third method of enhancing RFID: combining the tag and reader into one device. This offers two-way communication between both devices, each device can act as either a tag or a reader. Especially for mobile equipment, e.g. a PDA or mobile phone, this can be a useful feature. Sometimes the PDA acts like a tag, communicating with existing readers. On other moments the PDA can read RFID tags itself.

The only technology at this moment which is using this approach is NFC: *Near Field Communication*. NFC started as cooperation between Philips and Sony in 2002, Nokia joined soon afterwards. NFC is designed, as the name already indicates, for very short range (10 cm) wireless communication. Its purpose is to securely transport small amounts of data mainly for configuration purposes or initiating actions and/or communication. It uses the 13.56 MHz RFID frequency and has a data exchange rate of up to 424 kbit/s.

Figure 4-3: NFC architecture



NFC is a smart combination of existing and new technologies. For secure communication it relies on Mifare / FeliCa. Both technologies are compatible with each other and are using widely accepted standards for secure RFID. Payment possibilities are added using existing SmartCard technology. Besides combining all these existing technologies, the only really new feature of NFC is two-way communication.[36] This makes it possible to exchange information between two NFC devices in an efficient manner. The focus of NFC is on small amounts of data and not on streaming data flows. It can however be perfectly used to set up a streaming data flow, automatically configuring all the aspects needed to make the stream flow. In case of configuring a WiFi connection, think about the IP address and mask the IP address of the DNS server, WEP key, etc.

The main application areas for NFC:

- Configure the device to use securely an existing communication network such as WiFi or Bluetooth. Setting up the necessary keys, IP addresses, etc. can be quite complex. With NFC you only have to hold the two devices close to each other and the necessary configuration information can be exchanged in a secure manner.
- Configure consumer appliances to interact with each other. For instance holding your mobile phone next to the audio system will automatically configure the mobile phone and the audio system to start streaming your favourite mp3s.
- Configure the train ticket you need. Just by holding your NFC enabled phone / PDA towards a map of the railway stations, the exact e-ticket from the current station towards the desired station can be transmitted to your device.
- The SmartCard technology within NFC can assist in the payments for goods or tickets, using a standard way to specify how much money between which parties must be transferred. A special service provider, a bank for instance, will perform the actual money transfer.

[36] Two-way communication is defined as a mode where both communication partners are able to initiate communication. However, in a session it is possible that one or both partners are sending information; the first one with requesting data, the second optionally with response information.

The future of NFC is still uncertain. At this moment a number of field trials are happening all over the world. There are still a very limited number of mobile phones equipped with NFC, let alone WiFi base stations, TVs, camera's etc. The technology is promising in its capabilities. Making it all work depends not only on technology but also on standards, interoperability, and service providers.

RFID middleware

Enhancing technologies not only apply to the RFID tag and/or reader themselves, but also to the information systems which process the RFID events. Using RFID events within existing applications, such as Enterprise Resource Planning (ERP) or Customer Relationship Management (CRM), poses the need of some form of adaptation. This functionality is performed by the so called RFID middleware. This middleware has four major tasks:

1. Be able to connect RFID readers from different manufacturers. Unfortunately there is still not a single standard to connect a RFID reader. So adapters for each manufacturer are still necessary.

2. Filter the RFID event stream. When holding a RFID tag within the field of a RFID reader produces a flow of events telling that the tag is still in the field. In most cases only the entrance of the tag is important. Therefore all the "double reads" of the RFID tag must be filtered out.

3. The RFID tag contains in most cases only a (U)ID, an unique number. The existing applications do know nothing about these numbers, so they must first be converted into known references of the object the tag is attached to. For instance in the case of a chair, the serial number.

4. At this stage the object is identified in a know manner and the event is ready to be send to the existing application. Unfortunately each application had its own interface demands. So again an adaptation layer is necessary to be able to interface with the application and deliver the RFID event.

In single application domains it is relatively simple to discover object information based on the UID. However, in more distributed application domains a central operating registry is responsible for the search and discovery of object information. In the EPCglobal architecture the ONS (Object Name Server) is responsible for this functionality.

RFID middleware is a complex subject which is in full development at this moment. This is outside the scope of the deliverable.

4.2.4. Concurrent technologies

The concurrent technology class is about network technologies which offer (part of) the same functionality as RFID does, they are *concurrent* towards RFID. As introduced in section 4.1.3 , we have described RFID based on three aspects:

- Identification
- Location
- State

The following three paragraphs describe today's most important technologies which can also be used to implement that specific aspect. This tends not to be a complete list.

Identification

For identification purposes the most obvious alternative of RFID is the *barcode*. A barcode is a visual image containing black and white bars in a certain pattern. Using an optic device like a camera or laser reader, the barcode can be read and the code deciphered. The advantage of barcode is that it is extremely cheap. The disadvantages are its vulnerability to physical damage, the need for a line of sight between the barcode and the reader and the lack of dynamic content (memory, sensor, etc) (See also section 1.2.4).

Another possibility for identification of an object is the use of an existing wireless communication infrastructure, for instance *WiFi*. Each WiFi enabled device has a wireless interface with its own identification within the WiFi network, its MAC (medium access layer) address. Each base station within the WiFi network knows which MAC addresses are available within its field, and therefore which WiFi devices are present. By linking a WiFi device one-to-one to an object, identification of that object becomes possible.

Especially in situations which already have a WiFi network this can be a useful and cheaper solution than installing RFID readers and tagging all the objects. Note that when operability is needed between different sites, technically meaning different WiFi networks, things get complicated because all the WiFi devices must be known on all locations, without necessarily giving them access to the entire (company) network.

UWB can be used in a similar manner for identification and location. Special UWB tags which continually transmit a unique ID are detected by location detectors. Time, place and optionally direction are being measured, resulting in an absolute location within the UWB network area.

A new emerging technology which has promising aspects to be used for identification and location is *Zigbee*. For more information and applications of Zigbee see section 4.2.2.

A special note on identification: there is a risk in using technology related identification, e.g. the factory UID in a RFID tag, to identify an object. In case of loss of a tag or unrepairable damage, it is problematic to acquire a new tag with the same UID. So although the object is still the same, it gets a new identification. Using an identification scheme which is separated from the technology avoids this problem. For instance using tags with memory to store their own ID.

Location

Passive RFID does only offer a discrete solution to determine the location of objects. Only when the tag is within the field of the RFID reader it can be located, in fact it can be related to the location of the reader itself. In the same manner barcodes could be used for location purposes too.

With *active RFID* the location of a tag can be determined in a much larger area with respect to passive RFID and for some types of active tags distances up to 100m are possible. When using triangulation methods between the measurements of several active RFID readers, a more precise accuracy is possible. Using such methods can bring location accuracy close to the 0.5m, thus similar to passive RFID.

In a similar manner WiFi can be used for location purposes. Existing equipment, such as PDA's or laptop, can be pinpointed to a certain WiFi-base station. This provides a rough but very cheap location mechanism. It just uses the existing WiFi network which is already in use. A small software extension can provide the location information.

As explained in the previous section on location, UWB can also be used for location purposes.

When even the range of active RFID becomes too small, other options remain: using networks with a global coverage (GPRS) or GPS. GPS uses satellites to determine the location of the GPS device. On other cases computer vision can be used to identify and locate. Perhaps even ultrasound or infrared sensors can be used, although the range is not necessarily larger then active RFID.

RFID can be used for *location based services*. Using passive RFID objects or people can be located on a specific location at a certain point of time. These locations can be anywhere in the world, but are only snapshots in time. Using active RFID provides a lot more real time location capabilities, but only in a local area. For advanced location based service several technologies, among which RFID, can be combined generating a more accurate view of the location of the object / person.

State

Adding state information is no different to RFID than to any other technology discussed in this deliverable, in both cases sensors are an addition. Sensor technology is a special field which is outside the scope of this deliverable.

Relation with RFID

In Table 4-1 a comparison is made between the different RFID tags available on the market today and the three aspects discussed in this paragraph: identification, location and state.

Table 4-1: RFID tag types versus identification, location and state

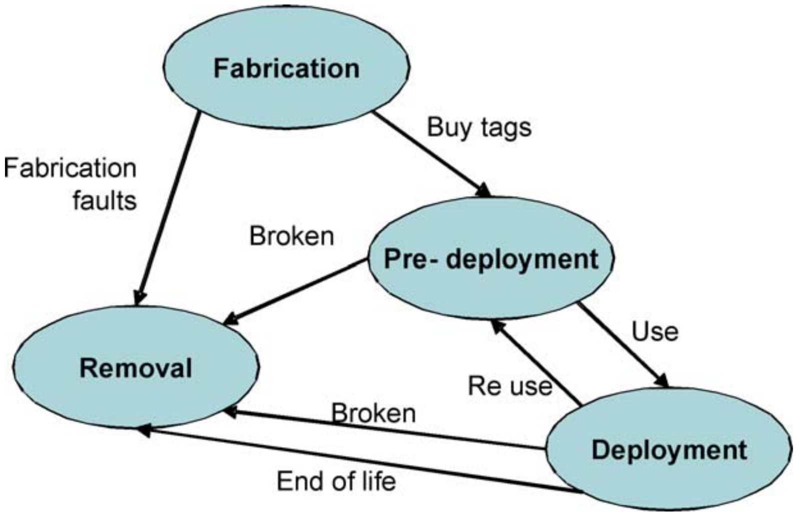
	Identification	Location	State
LF	++	+	n/a [37]
HF	++	+	+
HF active	++	++	++
UHF	++	+	n/a

From this table it can be concluded that all RFID tags are useful for identification purposes. Location is mostly dependent on the range, therefore active RFID is best, then UHF and with LF and HF it is still possible but only for local positioning. State information together with RFID is at this moment only possible in the HF range. There is no technical reason for this, but they are the only ones on the market today. Most of them need additional power, therefore HF active has a '++' indication.

4.3. RFID lifecycle description

In this section the different states in the lifecycle of a RFID tag are described. There are four major states: fabrication, pre-deployment, deployment and removal. Each of these states is described in more detail in the next subsections. *Figure 4-4* presents the four major states in the lifecycle of a tag and their relations.

Figure 4-4: RFID lifecycle



4.3.1. Fabrication

The first step in the life of a RFID tag is its fabrication. Depending on the market growth RFID will be produced in massive entities, lowering the price per tag. At this moment the price of passive RFID tags is about $0.25, and is still being reduced. One expects the price to decrease to a few cents per tag within the next ten years. During fabrication each tag gets its own unique identification, the factory UID. If the customer wants its own ID in the tag, it must be programmed during the pre-deployment phase.

4.3.2. Pre-deployment

After the tag has been fabricated it must be made ready to be deployed in an operational environment, it must be pre-deployed. In this phase the tag must be physically and functionally connected to the object.

Physically connecting the object can be done by simply gluing it onto the object, but also more reliable and durable solutions are available. A lot of development is going on into smart packaging. Plastic containers are developed with an RFID tag

[37] The authors do not know of any LF or UHF tags with state capabilities at this moment

encapsulated within the walls of the container. This poses high demands on the heat endurance of the tags.

RFID tags can not be read by a human without special equipment. Often it is desirable that the object is still human identifiable. This makes it not only necessary to attach the RFID tag to the object, but also a human readable label sometimes combined with a barcode for backwards compatibility has to be attached to the object.

Making the link between the physical object and the internal ID of the RFID tag requires an accurate and computerized mapping process. Often after a (random) RFID tag is put onto the object, the object is scanned by a reader and the link between the specific object and the ID of the tag is made. Registering the object – tag relation is a very costly process which must not be underestimated.

If one does not use the internal ID of the tag but a specific ID such as the EPC code, the tag must also be programmed. After attaching the tag to the object, the correct unique code can then be programmed into the tag identifying the object in a universal manner. Note that this step can be performed by the manufacturer of the tag, pre-deploying the tags for its customers. In most cases this is only possible when ordering very large quantities at once.

After these steps the tag is ready to be deployed.

4.3.3. Deployment

Now the object has an RFID tag onto it. An information system registers which object has which ID. The object is ready for operational usage. This is still far from a plug&play scenario. It is still very difficult to set up a RFID environment with a read rate of more then 99%. In most cases it starts with read rates not higher than 80% which should increase by fine tuning the system. At all times it is wise to be prepared for these uncertainties and be able to deal with them in the RFID middleware and applications. Also the deployment of the readers is not always easy; placing antennas, connecting them to the readers. Connecting the readers to the middleware via the local IP network, serial interfaces, or other means takes a lot of effort. In case of large deployments also the traffic on the backbone generated by the readers can become an issue.

In some usage scenario's tags are being reused and attached to other objects. This requires that tags be physically and functionally removed from the object and moved back to the pre-deployment state. Especially when the internal ID of the tag was used, removing the functional relation can be difficult because the same ID must now be related to another object; requiring that all references in all information systems must be removed. This is not an easy task because there is no track record of all the places (RFID readers) the object has visited during its life time. Therefore re-using RFID tags is only practical when the internal ID is not used but instead a tag independent ID.

Another issue when re-using tags can occur when the use of the object changes, but still the same RFID tag must be used. Thus the same object is used in two different value networks, both using the same RFID tag. A good example is a bottle of medicine with an RFID tag. In the first value network the bottle is tracked from the factory to the pharmacist. The second value network starts when the bottle is sold to a patient, based upon the prescription of a general practitioner. The RFID tag can then be used to hold the prescription of how the patient should use the medicine.

In most cases the RFID tag will be physically and/or logically removed from the object when there is no longer a purpose of tracking the object. For example once it is sold to the customer, there is no need for the tag anymore. In these cases the tag moves to the removal state of its life cycle.

4.3.4. Removal of tags

The final stage of the life-cycle of each tag is its removal. Removal of tags can be induced by different reasons:

- During manufacturing faults can be made rendering the tag useless.
- During pre-deployment and deployment the tag can be physically broken. Some physical problems can occur which make the tag useless.
  EPC Class 1 tags have the capability to destroy themselves, so as to enhance privacy protection.

- After deployment the tag can be no longer needed, it has reached the end of its life.

In all these cases the tag has ended its functional life time. This does not necessarily mean that it has reached also its physical lifetime. Probably in most cases the tag will not be removed from the object itself. In order to meet the customer's requirements that a tag – having ended its functional life-time – can no longer be used to monitor or track a customer, tags are being developed in such a way that they can be "shutdown". This results in a broken tag which physically is still present but will never react to a reader again. EPC Class 1 tags already have this capability.

4.4. Typology of RFID usages

Within this section we will present an application usage domain model which can be used to characterize RFID based application in terms of configuration types and business usage domains

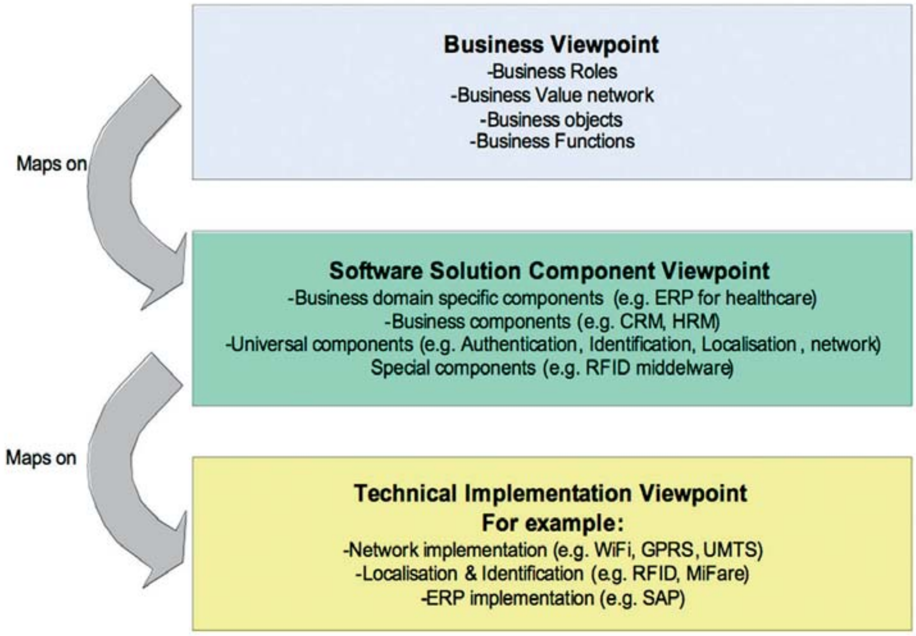
We will first position business aspects and technology to each other. Then, we will formalise the usage typology on the basis of information- or privacy sensitivity and their business usage domains. Specific RFID based applications as well as more abstract application domain groups can be positioned to demonstrate their demands on particular technology.

At the end of the section we will illustrate the usage typology in three use cases selected from different business domains. The three use cases describe possible scenarios in healthcare, personal identification and food control.

4.4.1. Realization framework

Figure 4-5 below presents a 3-tier reference model which positions the business viewpoint aspects and the technical implementation aspects in one model.

Figure 4-5: 3-tier reference model


Business Viewpoint
-Business Roles
-Business Value network
-Business objects
-Business Functions
Maps on
Software Solution Component Viewpoint
-Business domain specific components (e.g. ERP for healthcare)
-Business components (e.g. CRM, HRM)
-Universal components (e.g. Authentication, Identification, Localisation, network)
Special components (e.g. RFID middelware)
Maps on
Technical Implementation Viewpoint
For example:
-Network implementation (e.g. WiFi, GPRS, UMTS)
-Localisation & Identification (e.g. RFID, MiFare)
-ERP implementation (e.g. SAP)

Within this framework the business viewpoint aspects identify business roles, business objects and business functions. The specification of these items and their mutual relationship forms the base of a business system that needs to be implemented with technology.

In the technology viewpoint we identify communication, information and processing technology like e.g. WiFi, Bluetooth, Mifare and database systems like SQL server. Also ERP implementations like SAP are part of this viewpoint.

The layer in between forms the functional solution component viewpoint, and can be considered as a more abstract, implementation independent layer which transforms the business specification onto the specification of (generic) functional components with preferable standardized functionality and interfaces. The primary objective for this layer is to create a solution independent specification which enables an architecture where business adaptation and solution technology changes are invisible for each other.

Let us illustrate the model with a medical logistic value network example. A value network includes three business roles responsible for the supply, distribution and reception of medicines. The supplier role is played by the manufacturer of the medicine; the distribution role is performed by a logistic partner while the hospital is the receiver of the medicines. These roles together form the medicine logistic value network. The logistic partner in this network is special, because their business services are unique and based on organization specific logistic functions.

From the software solution component viewpoint the implementation of this business function is realized with the help of a tracking and trace component and real time tracing information. A unique combination of different solution components and interfacing concepts makes this system work more efficiently than the competitors' solution.

The technical realization viewpoint focuses on the technology, necessary to implement the component view. Software applications like e.g. SAP ERP in combination with RFID based localization technologies can be used to realize the logistic business function for the logistic partner. From the business point of view, the technical solution should provide two types of flexibility: the logistic partner should be enabled to adapt current implementations of a logistic business function without changing the technical solutions. On the other hand, new technologies have to be introduced without disturbing current business functions. These two aspects are important for up to date and reliable business system.

4.4.2. Usage typology model

In the model below (*Figure 4-6*) we use the vertical scale for information protection from less focus on privacy/security up to a high demand for the protection of information. We have identified here two main groups: "physical object" and "persons and animals". In fact everything can be considered as a physical object; however, from the privacy perspective it is useful to make a difference between these groups. Within the "physical object" group we distinguish between objects with no information storage, with temporal and with permanent information storage or reference.

In the first category we identify objects and primarily focus on the tracking and monitoring of any object. No information related to object is stored.

In the second category, objects are identified for which during a particular period of time information is stored or referenced. For example tracking and tracing applications in the logistic domain, where information about packages is stored only until delivery of the package. The removal of information is based on the event that a package leaves a certain application domain while the object itself is not necessarily removed.

In this second category, the information about an object is stored during the (relevant) lifecycle of the object. In this category information about an object is stored for a longer period of time and there will be a higher demand for information security than in the first category.

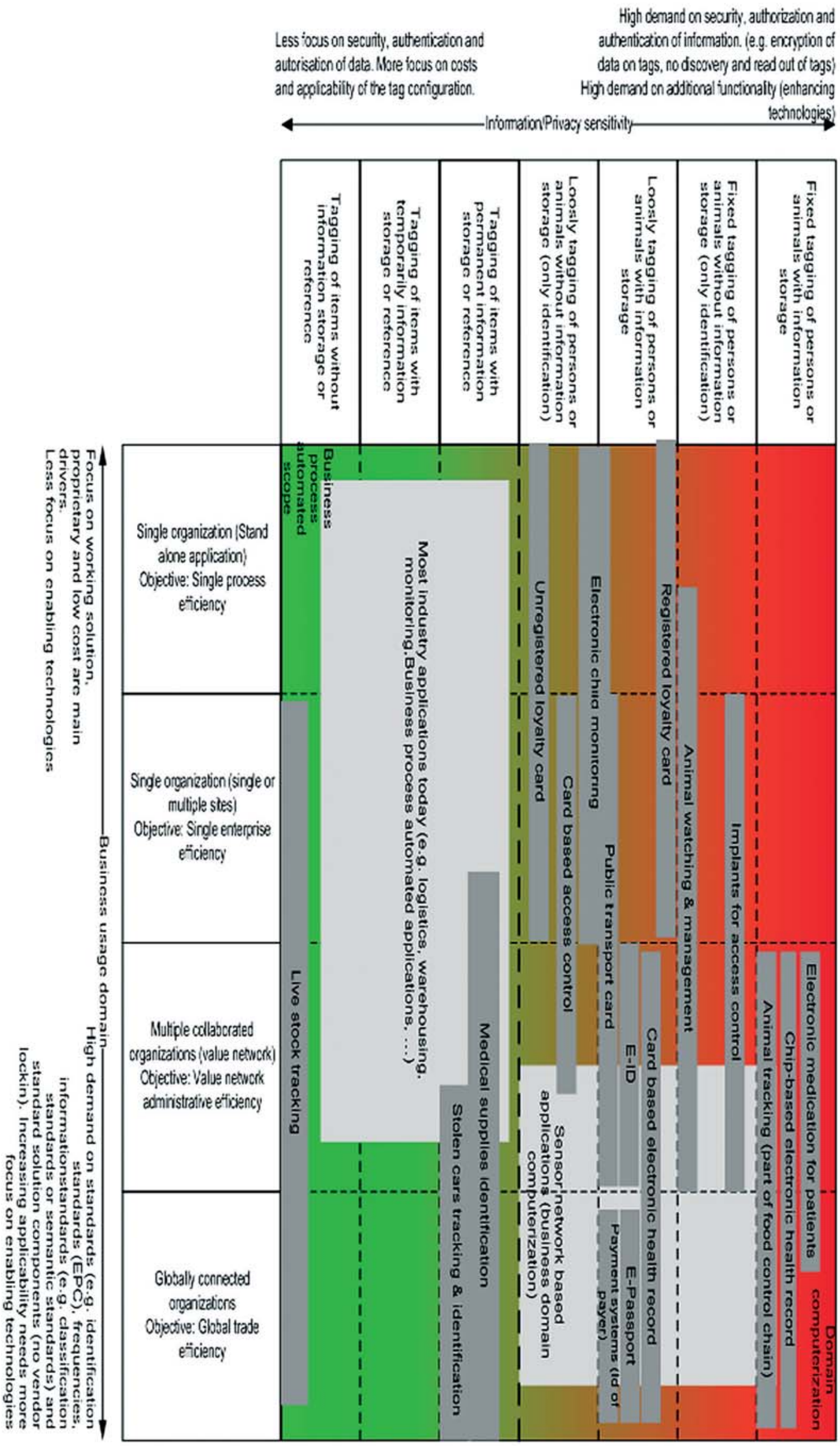
In the "persons and animal" group we distinguishes between fixed and "loosely coupled" identification, optionally with or without information storage. Loosely coupled identification means that there is no physical fixation between the person or animal and their identification. For example, card based identification methods are considered as loosely coupled while ID cards are not always linked with the person or animal. In case where persons or animals have implants or physically coupled ID mechanism we consider them as "fixed tagging" systems.

The horizontal axis plots the business usage domain. The business usage domain identifies four categories of business environments where applications are used. The most left category identifies a single organization located on one site. The main drive of using an automated application is the efficiency of a current business process or process step. The second and third category focuses respectively on a single organization with multiple sites and multiple collaborative working organizations. Both categories have an increasing complexity in terms of dependencies with other applications and organizations. The last category identifies globally connected organizations which try to make the collaboration efficient and easy. An important characteristic for all these domains is standardization and the use of enabling technology.

In the first category the application is working in a more or less standalone setup. In general the main focus is on the optimization of the business process or process step while collaboration with other organizations is not a focus point. Low cost and proprietary solutions are populating this category. In the fourth category we have the globally connected organizations. Globally working solutions are in general based on standards; standards on technology, security, frequencies and information. Especially the information standards are important to guarantee the exchange of all type of information. Besides standards on information syntax we recognize semantic as well as classification standards.

Finally, we recognize in this partition a second important characteristic: the increasing demand for enabling technologies to build globally connected networks to support globally collaborated organizations. In paragraph 4.2.2 we have identified the enabling technologies which increase the applicability of RFID. It is clear that in a globally connected business usage domain there is a higher demand for this type of technologies.

Figure 4-6: Application usage model


High demand on security, authorization and authentication of information. (e.g. encryption of data on tags, no discovery and read out of tags) High demand on additional functionality (enhancing technologies)
Less focus on security, authentication and autorisation of data. More focus on costs and applicability of the tag configuration.
Information/Privacy sensitivity
Fixed tagging of persons or animals with information storage
Fixed tagging of persons or animals without information storage (only identification)
Loosly tagging of persons or animals with information storage
Loosly tagging of persons or animals without information storage (only identification)
Tagging of items with permanent information storage or reference
Tagging of items with temporarily information storage or reference
Tagging of items without information storage or reference
Single organization (Stand alone application) Objective: Single process efficiency
Single organization (single or multiple sites) Objective: Single enterprise efficiency
Multiple collaborated organizations (value network) Objective: Value network administrative efficiency
Globally connected organizations Objective: Global trade efficiency
Business usage domain
Focus on working solution, proprietary and low cost are main drivers. Less focus on enabling technologies
High demand on standards (e.g. identification standards (EPC), frequencies, informationstandards (e.g. classification standards or semantic standards) and standard solution components (no vendor lockin). Increasing applicability needs more focus on enabling technologies
Business process automated scope
Domain computerization
Electronic medication for patients
Chip-based electronic health record
Animal tracking (part of food control chain)
Implants for access control
Animal watching & management
Registered loyalty card
Card based electronic health record
E-Passport
E-ID
Payment systems (id of payer)
Public transport card
Electronic child monitoring
Card based access control
Unregistered loyalty card
Sensor network based applications (business domain computerization)
Most industry applications today (e.g. logistics, warehousing, monitoring,Business process automated applications, ...)
Medical supplies identification
Stolen cars tracking & identification
Live stock tracking

In the following section 4.5, appropriate examples of business scenarios making use of the usage model presented above, will be elaborated. Based on (IDTechEx, 2005b) we have identified main usage application domains based on forecast for volume and/or society impact. The model shows that current RFID based applications are mostly positioned in the lower part of the model; applications handling physical objects within a single- and multi-organization business environment. In the introduction of this document we have identified these applications as business process automated applications. Generally, these applications are using low cost tags and focus on improving efficiency in an organization or an existing value network.

Future applications are foreseen to be positioned in the upper part of the model. This means, applications making use of increasing and more sensitive information about persons and animals which require increased security and safety functionality. At the same time the business usage domain shifts more and more to organizations in value networks and globally connected organizations. A special category of application domains are the sensor network based applications. This type of application is based on the existence of a generally useable sensor network. This network is principally not biased to a particular application domain, and will serve different type of domains.

4.4.3. Business scope

RFID in the context of business process automation is particularly used to achieve specific (primarily role- or organization specific) optimization and efficiency without changing current service provisioning to an existing value chain. The drive for many of the use cases is to diminish the costs while improving the quality of the process. In this usage scenario human performed business processes are replaced by automated RFID based functions. For example, an application supporting a storehouse needs information about the objects in the store and the activities around storage and retrieval of goods. In pre-RFID times humans supply these applications with appropriate information about the incoming and outgoing goods. RFID adds automatic identification and location functions to this process, and based on these information elements the appropriate event type is generated (e.g. "register incoming good" or "register outgoing good"). In these setup organizations start building experiences with RFID usage and the integration with internal business applications.

In terms of the 3-tier reference model we can identify an existing value network by their business objects, business functions necessary to produce their service or product. RFID is used in this constellation to optimize one or more processes by enabling particular functionality in the solution component layer. The initially functional costs and the benefits aimed at have to justify the investment in RFID technology. Basically, this RFID typology is driven from current businesses and the need to improve the efficiency or the quality of the process or supply chain.

In case of RFID for business domain computerization usage the main driver is to provision a large group of business roles with generic event information. Information systems from different business roles are interested to receive event information. With the help of a generic sensor network a wide variety of information can be supplied to different roles. Efficiency and quality improvements are the main drivers here to start this usage scenario.

4.4.4. Proprietary versus standardized RFID solutions

In the application domain usage model the business domain aspects refer to the demand for a proprietary or standardized RFID solution. As mentioned before, current RFID based application domains are generally developed to diminish costs of current business processes. In these types of applications there is generally no need for sophisticated functionality and there is no vision on future collaboration with other organizations. This leads to relatively simple and proprietary solutions.

However in business domain computerization the lack of an existing value network and of the support for a variety of potential business roles, a standardized and open RFID based solution is preferred. Within such an environment it will be easier to integrate with future (customer) roles and to fulfil their requirements. The lack of support for (open) standards may restrict the potential business opportunities. For example, when a sensor network provider is not able to share a common installed infrastructure and support open access standards, additional costs have to be made to connect new business partners. This will result in higher operational costs for their sensor network. Also, if proprietary identification mechanisms are used for objects and/or locations, it will be hard to guarantee object identification to all objects without making extra workarounds.

In RFID supported cases we see a variety of tag types, frequencies, used identification code types and information standards. The type of frequency used is determined by the required reliability with respect to the environment and material of the tags' object. Low- (LF) and high frequency (HF) passive tags are mostly used in today's application domains and in supply chain. Because of the tendency to enhance process integration between different organizations, there is an increasing demand for (open) standards. The RFID air protocol (ISO/IEC14443) and object identification (EPC) standards are examples of standardization to increase the extensibility and compatibility of RFID technology.

4.4.5. Information sensitivity and RFID tag types

Information- or privacy sensitivity is essential to the future of RFID technology. Because of the ability to link physical objects and persons in the real world with information, RFID becomes a potential threat for misuse of sensitive information. As we have seen, the model distinguishes between physical objects and person and animals.

In general we distinguish four potential tag related information threats:

- Ability to access the information
- Ability to read information
- Ability to change information
- Ability to delete information

The first threat is based on the simple communication method between tag and reader. It is especially easy to access the information on the tag in this case. In more complex systems information can be protected against reading, changing and deleting through encryption, authorization and authentication (see Chapter 9). Although, there are enhancing technologies today to implement these protection mechanisms, this problem needs to be addressed also at the level of the information system.

In the case of business process automation the focus for useable tags is especially on identification of objects and location. For example, the business process of registration of incoming and outgoing goods identifies the goods and the location where the goods are read to generate the appropriate event. Objects in this business scenario type generally associate information with sometimes location and identification information only and other times with temporary information. The way RFID is enabling this functionality differs from the stored reference information (an address where the object related information can be found) or the storage of information itself. In the first type the RFID stored data is only address information. In this configuration there is generally less pressure on security of information stored in RFID tags. The security and safety functionality is part of the accompanying information system.

In case information is physically stored on the tag there is a higher risk for information misuse. Because security and storage functionality makes the tag more expensive, most applications will make use of reference information instead of distributed stored information.

Applications related to high value information and the requirement for offline information access will make use of this more expensive type of tags. In the upper right corner of the model in Figure 4-6 some application domains are identified which may justify these requirements. For example, the ability to access offline patient health record information may be critical in special occasions, while in other cases the information has to be protected against misuse. This type of value network may justify the high costs of these tags.

RFID suppliers are working hard on the development of new types of tags and reader functions. Active tags, microwave frequencies, smart active labelling (SAL) and ubiquitous sensor networking (USN) are interesting developments for the development of the internet of things and global connected organizations. Based on these developments new universal functionality accelerates the support of new business opportunities (e.g. electronic health record and food tracking and tracing applications).

4.5. RFID usage in business domains

To illustrate the RFID usage typology scenarios we will present some example of business scenarios. These examples illustrate RFID technology in a variety of business domains, where the initial approach is to improve a current business processes. In a second step an example is given of the migration to a business domain computerized environment and the potential role of RFID in such a system.

4.5.1. Example business scenario healthcare

Today, several pharmacy producers, suppliers, distributors and pharmacists are using RFID tags on medical packaging to automate their collaborative production and delivery process. RFID technology is used to control the different steps in the value network and to share this information with other stakeholders in the value network. In today's use cases the passive tag variant is mostly used while the primary function is the identification and localization of medicines. To support this value network a simple passive read only tag is sufficient, while information is shared via an accessible information system. When the proper drug is delivered at the pharmacist the resulting service of this value network is completed. However, besides this logistic value network the pharmacist is part of another value network with the general practitioner and the patient. The pharmacist provides in this network the delivery of the prescribed medication to the patient. The general practitioner is responsible for the prescription of the drug and the operational instructions. The problem in this network is how the instructions are joined to the delivered medication. Experience shows that groups of patients are not always able to understand and follow the instructions with sometimes serious consequences. To solve this problem a spoken drug instruction could help this group of patients. Based on an existing device which translates text into spoken words, the operational instructions can be stored on the medicine and provide the patient with personalized instructions. The pharmacist receives from the general practitioner the medical operational instructions and digitally writes the instructions on a writeable tag. An RFID based speech device reads these instructions and tells them to the patient. Because of the storage capabilities of information on a tag, there is no need for the patient to have an online connection.

In relation to the layered reference model we see that the box of drugs participates in two different value networks. In both cases RFID tags are used to store information, in the logistic value network the object identification information is stored while in the second value network medical instruction information is stored as well. To avoid double tagging, measures have to be taken to assure that one and the same tag can be used in both cases. Replacing the old tag with a new one will result in definitive removal of the object from the logistic value network. Information about the logistic information in the first value network can no longer be accessed via the original tag.

Another option is the reuse of the original tag and identification, but how do we guarantee that the pharmacy producer adds a more expensive tag to the medicine with the writable functionality?

Tag- and information standardization solve this problem partly. A standardized identification mechanism could identify the medicine uniquely in both networks. However, the main challenge is the division between business opportunities and corresponding costs.

4.5.2. Example business scenario electronic identity cards

Identity cards and passports are excellent examples of a paper based identification technology for persons. The ID-card and passport prove that a person is who he said he is, primarily based on a photo and the authenticity of the card or passport. Because of the limited functionality and capability of these paper based identification mechanisms, there is a need for another and safer mechanism.

Based on latest technology developments RFID is used in combination with paper based identification mechanism. In addition to the readable information in the card or passport, RFID adds the possibility to store electronically person specific biometric information. The main objective here is the higher level of protection of the stored information; however, RFID enables also automation of particular authentication functions like e.g. iris scan or finger print checking. Experience shows that all traditionally written information can be changed or manipulated. With the help of RFID an extra technical obstacle is created to prevent corruption of the electronically stored information. Besides this, it opens the possibility to automate parts of the identification functionality. After all, person specific information is electronically stored on a device which can be read out wirelessly, while these characteristics can be checked with e.g. an eye-scan or a finger print verification. Even a real time DNA scan might be possible in the future.

Today there are lots of entrance systems which work on a traditional LF or HF RFID tag. In combination with a passive RFID tag with extended memory capabilities, person specific information can be stored on the tag. Because of the sensitivity of the stored information, extra attention should be given to the protection of the information by unauthorized persons. People wearing these types of identification tags are not aware when information is read or not. Also the protection of re-writing of information is an issue to address. In the future tags will be created where people are able to interfere in the exchange of information between tag and reader, e.g. based on pressing a simple button through fingerprint recognition. With the help of this type of tags a higher level of protection can be achieved.

4.5.3. Example business scenario food quality

Today there is a high demand from society to food producers in the food chain to guarantee the quality of meat that consumers buy. Consumers want suppliers to show them the origins of the beef or the type of food the pigs have had. Since many years cows and other animals are identified with help of RFID technology while information about these animals is already stored. In particular high tech farmers use these tags to track and trace animals and store information about food quality, disease and medication. Traceability of the animal however stops at the time of its death. The meat products are then provided with printed information about the type of meat and the process followed, while detailed information about the particular animal is omitted. An interesting aspect in this scenario is the fact that an object disappears from the real world while offspring objects require an association with the disappeared animal-object. From a RFID perspective the associated information of the slaughtered cow disappears and new object-tags will be created and attached to the associated beef products.

By identifying meat products with read-write tag types, more detailed information could be provided to consumers. However, this case shows that consumers will need a universal reader to interrogate this type of information. Also information on the tag should be stored according to common information standards.

Based on current meat-sensor research, this opens up the possibility for active tags reporting if the beef is proper for consumption. Although this seems an expensive mechanism, it could prevent food poisoning and related medical and litigation costs. Based on this example, we may conclude that systems like this can only be elaborated on standardized technical solutions to assure the interoperability between the associated value networks.

4.6. Summary and conclusions

We have described RFID technology from different, technically oriented, viewpoints. Today's usage analysis shows two abstract fields of usage application; business process support and business domain computerization and the respective application usage domain for sensor networks. In this chapter we have described RFID from a technology, usage, standards and frequency point of view. Based on these viewpoints we draw the following conclusions:

- RFID is an important technology to use in the implementation of a universal sensor network; RFID is an appropriate technology to transfer real-world objects and corresponding events to feed information systems with real time information. Furthermore, RFID is well equipped to provide sufficient context information with the generated events.
- The drive for universally usable, sensor network based applications will create a demand for more standardization to increase the compatibility and the usability of RFID based information systems. Besides standardization on RFID technology (tags and reader functionality) more standards on the

information semantic level of RFID tag stored information is needed. This type of standards will increase the usability of tags and (sensor) information for different purposes. Also the interaction between companies will be easier if both parties use the standardized information.

- An important point of interest is how to attach the appropriate tag to an object. To enable the exchange of the same tag between different value networks, criteria or rules have to be defined to determine which type of tag has to be attached to which type of product. Especially when there is a public interest the government or European Commission may setup rules for special product categories to determine the tag type.
- There is a variety of technologies which can enable and/or enhance RFID. These combinations make the use of RFID in a variety of application domains possible. Readers can become mobile and or distributed tags can be enhanced with sensors and other functionality. At this moment there is not an obvious killer combination, the market will have to determine which combinations become standard. In the usage application domain model the tendency seems to be that the development from RFID based application goes from business process automation scope up to domain computerization. For the last type of usage application more enhanced and sophisticated tags are necessary.

Part two

Market perspectives and socio-economic issues

Institute for
Prospective
Technological Studies

■ 5. RFID market perspectives

Several technologies are included under the RFID umbrella and each one has its own market implications. The major role no doubt will be played by applications for the retail supply chain, where a massive deployment of RFID hardware and software is expected. This is however, still not happening except where forced by retail giants Wal*mart in USA, METRO and Marks & Spencer in the EU. Nevertheless it should not be neglected that there are a number of minor and niche applications where RFID technology is successfully and widely exploited including, but not limited to, logistics, personal identification, ePayment, and ticketing.

This chapter attempts an analysis of the main forces driving the RFID market evolution, what actors are involved and what is the role they play. Although some market figures will be provided, the focus is rather on the dynamics of the market trying to figure out what could be the evolution path. The discussion will start with the description of the market actors, then what are felt to be the key drivers and finally the market figures.

5.1. Actors and stakeholders

5.1.1. The RFID value chain

The RFID applications value chain is quite complex. IDTechEx proposes a scheme (Figure 5-1) aiming at encompassing in a few blocks the main industrial activities involved. It has to be noted that the proposed structure does not mean that any real company should exactly fit into one box: some might span over more boxes or just cover a part of a single one. Moreover the boxes are ordered from left to right with growing value: each one uses as source the output of the boxes on the left, adds its own value and feeds into the boxes on its right.

Two main flows (from left to right) are represented. The first refers to the “Chip Tags”, the ones that are built around a silicon[38] core. There are silicon foundries building the chips and others putting the chips together with the antennas. The third box refers to companies that produce the product to be consumed (e.g. rolls of sticking labels or hard packages for reusable tags) having the RFID enclosed. These first three boxes are fed by a “licensors of inventions” box referring to the RFID patent holders, for example Intermec holds a relevant number of these.

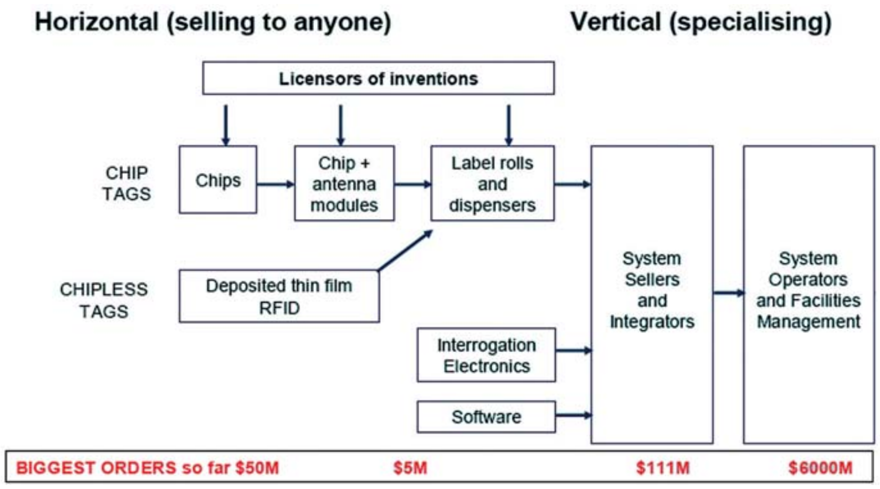
On the second row a single box represents the manufacturing of the chipless tags: no chip implies that no integration with the antenna is needed; packaging of the tags in consumables is however still needed.

On the bottom rows we see the manufacturers of hardware, namely readers and reader antennas and printers etc., and software providers for middleware and applications.

At the end of the chain the companies that make things work in broad terms are identified. These span from business process consultants that focus on “why” and “where” the RFID technology deserves to be applied, down to system integrators, knowing “how” to make the hardware and the software work together.

[38] Polymer chips might be considered as well in this box although nowadays they are mainly in R&D phase.

Figure 5-1: RFID value chain[39]


Horizontal (selling to anyone)
Vertical (specialising)
Licensors of inventions
CHIP TAGS
Chips
Chip + antenna modules
Label rolls and dispensers
CHIPLESS TAGS
Deposited thin film RFID
Interrogation Electronics
Software
System Sellers and Integrators
System Operators and Facilities Management
BIGGEST ORDERS so far $50M
$5M
$111M
$6000M

Finally, companies providing for system operations and management services, outsourcers, and service providers are rated at the top of the value chain.

5.1.2. Market actors

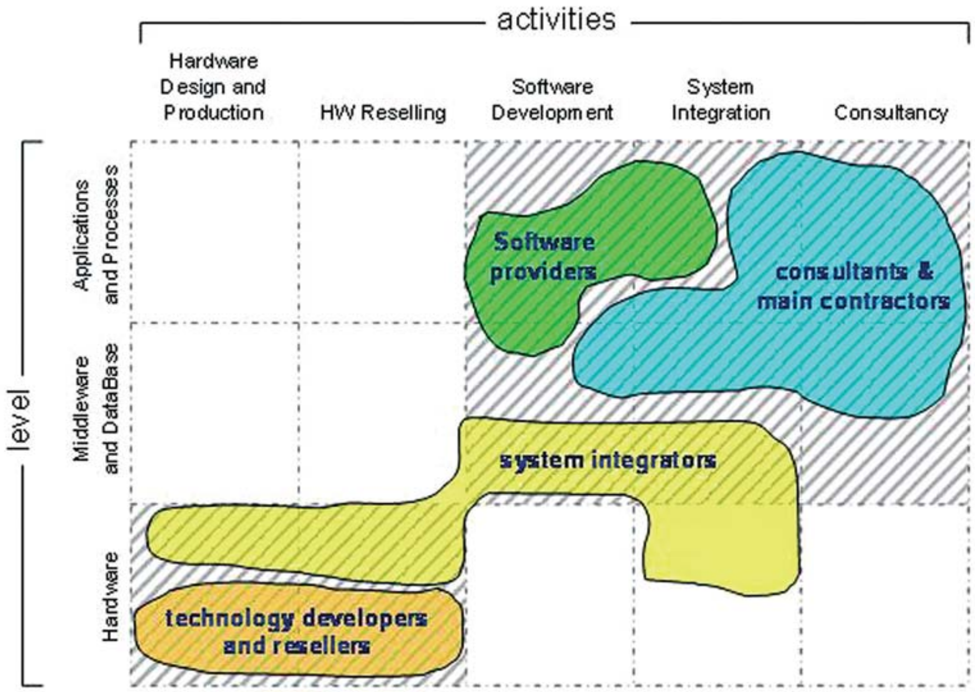
In a study published by Milan Polytechnic in 2005 a scheme has been proposed for the clustering of the companies operating in the RFID market. One axis presents the activities that compose the already described value chain,[40] while the other axis proposes three component levels. The Hardware level encompasses all the physical elements: tags, readers, antennas, etc. The "Middleware and DataBase" level owns the software infrastructure components that are common to most applications (thus named "application independent"). The third level is named Application and Processes and refers to the components that are developed for a specific application and/or tuned to meet the requirements of a specific customer.

On the basis of these criteria/axes, a number of companies has been mapped on a chart with respect to their products and services. Four main "clusters" of companies have been identified (See Figure 5-2). A list of the technology players in each cluster is also provided. Please note that, as there is not a deterministic way to assign a company to a specific cluster, the company names hereafter reported might be somehow arbitrary. Nevertheless the list is deemed useful in order to allow the reader to associate some real world names with the clusters. The names are to be considered as examples and the proposed lists are thus not exhaustive; their cardinality does not represent the real number of companies in the cluster.

[39] Source IDTechEx, 2005a. Note that "Deposited thin film RFID" and later on "Laminar transistor circuits" refer to technologies, currently under research, making use of polymers instead of silicon.

[40] Though the value chain proposed in the cited study does not exactly match the one by IDTechEx, nevertheless the activities can be quite easily mapped one to the other.

Figure 5-2: Map of RFID offering actors



Technology developers and resellers

This cluster includes those actors that provide RFID specific hardware components (tags, readers, antennas, printers, …) independently of whether they are developers or resellers. In this cluster companies that carry out hardware design and engineering activities (e.g. the ones that develop on demand customized packaged tags) are also included.

5.1.3. RFID tag manufacturers

- HITACHI, *http://www.hitachi.co.jp/Prod/mu-chip/index.html* (JP)

  Headquartered in Tokyo, Japan, is a leading global electronics company, with approximately 340,000 employees worldwide. Fiscal 2002 (ended March 31, 2003) consolidated sales totaled 8,191.7 billion yen ($68.3 billion). The company offers a wide range of systems, products and services in market sectors, including information systems, electronic devices, power and industrial systems, consumer products, materials and financial services. Mu-solutions is a Hitachi RFID division under Information & Telecommunication Systems. Mu-solutions builds and manages a complete platform for μ-chip solutions.

- Motorola, *http://www.motorola.com/mot/doc/0/202_MotDoc.pdf* (US)

  Motorola, with 150000 employees, headquartered in Illinois, USA, is a leader in wireless and broadband communications systems. Their "Seamless Mobility" vision aims at technology to get and stay connected simply and seamlessly to the people, information, and entertainment. Motorola had sales of US $36.8 billion in 2005. Motorola BiStatix™ is a new solution that allows the creation of cost-effective "smart labels." Radio frequency identification (RFID) antennas are printed on materials using conductive non-metallic ink.

- Philips, *http://www.semiconductors.philips.com/products/identification/index.html* (EU)

  Royal Philips Electronics of the Netherlands is one of the world's biggest electronics companies and Europe's largest, with sales of EUR 30.4 billion in 2005. With activities in the three interlocking domains of healthcare, lifestyle and technology and 158,000 employees in more than 60 countries, it has market leadership positions in medical diagnostic imaging and patient monitoring, colour television sets, electric shavers, lighting and silicon system solutions. Philips provides a complete range of RFID ICs including smart cards, tags, labels and readers. They address a number of applications, from low-cost smart label ICs for high-volume supply chain management applications through next generation 32-bit smart-computing platform for powerful multi-application smart cards.

- Siemens, *http://www.automation.siemens.com/rfid/index_76.htm* (EU)

  Siemens (Berlin and Munich) is a global leader in electrical engineering and electronics. The company has around 461,000 employees both for manufacturing products and developing customized solutions. The company focuses on the areas of Information and Communications, Automation and Control, Power, Transportation, Medical, and Lighting. In fiscal 2005 (ended September 30), Siemens had sales from continuing operations of EUR 75.4 billion and net income of EUR 3.058 billion. Siemens offers a complete RFID portfolio – from products and systems, technical and operational consulting as well as process design up to technology, process and IT integration.

- Texas Instruments, *http://www.ti.com/rfid/* (US)

  Texas Instruments (TI) is a global semiconductor company and one of the world's leading designers and suppliers of real-world signal processing solutions. The company's other businesses include Sensors and Controls, as well as Educational and Productivity Solutions. Headquartered in Dallas, Texas, TI has more than 34,000 employees worldwide with corporate, sales and manufacturing facilities in more than 30 locations across Asia, Europe and the Americas. TI is the world's largest integrated manufacturer of radio frequency identification (RFID) transponders and reader systems.

Components developers and resellers

- Alien Technology, *http://www.alientechnology.com/* (US)

  Alien Technology is a venture funded, privately held company. They provide UHF Radio Frequency Identification (RFID) products and services to customers in retail, consumer goods, manufacturing, defence, transportation and logistics, pharmaceuticals and other industries. Alien's products include RFID tags, RFID readers and related training and professional services. Alien employees about 235 people worldwide. The company's corporate headquarters is in Morgan Hill, CA and sales offices are in the US, Europe and Asia. Alien is a member of EPCglobal.

- AVID, *http://mail.avidid.com/web/index.htm* (US)

  AVID Identification Systems, a privately held company was founded by a veterinarian in 1985 and is a major supplier of microchips in the United States and around the world. AVID invented, designed, introduced and implemented the microchip based pet recovery system as it is globally known today (37 patents to date). Horses, cattle, dogs, cats, other companion animals and livestock, etc. are able to be permanently identified with a secure unique number. They provide syringe delivery systems, multi-mode reading systems, and pocket size readers are examples of standards set by AVID. AVID is headquartered in 3185 Hamner Ave, Norco, CA, USA.

- CAEN, *http://www.caen.it/rfid/index.php* (EU)

  CAEN is based in Viareggio, (150 employees) Italy and is specialized in manufacturing mission critical electronics systems:

  - design and manufacture electronic equipment for the Nuclear and Particle Physics such as Low Voltage & High Voltage Power Supply Systems, Front-End and Data Acquisition Electronics;
  - design and production of high reliability electronics for Space applications and collaborates with the main Space Agencies (NASA, ESA, ASI, CNES);

- complete microelectronics design service for digital, mixed/analog ASICs and complex FPGA designs, with a wide offering of HW and SW Intellectual Properties (IP) blocks;
- readers and tags for UHF Radio Frequency Identification technology.

• Intellident, *http://www.intellident.co.uk/* (EU)

Intellident, (part of the £1.2 billion LINPAC group), design, build and deliver advanced wireless tracking solutions, based on innovative RFID and bar code technologies. The company is based in Manchester, UK.

• Intermec, *http://www.intermec.com/eprise/main/Intermec/Content/Technology/RFID/RFID* (US)

Intermec Technologies Corp. is a leader in global supply-chain solutions and in the development, manufacture, and integration of wired and wireless automated data collection, RFID (radio frequency identification), mobile computing systems, bar code printers, and label media. Based in Everett, Washington, the company has 2,700 employees worldwide.

• PSC, *http://www.psc.com/* (US)

PSC Inc. is a global provider of data-capture solutions for retail supply chains. Its broad array of products and services include point-of-sale scanning, warehousing & distribution, and wireless networking. PSC is a privately held global company. Rival Datalogic acquired PSC from the private equity firm Littlejohn & Co. for around $195 million in 2005. With a presence of 750 plus employees in more than 100 countries, PSC's headquarters and major manufacturing facilities are located in Eugene, Oregon, while sales and service offices are located throughout the Americas, Europe, Asia and Australia.

• PSION, *http://www.psionteklogix.com* (US)

Psion Teklogix Inc. is a leading provider of rugged mobile computing solutions to a range of industries around the world. It was formed in September 2000 as a result of the merger between U.K.-based Psion Enterprise division of Psion PLC, and Canadian-based Teklogix Inc. Psion Teklogix is headquartered in Mississauga, Ontario, Canada with additional corporate offices located in Europe, the United States, Asia, Latin America and the Middle East with about 600 employees.

• Sirit, *http://www.sirit.com/* (CA)

Sirit Inc. has been providing Radio Frequency Identification (RFID) solutions to customers worldwide since 1993. The company designs, manufactures and sells RFID products which support a broad range of RFID tags (EPC and ISO) and frequencies (LF/HF/UHF). On April 13, 2006, Sirit Inc. acquired the assets of SAMSys Technologies Inc. including all of its RFID products and solutions. SAMSys Technologies Inc. (SAMSys), founded in 1995, was a world-leading provider of radio frequency identification (RFID) hardware solutions and RFID integration consulting services designed to evaluate and recommend optimal RFID solutions to enhance existing business process. Sirit is headquartered in Mississauga, Ontario, Canada.

• Sarnoff, *http://www.sarnoff.com/products_services/communications_solutions/rf/index.asp* (US)

Sarnoff Corporation produces innovations in electronic, biomedical and information technology. Founded in 1942 as RCA Laboratories, it develops breakthroughs in ICs, lasers, and imagers; drug discovery, manufacture and delivery; digital TV and video for security, surveillance, and entertainment; high-performance networking; and wireless communications. Its history includes the development of color TV, the liquid-crystal display, and the disposable hearing aid, and a leadership role in creating the new U.S. digital and HDTV standard. It is a subsidiary of SRI International and is headquartered in Princeton, NJ, USA.

• Symbol, *http://www.symbol.com/products/rfid/rfid.html* (US)

Symbol Technologies, Inc. engages in the design, development, manufacture, and servicing products and systems used in enterprise mobility solutions. Its products include data capture products, mobile computing platforms and software management tools, wireless infrastructure, and radio frequency identification infrastructure and tags, and are sold as both integrated solutions and individual devices. Symbol Technologies was founded in 1973 and is headquartered Holtsville, New York.

- TEK Industries,
  http://www.tekind.com/rfid.htm (US)

  TEK Industries is a privately held company based in Vernon, CT, USA. TEK Industries offers a full range of readers, handheld data collection terminals, and specialty RFID tags.

- UPM Raflatac,
  http://www.rafsec.com/homeb.html (EU)

  In January 2006, RF and contactless technology developer UPM Rafsec has merged with label-maker Raflatac to form UPM Raflatac. The combined Finland-based company has 2,300 employees and annual sales of 850 million EUR. UPM Raflatac develops and manufactures RFID (radio frequency identification) tags used in e.g. product identification and supply chain management. UPM UPM is a world leading RFID tag manufacturer and a pioneer of the EPC (electronic product code) standard, specialized in high-quality, high-volume production. The company is headquartered in Tampere, Finland and it has a factory in Jyväskylä, Finland. Sales offices are in the USA, Netherlands, Germany, China, Japan and Singapore.

- Xtag,
  http://www.xtagltd.co.uk/ (EU)

  Xtag is a Leeds, UK, based firm providing RFID specialized solutions for healthcare. Their Xtag Baby System is a leading infant protection system.

- Zebra Technologies,
  http://www.zebra.com/id/zebra/na/en/index/products/printers/rfid.html (US)

  Zebra Technologies is a global provider of rugged and reliable specialty printing solutions, including on-demand thermal bar code label and receipt printers and supplies, plastic card printers, RFID smart label printer/encoders, certified smart media, and digital photo printers. Zebra Tech. is based in Chicago, IL, USA, and has 28 other locations in 19 countries with about 2500 employees.

5.1.4. System integrators

Here are included the technically smart companies that provide typically small turn key RFID systems making work together hardware and software infrastructure components. They typically operate in deep contact with customers cooperating with them in the identification of the (technical) needs and proposing alternative solutions. Eventually they will provide the needed hardware and software components, may be produced on their own, and install them at the customer premises and ensure they work together correctly. The most of them will not take care of application specific aspects.

- Aeroscout,
  http://www.aeroscout.com/ (US)

  AeroScout provides enterprise visibility solutions that bridge the gap between Wi-Fi, RFID and GPS. AeroScout enables standards-based location and presence-based applications for indoor and outdoor environments where real-time visibility of assets and people is required to drive revenues or cut costs. Aeroscout is base in San Mateo, CA, USA.

- Checkpoint Systems,
  http://www.checkpointsystems.com/default.aspx?page=epcrfid (US)

  Checkpoint Systems, Inc., is a multinational manufacturer and marketer of technology-driven solutions for retail security, labelling, and merchandising. Checkpoint is the leading provider of radio frequency- (RF) based shrink management solutions to the global retail industry. The company has some 4000 employees and is headquartered in Thorofare, NJ , USA.

- Feig Electronic,
  http://www.feig.de/ -> OBID (EU)

  FEIG ELECTRONIC GmbH has specialized in contactless identification (RFID), door controllers and traffic sensor technology. FEIG ELECTRONIC was established in 1970 and employs about 150 staff members. The company is located in Weilburg, Germany.

- Savi Technology,[41]
  http://www.savi.com (US)

  Savi Technology provides supply chain asset management, security and collaboration software that is uniquely integrated with automatic data collection and identification systems to provide real-time logistics solutions. Founded in 1989, Savi Technology is headquartered in Sunnyvale, California, USA with offices in London, South Africa, Taiwan and Singapore.

- RFCode,
  http://www.rfcode.com/ (US)

  RF Code is a developer of hybrid RFID data management software and enabling technologies. They provide software suite for Auto-ID data collection and distribution. RF Code manufacture active RFID tags and readers. RF Code is a privately-held company headquartered in Mesa, Arizona, USA.

5.1.5. Software providers

These are the companies that are focused on the development and integration of the software components needed for RFID applications. These components can be at the middleware & DB level as well at the Application & Processes level. Here might be identified both small local software houses that cooperate with system integrators to provide complete solutions, and big players like Oracle, BEA, etc.

- BEA,
  http://www.bea.com/content/products/weblogic/rfid/index.htm (US)

  BEA Systems, Inc. (BEA) is provider of enterprise application and a line of service infrastructure products to facilitate service-oriented architecture (SOA) implementations. BEA has acquired in 2005 Connecterra, one of the first developers of RFID middleware. BEA is active in EPCglobal as contributor and leader of working groups. The company is headquartered in San Jose, CA, USA, and has some 4000 employees.

- CISCO,
  http://www.cisco.com/web/strategy/retail/RFID.html (US)

  CISCO Systems Inc. is a global company that manufactures and sells networking and communications products and provides services associated with that equipment and its use. In their Application Oriented Networking (AON) solution, intended to add application level value to networking equipment, they provide the Connecterra RFID middleware solution. CISCO has more than 38000 employees, worldwide offices, and is headquartered in San Jose, CA, USA.

- Globeranger,
  http://www.globeranger.com/ (US)

  GlobeRanger is the leading provider of RFID, mobility and sensor-based software solutions. iMotion platform serves as the foundation for GlobeRanger and its partners to develop, deploy and manage edge solutions. Founded in 1999, GlobeRanger is headquartered in Richardson, Texas, USA with some 50 employees.

- Microsoft,
  http://www.microsoft.com/industry/retail/solutions/rfid.mspx (US)

  Microsoft Corporation engages in the development, manufacture, licensing, and support of software products for various computing devices worldwide. It operates in three divisions: Platforms and Services, Microsoft Business, and Entertainment and Devices. Microsoft's RFID infrastructure taps the power of the .NET Framework, SQL Server and Visual Studio .NET to make integration and deployment of RFID easier and less costly. Microsoft was founded in 1975 and is headquartered in Redmond, Washington and has 71,000 Full Time Employees.

- OATSystems,
  http://www.oatsystems.com/ (US)

  OATSystems, Inc. is a leader company providing software to support businesses based on RFID framework. As a pioneer in the development of RFID technology, OAT has

[41] In June 2006 Savi Technology has been acquired by Lockheed Martin.

been setting the standards in RFID since the first times for over half a decade. OAT's multinational client base consists of over 75 customers in retail, CPG, consumer electronics, manufacturing, life sciences, aerospace and defence. Headquartered in Waltham, MA.

- Oracle, *http://www.oracle.com/technologies/rfid/index.html* (US)

  Oracle Corporation, together with its subsidiaries, engages in the development, manufacture, distribution, servicing, and marketing of database, middleware, and application software. It offers software license updates, product support, and other services. The company operates in five segments: New Software Licenses, Software License Updates and Products Support, Consulting, On Demand, and Education. Oracle Sensor-Based Services are a comprehensive set of capabilities to capture, manage, analyze, access, and respond to data from sensors such as RFID, location, and temperature. Oracle Corporation was founded in 1977 and is headquartered in Redwood City, California. Full Time Employees: 56,133.

- RedPrairie, *http://www.redprairie.com/uk/default.aspx* (EU)

  RedPrairie provides comprehensive, integrated solutions for supply chain management to a variety of industries. The technology suite includes warehouse management and quality control, transportation and global trade management, workforce performance management, event management, slotting, visibility, performance measurement, and RFID for EPC / ISO compliance and mobile resource management. Stokenchurch, UK(EMEA HQ), Waukesha, Wisconsin (HQ)

- Sybase, *http://www.sybase.com/products/mobilesolutions/rfid_anywhere* (US)

  Sybase, Inc. provides enterprise and mobile software solutions for information management, development, and integration in the United States. Its solutions integrate platforms, databases, and applications; and extend those applications to mobile workers through mobile and Wi-Fi technologies. The company operates through two segments, Infrastructure Platform Group and iAnywhere Solutions, Inc. The Sybase RFID architecture and complementary RFID solution consists of modularized plug-and-play products.. The company was founded in 1984 and is headquartered in Dublin, California. Full Time Employees: 3,715.

- TIBCO, *http://www.tibco.com/solutions/rfid/default.jsp* (US)

  TIBCO Software, Inc. provides business integration and process management software. TIBCO's solutions include three categories of software: Business Process Management Software, Business Optimization Software, and Service-Oriented Architecture. TIBCO is an independent provider of business integration software and standards-compliant RFID solutions. The company was founded in 1985 and is headquartered in Palo Alto, California. Full Time Employees: 1,505.

5.1.6. Consultants and main contractors

These are mostly multinational organizations that lead business projects for medium large organizations. They provide the whole solution starting from the business processes analysis down to the actual system deployment, that is typically subcontracted to system integrators. This cluster can be subdivided into the big technical players (IBM, HP, SAP, etc.) and the business consultants (Deloitte, Accenture, etc.) that are extending their consultancy on technical aspects.

- Accenture, *http://www.accenture.com/* (US)

  Accenture, Ltd., through its subsidiaries, offers management consulting, technology, and outsourcing services worldwide. It operates in five segments: Communications and High Tech (CHT), Financial Services (FS), Products and Services (PS), Resources (RS), and Government. The company was founded in 1995 and was formerly known as Andersen Consulting and changed its name to Accenture, Ltd. in 2001. Accenture provides clients with total end-to-end RFID solutions through its broader supply chain and technology capabilities, including enterprise integration, supply chain execution systems implementation and infrastructure services. Accenture, Ltd. is based in Hamilton, Bermuda. Full Time Employees: 123,000.

- ATOS,
http://www.atosorigin.com/wp_RFID.htm (EU)

  Atos Origin is a leading international IT services provider. The company, that is also the official worldwide IT partner for the Olympic Games, offers the entire spectrum of information technology consultancy and services. Its areas of expertise include consulting, systems integration and outsourcing. Currently generates an annual turnover of more than 5.5 billion euros and employs a workforce of 47,000 in 40 countries. Atos Origin has the capability to provide consultancy and design, build and operate RFID technical solutions. Atos Origin is quoted on the Paris Euronext Premier Marché and trades as Atos Origin, Atos Euronext Market Solutions, Atos Worldline, and Atos Consulting.

- Cap Gemini,
http://www.capgemini.com/resources/success-stories/by_solution/rfid/ (EU)

  Capgemini is one of the world's foremost providers of Consulting, Technology and Outsourcing services. The company helps businesses implement growth strategies, leverage technology, and thrive through the power of collaboration. Capgemini employs approximately 60,000 people worldwide and reported 2005 global revenues of 6.954 billion euros. As one of the early RFID pioneers, they have deployed RFID for clients in multiple industries and around the globe. They are actively involved with Electronic Product Code (EPC) standards, and are currently leading several RFID pilot projects.

- Deloitte,
http://www.deloitte.com/ (EU)

  Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With 135,000 employees worldwide, Deloitte delivers services in four professional areas—audit, tax, consulting, and financial advisory services—Deloitte Consulting offers consultancy services on RFID business process methodology and strategic assessment.

- HP,
http://h20223.www2.hp.com/ (US)

  Hewlett-Packard Company provides products, technologies, solutions, and services to individual consumers, small and medium sized businesses, and large enterprises worldwide. The company provides industry standard servers and business critical servers and a number of other computer technologies. HP and OAT deployed RFID at multiple locations across HP's supply chain to provide real-time visibility of inventory and goods movement. HP and OAT developed best practices for delivering RFID solutions in manufacturing and distribution operations and now offer this integrated, tested solution to other customers. Hewlett-Packard was founded in 1939, is headquartered in Palo Alto, California. Full Time Employees: 150,000.

- IBM,
http://www-03.ibm.com/solutions/business-solutions/sensors/index.jsp (US)

  International Business Machines Corporation (IBM) operates as an information technology (IT) company worldwide. It has three segments: Systems and Financing, Software, and Services. The company offers its products and services to a broad range of sectors. IBM's RFID offerings span from consultancy to actual implementation and outsourcing fo applications such as supply chain management or asset management. The company is based in Armonk, New York. Full Time Employees: 341,750.

- Lockheed Martin,
http://www.lockheedmartin.com/ (US)

  Lockheed Martin Corporation engages in the research, design, development, manufacture, integration, operation, and sustain of technology systems, products, and services. The company's Information and Technology Services segment provides IT and related, and other technology services to federal agencies and other customers. Lockheed Martin Corporation has entered the RFID market with the acquisition of Savi Technology, Inc.(Savi), a provider of active radio frequency identification (RFID) solutions. Lockheed Martin was founded in 1909 and is headquartered in Bethesda, Maryland. Full Time Employees:135,000.

- Manhattan Associates, *http://www.manh.com/* (US)

  Manhattan Associates, Inc. engages in the development and provision of supply chain software solutions for the planning and execution of supply chain activities. Its solutions include Integrated Planning Solutions, Integrated Logistics Solutions, Performance Management, and Logistics Event Management Architecture. Manhattan Associates has a team of qualified RFID professionals that has significant experience in supply chain operations. The company was founded in 1995 and is headquartered in Atlanta, Georgia.

- Northrop-Grumman, *http://www.it.northropgrumman.com/offer/enterprise/rfid.html* (US)

  Northrop Grumman Corporation provides products, services, and solutions in information and services, aerospace, electronics, and shipbuilding to the military, government, and commercial customers in the United States and internationally. The company provides airborne radar, navigation systems, electronic countermeasures, precision weapons, airspace management systems, space systems, marine and naval systems, communications systems, government systems, and logistics services. Northrop Grumman provides support to companies in implementing RFID within their supply chains. For nearly 2 decades Northrop Grumman has performed as a systems integrator of Automatic Information Technology, AIT, including RFID, solutions. The company was founded in 1939 and is headquartered in Los Angeles, California. Full Time Employees: 123,600.

- SAP, *http://www.sap.com/solutions/business-suite/scm/rfid/index.epx* (EU)

  SAP AG engages in developing and licensing business software solutions. Its solution portfolios support the business processes of approximately 25 industries, including high tech, retail, financial services, healthcare, and the public sector. Powered by the SAP NetWeaver platform, SAP business applications enable enterprises of various sizes around the world in managing customer relationships, partner collaboration, and supply chains and business operations. As a market leader in solutions that link RFID data to business application software, SAP is actively supporting standards bodies that are seeking to develop ways to implement this promising technology in a practical and responsible way. SAP was founded in 1972 and is headquartered in Walldorf, Germany. Full Time Employees: 35,873.

- SUN Microsystems, *http://www.sun.com/software/products/rfid/* (US)

  Sun Microsystems, Inc. focuses on providing products and services for network computing. It provides network computing infrastructure solutions that consist of computer systems, network storage systems, support services, and professional and knowledge services. These services enable the company's customers to architect, implement, and deploy systems within their information technology environments. The company also offers a range of system/network architecture, implementation, and management, as well as consulting, skills migration, and training. Sun Industry Solutions comprise a set of pretested, RFID-specific solution architectures that use Java System RFID Software and thirdparty products to address specific industry problems. Sun Microsystems was founded in 1982 and is headquartered in Santa Clara, California. Full Time Employees: 31,000.

5.1.7. Non offering related actors

On different planes from the one depicted, other entities that might have a role on RFID issues can be considered. These are e.g. customer organizations, standardization bodies, governments. All of them play a regulating role aiming at achieving common agreements and protecting public interests. As they will mainly react to the market evolution rather than play a leadership role, they will not be considered in this discussion.

- Indicod ECR, *http://www.indicod-ecr.it/progetti/index.php (EU)*

  Indicod-Ecr is an institute that associates more that 30.000 industrial enterprises of large consumption and active modern distribution in Italy. Its mission is the improvement of the large consumption companies' operation effectiveness and efficiency. With reference to the RFID, Indicod-Ecr is taking care of the diffusion in Italy of the EPC standard, developed by Ean International in collaboration with the Massachusetts Institute of Technology.

- EPCglobal, *http://www.epcglobalinc.org/* (US)

  EPCglobal is leading the development of industry-driven standards for the Electronic Product Code™ (EPC) to support the use of Radio Frequency Identification (RFID) in today's fast-moving, information rich, trading networks. It is a subscriber-driven organisation comprised of industry leaders and organisations focused on creating global standards for the EPCglobal Network™. Their goal is increased visibility and efficiency throughout the supply chain and higher quality information flow between companies and their key trading partners.

- Privacy Commissioners Conference, *http://www.privacyconference2003.org*

  The theme of this year's Conference is "Practical Privacy for People, Government and Business". In this, the 25th year of the conference looks forward to exploring advances in privacy and building platforms and solutions that enhance the privacy choices of all citizens. The aim is to provide the opportunity for Commissioners to engage in private and thoughtful discussions as well as allowing for debate with delegates and speakers from the private sector, public administration and other interested groups.

5.2. Market key drivers

5.2.1. Radio standards and spectrum allocation

Everybody agrees on the fact that RFID standards are available. Indeed there are a lot of them incompatible one with the other. At the radio level, two of them are emerging as the most relevant: 13.56 MHz ISO18000-3 and UHF (860-960 MHz) ISO 18000-6 as they are almost worldwide adopted (in the sense that the same tag is readable in USA and in Europe as well; see Section 3.2 for a general overview of ISO standards). The first one allows for tags to be read from a distance of a few centimetres and thus is suitable for ePayments, eTicketing, personal identification. The UHF tag can be read from a reader placed some meters away and this makes it suitable for logistics and supply chain applications. It should be noted that the ISO-18000-6 UHF spectrum standard though endorsed in most countries by local legislation has not yet been made completely available by governments for actual applications, as happens in France, Italy, Turkey. This situation blocks initiatives and market development.

Relevance should be given to EPCglobal that is the only body active on the definition of global standards for the Supply Chain on radio level, coding level, software interface level in order to allow for an open supply chain and goods traceability.

5.2.2. RFID versus barcode

As was described in 2.2.4, RFID technology presents advantages over BarCode technology (no line of sight, environment independent, etc). Also, RFID tags can be read through e.g. the sides of a carton aggregated package. Major drawbacks are technological and related to known interference of radio signals with metals (reflecting radio waves) and water (absorbing radio waves) that makes it hard to use this technology on water bottles (almost solved with EPCglobal Class 1 Gen 2 tags) and on beer cans. RFID is a new technology and still requires fine tuning of antennas and readers in order to achieve a high rate of read success.

The barcode technology is mature and is reliable at higher level than RFID. Moreover the tag itself has negligible cost (see Section 5.2.5). One of the main drawbacks is the need for human intervention in reading the tag in order to find the tag on the package and to point the laser reader on it.

Last but not least the barcode only identifies a class of items while RFID (actually EPC) has the capability of identifying the item itself.

Retail supply chain is today still relying heavily on barcode technology and the drivers to move to a new expensive and not yet stable technology are to be carefully evaluated by all actors (see: The ROI issue).

5.2.3. The "return on investment" challenge

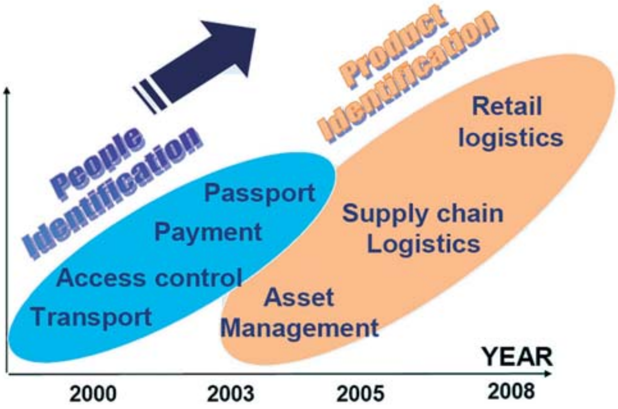
This is the main issue put forward by firms evaluating the opportunity of introducing RFID technology. Most companies being forced by Wal*Mart to supply goods tagged with RFID have chosen the so called Slap-N-Ship solution: they just added RFID printers station on outbound logistics gates and tag packages while they are being shipped. This is also called the "Compliance" or "Mandate" solution, the minimum investment needed to comply with the retailer requirements. This makes the point in the sense that it is felt by companies as an add-on cost affecting retail prices.

The point made by RFID technology manufacturers and consultancy firms is that this technology can support the automation of the production and distribution processes, improving quality control and thus allowing for cost savings and overall better performances. This can be achieved by thinking of internal processes in a completely new way and restructuring the company. This would require major expenses and investments with the involvement of consultants for the reorganization of the processes specialized firms to identify the proper RFID technology (active/passive, frequency, packaging, reader gates,…), software companies providing applications, system integrators to put together the new system with legacy systems. The question is what would be the return of these investments: most companies today feel that the added value of putting RFID to work does not deserve the required effort.

5.2.4. Privacy concerns

Since RFID tags can be scanned at a distance, people having with them items tagged with RFID could be scanned by RFID readers without them being aware. And if there is some way to associate the tagged items with the identity of people (e.g. the fidelity card or the bank card used when the items where bought) then there is a privacy abuse issue. Although Class1Gen2 are claimed to be very secure and they can be "killed", still there is no way to ensure that this is effectively done and, any how, people are very concerned with the possible misuse of the technology. Retailers are consequently very concerned on the issue because if they adopt the RFID technology, customers might prefer to choose more privacy enhanced solutions.

Figure 5-3: RFID applications evolution[42]



[42] Source: ASK

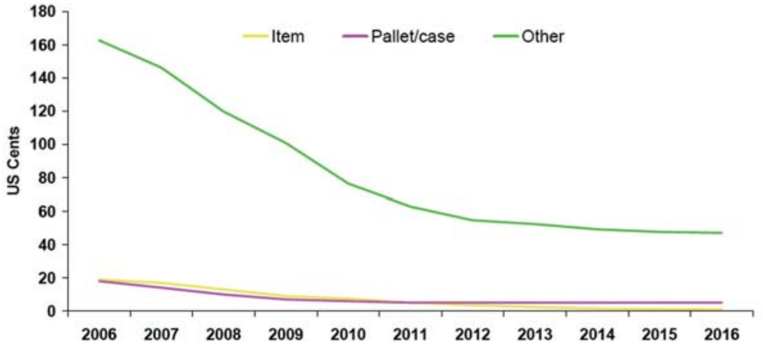
It has to be noted that these concerns are not referring to "people identification" applications that are already being successfully deployed (Figure 5-3). The focus is here put on the possible association of the identity of people and the tagged items they are carrying with them. Without them being aware, a reader might get the data of e.g. the medicine they are carrying in the bag, thus enabling the identification of their health status.

5.2.5. The tag cost

Currently (April 2006) major technology providers say they might accept big orders of packaged Class1Gen2 RFID tags for 0.20 USD each. The tag price is decreasing but the added cost is not yet acceptable for applications at item level (except for valuable goods), see *Figure 5-4*. Tag price is expected to drop within a few years down to the 0.05 USD that, analysts say, will boost the wide scale adoption of item level tagging. The tag price is dependent on a number of factors related to the silicon chips, the packaging (putting together the chip with the antenna on a suitable carrier e.g. a paper sticker), the royalties for patents and indeed is influenced by the still small demand. From a hard technology standpoint the research being carried out on polymer based IC, and on alternative radio technologies (e.g. Digital Chipless Tag), might bear results in short time. Metallic ink printing is already used to "print" antennas on the tag package instead of using photolithography technology. *Figure 5-5* presents categories of technologies related to cost and volume of tags.

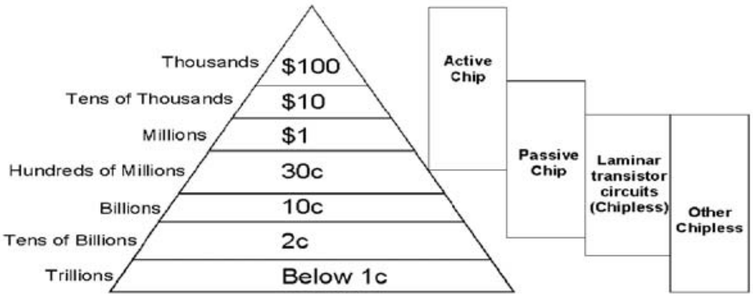
The price performance contest will probably not be an issue, at least in logistics applications. In fact EPCglobal philosophy sounds like "keep all intelligence out of the tag": the tag is needed just to identify goods and putting too much information on those might result in greater possibility for counterfeiting. Moreover the logistics RFID market will be volume based. A different evolutionary path might take place for active tags: as prices fall down and as, once purchased, active tags are expected to function for some time, manufacturers might push more capabilities on board in order to keep the prices high.

Figure 5-4: Average TAG price per application 2006-2016



Source IDTechEx

Figure 5-5: Technologies appropriate to the different level of TAG cost and volume



Source IDTechEx

5.2.6. Goods traceability

As already mentioned the Electronic Product Code (EPC), information component of the RFID tag encompasses the identification of each single item, whereas the bar code is capable of the identification of an item class. This means that the EPC on, e.g. a heating equipment, allows ideally anybody to go back to where and when it was built, with which components etc. This helps very much the maintenance of the equipment as the field technician can rapidly identify the spare parts needed for that specific item. The manufacturer can as well check for problems common to that specific shipment and eventually recall the equipment to solve possibly harmful defects. This would highly enhance the quality of the products as well as the "after sales" services. Moreover, Governments have the opportunity to require manufacturers to be able to rapidly recall defective goods, either equipment or food, possibly relevant to the same shipment, in order to ensure population safety.

5.2.7. "IT doesn't matter" paradox

From a more general standpoint, there is a still ongoing discussion on the fact that a company investing in IT does not necessarily perform better than the others. A provocative article (Carr, 2003) sustained that IT is becoming a commodity (is a widely available not differentiating resource) and in this context it is preferable to be a follower than a leader with respect to IT innovation. This reflects what is a common feeling, especially in case of SMEs that typically are reluctant to invest in ICT innovation because this implies either the training and allocation of skilled resources or expensive outsourcing solutions. In both cases resources would be diverted away from the core business. The disruption of this situation might come from external (international) competition that will probably force ICT "laggards" to recover the situation in order to cooperate with peers and widen the market reach.

5.3. Strengths, weaknesses, opportunities, threats

A SWOT Analysis is "a strategic planning tool used to evaluate the Strengths, Weaknesses, Opportunities, and Threats involved in a project or in a business venture or in any other situation requiring a decision".[43] Though no decision issue is being tackled in this document, this tool might be found nevertheless helpful to give a more synthetic view on the question whether, in very general terms, it is worthwhile to a company to make investments in RFID technology. *Table 5-1* presents a mapping of the described market drivers on a SWOT analysis chart, together with other elements presented in more details later in the study.

Table 5-1: SWOT analysis of RFID market perspectives

STRENGTHS: *What are the factors that make it valuable?* - Technology characteristics: radio readable, programmable, compact, robust, low power, - Maturity: the technology providers market is well developed; - Large scale projects are moving onward and give feedback valuable field experience;	**OPPORTUNITIES:** *What are the factors pushing for it?* - RFID can help European small companies in finding new ways to aggregate and compete with larger companies; - An enhancement of the overall quality of the production can be achieved with an automated monitoring; - Keeping update with the technology will allow to keep customers (e.g. Wal*mart);
WEAKNESSES: *What are its actual limitations?* - Technology limitations: e.g. the tagging of metal or water rich (including food) stuff is often unreliable; - Still expensive in terms of tag, equipment, implementation for a number of applications; - Lack of well established standards: many are in place and poor agreement on which ones will survive.	**THREATS:** *What bad factors might hamper the investment exploitation?* - By making poor analysis about where are the technology benefit in the foreseen RFID application, there is the risk of missing real benefit; - In some cases the undervaluation of non technical issues (e.g. fear for security issues by people) might lead to unsuccessful results; - Though the technology is quite mature, patents on RFID are continuously being submitted: the most promising technology today might be displaced by a new one before the mass adoption.

[43] *http://en.wikipedia.org/wiki/SWOT_Analysis*

5.4. Market forecasts and trends

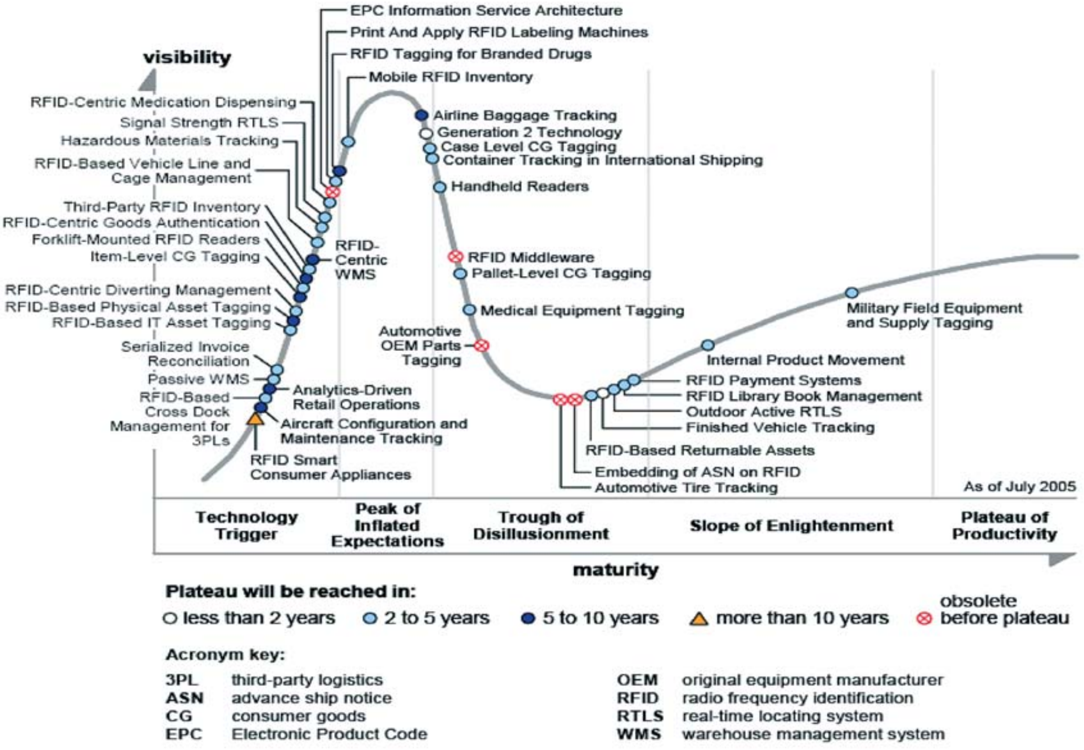
5.4.1. RFID maturity: the hype cycle

Technology consultant Gartner propose the RFID Hype Cycle scheme (Gartner, 2005a), presented in *Figure 5-6*. This is a curve that will be transited by any new technology at different speeds. Instead of a time axis there are five maturity phases. The other axis represents the "visibility" factor indicating how much the technology/application is under the spotlights.

The interest in a technology, in very general terms, Gartner says is initially triggered by some demonstration or proof of concept which is given resonance by the media. Then enthusiastic expectations will take the stage with often unrealistic projections. After a number of failures the attention will be lost while the technology is still there and becomes better understood in its potential and limitations. At that point it starts to be applied in an effective way through the availability of mature products.

As far as the hype cycle for RFID technologies and applications (*Figure 5-6*) (Gartner, 2005c), most of them are still considered to be immature. Though with sometimes questionable distinctions, Gartner's position is that much resonance has been given to the potential of RFID but still there is a number of scattered technologies under the same umbrella without a common rationale and most applications are still mainly just a matter for newsletter's breaking news. Nevertheless, taking into account the colour code (light blue ones) of the bullets on the curve, it is clear that they agree on the fact that in a few years a number of them will become mature. Apart from military applications that are subject to quite peculiar rules, the maturity is being currently reached by asset tracking and management applications (healthcare and/or industrial) and in others where tags can be reused (Library Management, Returnable Assets). This can be easily explained by considering that the tags are still expensive and their reuse can dramatically lower OPEX[44] components in ROI calculations and make the application profitable.

Figure 5-6: RFID hype cycle[45]



[44] Operational Expenditures (OPEX) are the on-going costs for running a system while Capital Expenditures (CAPEX) refer to the cost of system development

[45] Source: *Gartner 2005a*

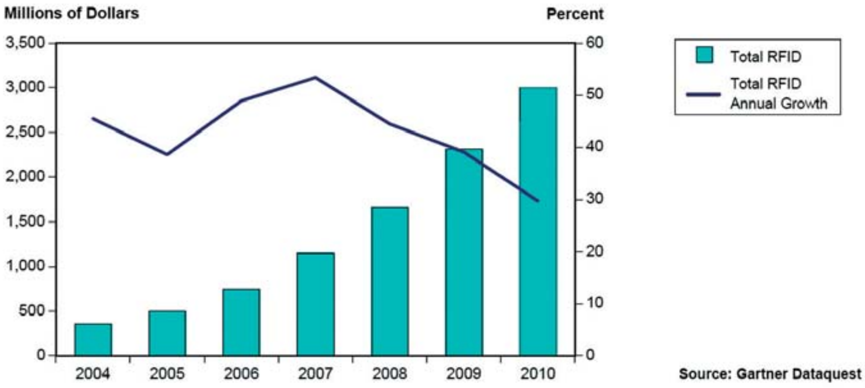
It has to be noted that Gartner's analysis does not take into account RFID for personal identification.

5.4.2. Market forecasts

Any RFID market forecast should be carefully evaluated with respect to the actual market it is referring to. A number of figures are made available to the public at conferences and on the web as well as in specialized reports, and they seem to propose sometimes contrasting numbers. In the following we will provide for a rationale to understand figures provided by Gartner Research and IDTechEx.

The first issue to take into account is the underlying market segmentation. As explained in the previous chapters, the term RFID encompasses a very broad variety of technologies and application areas and forecasts often refer to only a few application areas. As an example Gartner (Gartner, 2005b) claims that the RFID market will experience an annual growth rate somewhere between 30% and 50% in the years 2004-2010 ending up at 3 billion USD in 2010 (see Figure 5-7). They say this refers to "*the use of RFID technologies within a supply chain environment to improve the visibility, management and security of cargo shipments or supply chain assets, such as conveyances or valuable mobile assets. The applications and hardware that are used outside of the above environment were excluded. These would include consumer uses, such as contactless smart cards.*"

Figure 5-7: RFID, worldwide size and growth, 2004-2010



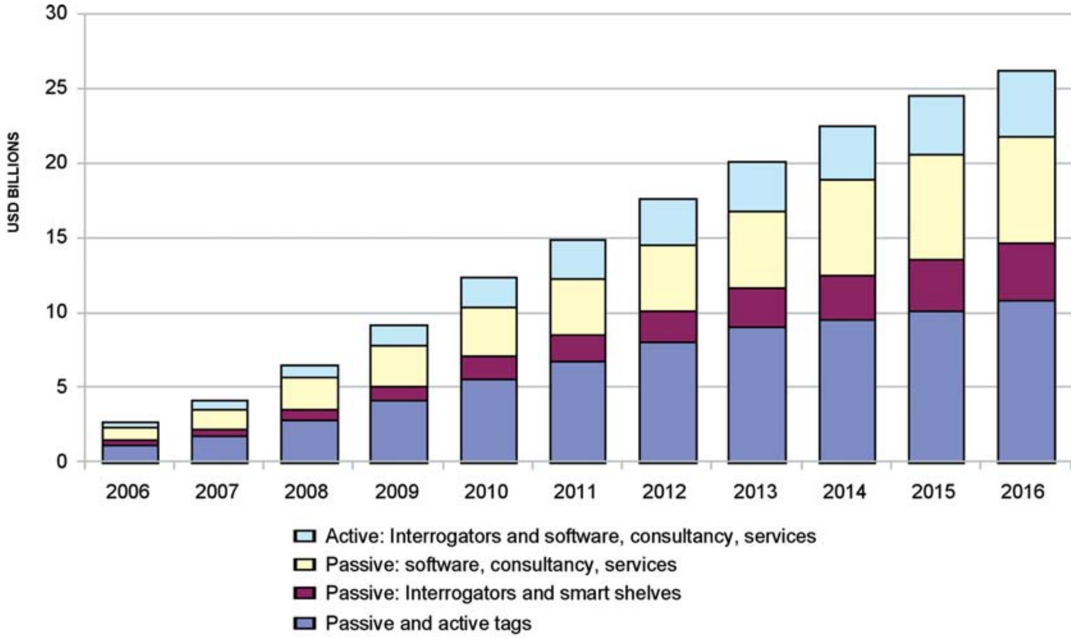
Source: Gartner Dataquest (September 2005)

This means that they include in the forecast both passive and active RFID technologies of all kind in Supply Chain applications. They exclude any non supply chain related application (in addition to the explicitly cited contactless smart cards) and thus animal identification, highway toll payment, patient tracking and blood-patient cross check in healthcare, and, (it is not clear) ship container management and tracking. Moreover, although not explicitly tackled by Gartner, we might assume that the forecast refer to both CAPEX (needed HW and SW and other infrastructure as well as initial set-up services including consultancy) and OPEX (consumables and operational services) related to RFID projects.

IDTechEx (2005a) provides an overall forecast for RFID technology. With this approach the (about) 12 billion USD figure in 2010 is compatible with but not directly comparable to the Gartner's 3 billion USD. Neither is the 2006 IDTechEx 2500 million USD vs. Gartner's 700 million USD in the same year.

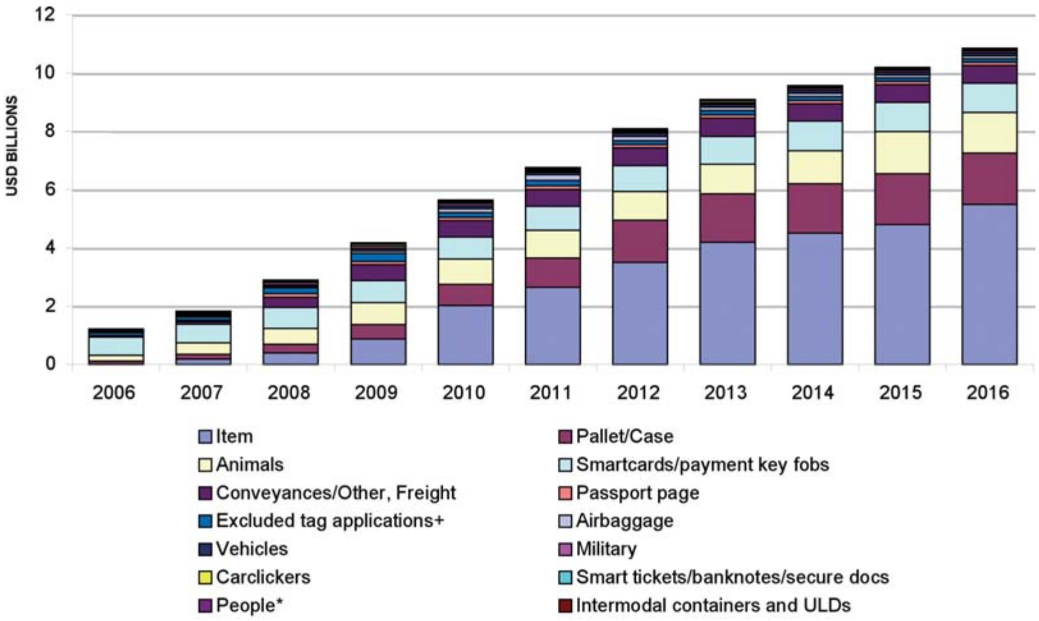
The IDTechEx report provides some more data as depicted in Figure 5-8. The bottom series represents the tag (both passive and active) market value which is then splitted into the different application areas in Figure 5-9. The two bottom series ("Item" and "Pallet/Case") in Figure 5-9, can be assumed as the only ones referring to supply chain applications.

Figure 5-8: Total RFID market projections 2006-2016[46]



Though IDTechEX does not provide a splitting of the non-tag costs (hardware, software, services) per application area, we can have an indication by observing in Figure 5-9 that these are more than the tags costs. By extrapolating this observation and applying it to the two bottom line series in Figure 5-8, we can get values comparable to Gartner ones.

Figure 5-9: RFID tag market forecast[47]

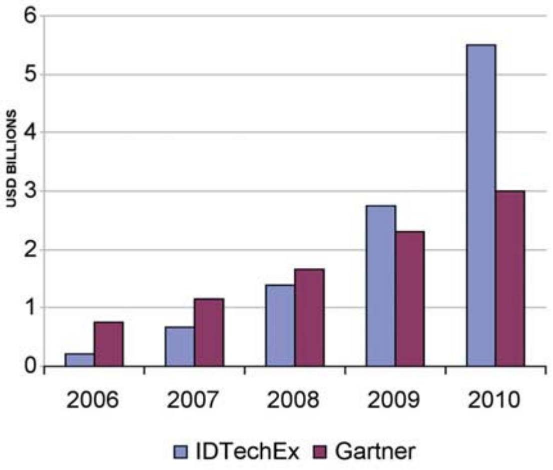


[46] Source IDTechEx, 2005a

[47] Source IDTechEx, 2005a

A comparison is proposed in Figure 5-10 where it can be seen that the two mainly agree on the dimension of the market but IDTechEX seems to forecast a steeper growth.

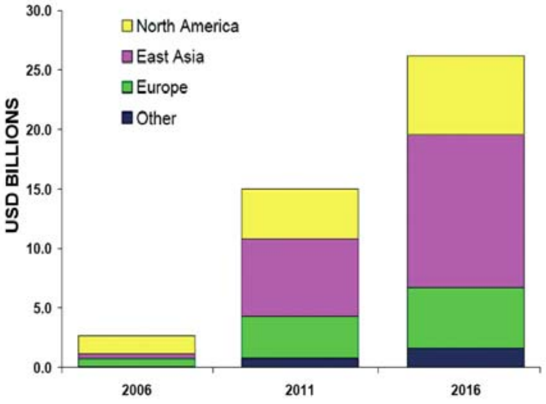
Figure 5-10: IDTechEx (elaboration) and Gartner forecasts comparison



It is also evident that the major share is taken by Supply Chain applications that make almost half of the total. Nevertheless it should be noted that, though item level tagging will determine an exponential growth of passive tag volumes, it is expected that the other applications will keep the pace. Among these, importance is given to animal tagging and electronic payment.

As far as geographical market distribution, it should also be noted that East Asia, which currently stays quite behind Europe and US is expected to gain the greatest share, as manufacturing will probably be massively moved to China. Nowadays, Europe is placed quite behind the US but it is expected to gain a comparable positioning (Figure 5-11). It should also be noted that Europe has still national frequency allocation issues to be resolved, that might put obstacles to the diffusion of EPCglobal applications in EU.

Figure 5-11: Total spend on RFID systems, service and tags by territory[48]



5.5. RFID patents

The number of patents assigned between year 1974 through 2003 is 4279[49] and 697 in the year 2004, with a year on year increase of 65% in the last few years.[50] These numbers give an idea of the growth of interest by manufacturers in this field. A study made by RFID Journal in 2005[51] reports some 150 patents to be relevant to RFID market. These are classified into four Technical Quality Ratings hereafter reported:

1. The most significant blocking RFID patents. They usually include a breakthrough technical specification and will be extremely difficult or impossible to work around.
2. Important patents with key technical innovation that appear to be difficult to work around when designing certain RFID products.
3. Useful patents with significant technical innovation but narrower scope. While they have technical merit, there are alternative solutions that could be implemented if necessary.
4. Secondary patents that – while perhaps useful for some special products –appear only marginally useful in mainstream RFID applications.

[48] Source IDTechEx, 2005a

[49] http://www.highimpactip.com/report_intro.htm

[50] http://www.centredoc.ch/en/centreE.asp/0-0-2667-132-76-0/, http://www.dutchrfid.com/artikelen/rfid/rfid-watcher-for-patents.html

[51] http://www.rfidjournal.net/live05/IP/Room_miss_100pm_stewart.pdf

Table 5-2 presents these 150 patents in 2005 by owner company and rank. It should be noted that all of them are US based with the exception of Tadiran that is Israeli based.

Table 5-2: Patent ownership summary (RFID Journal Live[52])

Company	A-Patents	B-Patents	C-Patents	Total
Intermec	7	13	9	23%
Checkpoint	1	8	10	10%
Motorola	3	5	6	10%
Micron	1	5	7	7%
Avid	2	2	—	5%
Lucent	1	3	2	5%
Samsys	—	3	2	3%
TI	1	—	2	2%
Sarnoff	1	1	—	2%
3M	1	—	—	2%
Alien	1	—	—	2%
Marconi	—	2	1	2%
Northrup	—	2	1	2%
Tadiran	1	—	—	2%
Tek	1	—	—	2%
U of Pittsburgh	1	—	—	2%
Others	—	20	25	19%

It should be noted that, with reference to the highest RFID volume application i.e. integrated logistics and EPCglobal, there is an ongoing legal war on how the patents should be used. Patents holders are demanding high licensing fees (5%), that no one is considering to pay. The most critical issue regards Intermec that claims a number of their patents is critical to Class1 Gen2 RFID, the most recent and promising EPCglobal spec. Nowadays Intermec and Alien Technology are disputing a legal battle on ten patents, the first saying they were infringed by the second and the second claiming that the patents are themselves invalid.

Nevertheless a couple of initiatives are to be reported. The first one was originated by Intermec that – with its "Rapid Start RFID Program" – has initially offered five critical patents for free and an additional nine patents on a "RAND" (reasonable and non-discriminatory) condition. But EPCglobal did not recognize the Intermec patents to be critical and Intermec thus revoked the offer and issued four patents portfolios.

On an opposite side Alien Technology and others[53] have formed an RFID Consortium and selected MPEG LA (*http://www.mpegla.com/index1.cfm*) as administrator of the consortium patents. The charter of the Consortium has not yet been published.

As more than 4000 patents refer to RFID technology with some 270 companies involved and 20 major patents owners it is likely that some litigation and/or licencing costs will be passed to users, also taking into account that a number of key patents are not referable to any particular specification and so cannot be easily overcome.

[52] *http://www.rfidjournal.net/live05/IP/Room_miss_100pm_stewart.pdf*

[53] *http://rfidtribe.com/news-05-12-19.html*

5.6. RFID and SMEs

It can probably be said that every on-going RFID project has been initiated by a big company either running the project entirely on its own or it has also forced other companies, also small ones, to get the technology. As explained in the "Demand key issues" paragraph, the fact is that today putting the RFID technology in place is very expensive in terms of equipment, consultancy to set up the equipment, human effort and cultural leap and consultancy to reorganize processes.

The result is that smaller firms, when forced, adopt the so-called "slap-n-ship" or "compliance" solutions: just what is needed to comply with the requirements issued by vital customers e.g. Wal*Mart and METRO. For this purpose manufacturers are providing all-in-a-box packages made by e.g. Reader+Antenna+Printer+Software needed to properly tag goods just when they are next to be shipped. All analysts agree on the fact that this RFID application has negative ROI. Project costs will sooner or later be passed on to the final customer.

A widespread usage of RFID in the supply chain and a more pervasive knowledge and culture about when and where it is to be successfully applied, will eventually drive SMEs to integration of RFID technologies into their processes.

As far as non supply chain related RFID, it has to be recalled that - as it often happens - the diffusion of these technologies within the mass market might also pull SMEs to adopt some of them to benefit their businesses.

6. Socio-economic aspects of RFID

RFID is a technology which enables a low-cost connection between the physical world and large-scale networks. It is to be expected that such a technology has far reaching implications for our society. The wide spread application of this technology raises privacy and security concerns; other implications of the application of this technology can be foreseen in the social interaction between citizens, and in economic transactions between actors in the market. This issue also includes the human aspects related to the use and acceptance of this technology, i.e. awareness, trust, and user related issues of technology transfer.

It is important for technology developers and policy makers to be aware of the socio-economic and legislative implications of large scale RFID deployment, so that in technological development and policy making appropriate measures can be taken to incorporate accepted social values in development and application of this technology.

The application of RFID might have specific effects on the workplace (i.e. cost reduction and development of new services) and as a consequence have large effects on the employment market in general. An adequate legal framework will be necessary to guarantee a widespread adoption and application of RFID technology.

In this chapter three issues will be dealt with related to the socio-economic and legislative aspects of the widespread deployment of RFID in our society:

- Legal, social and economic aspects of the widespread deployment of the various RFID classes identified;
- Influence of the introduction of RFID on the workplace and the employment market;
- Training requirements due to the widespread adoption of RFID technologies.
- In order to elaborate on these issues the following questions have to be answered:
- Which legal, social and economic aspects of the widespread deployment of RFID can be identified?
- Which of these aspects are applicable to RFID technology in general and which of these aspects are specific for the various applied RFID tag classes?
- What are possible (positive and negative) effects of the RFID technology on the workplace and the employment market and which conclusions can be drawn on the basis of analysis of these effects?
- What kind of different training requirements can be foreseen in relation to the widespread adoption of RFID technologies and which conclusions can be drawn in this context concerning the development and supply of adequate training facilities?

6.1. Framework of the study

6.1.1. Aims and objectives

The aims and objectives of this chapter are to generate an assessment of the socio-economic and legal-ethical aspects that may hinder or promote the diffusion of RFID in Europe. The study has to analyze what main barriers to adoption exist in order to clarify what makes adoption problematic. This analysis also has to elaborate on what can be said about cultural differences with respect to adoption issues.

The study results into a systematic appraisal of barriers and problems to widespread deployment and adoption of RFID in Europe. This study has the form of an essay. The essay describes different relevant perspectives and develops an argumentation for further policies and practices based on both an assessment theory-based framework and an evidence based framework

6.2. Methodology and reading guide

In order to deal with the socio-economic/legislative issues described above the following methodological approach was applied. The approach consists of two main parts.

The first part entails a systematic inventory and analysis of legal, social and economic aspects of the widespread deployment of RFID technology, specified according general issues and (if relevant) according to issues related to specific RFID tag classes. This analysis also includes the user related processes of diffusion and acceptance of RFID-technology. In section 6.4 we describe various aspects of diffusion and adoption of RFID-technology. In section 6.5 we deal with aspects of trust and acceptance of RFID-technology.

The second part (section 6.6) includes the inventory and analysis of labour and employment issues in relation to the application of RFID-technology and in addition gives an overview of training issues related to the operating issues of RFID technology.

To analyze the socio-economic and legal aspects of the wide-spread deployment of RFID the following methods were applied in this study: trend analysis based on desk research and impact analysis and policy options analysis based on expert discussions.

Each task was carried out on the basis of desk research (analysis of concept and models, various opinions, written statements and reviews of trends and developments) and discussions in the project team.

Based on an analysis of these issues a number of conclusions have been formulated concerning awareness activities, marketing efforts and training requirements which will be needed or can be foreseen in relation to the widespread adoption of RFID technologies.

6.3. Theoretical framework on adoption and diffusion of technology

This section brings into focus the process of adoption and diffusion of RFID technology. An important aspect from the perspective of *diffusion and adoption* of RFID technology is the issue of *user perception* in relation to the use of RFID applications. This issue is related to research on *innovation diffusion* and also to *technology acceptance and adoption* in general terms.

Information technology adoption research has been a key stream in the behavioural sciences for many decades. Research in this area has become particularly important to fields of organizational behaviour and management of information systems, given the diffusion of technologies in homes and deployment of information technologies in organizations. This research area also includes studies on the acceptance, adoption and usage of RFID technology, although results of research related to this topic are still rather scarce.

Diffusion and adoption of RFID technology can be considered first of all from the viewpoint of diffusion of innovation. General theories on innovation diffusion will also apply to the introduction of RFID technology in organisations. The same is true for more specific theories on technology acceptance.

6.3.1. Main theories on diffusion of innovation and technology acceptance

Various primary theories have been developed with regard to the acceptance of information technology: i.e. Innovation Diffusion Process Theory, Theory of Reasoned Action, Technology Acceptance Model, Theory of Planned Behaviour and the Socio-Technical Systems Theory.

All these theories are in general terms applicable to the process of introduction, acceptance and application of RFID technology. It goes beyond the framework of this study to discuss these theories in more detail. However, some insight into main theories on diffusion of innovation and technology acceptance might be helpful in understanding the process of diffusion and acceptance of RFID technology.

6.3.2. Innovation diffusion process theory

In 1962 Rogers published the first version of his book ‘The Diffusion of Innovations’, in which he presented his *Innovation Diffusion Process Theory.*

The model defines a process by which market actors adopt a new innovation (see Table 6-1). Actors must first become aware of the innovation. Once awareness of an innovation is established, market actors can at any point enter a persuasion stage during which the actors seek and process information in order to decide whether to adopt the innovation. The timing of the active portion of this stage is highly dependent on the individual and the context in which the individual is operating. At several points in time, the market actors may make a decision not to adopt, to postpone adoption, to continue the search for information, or to adopt the new innovation.

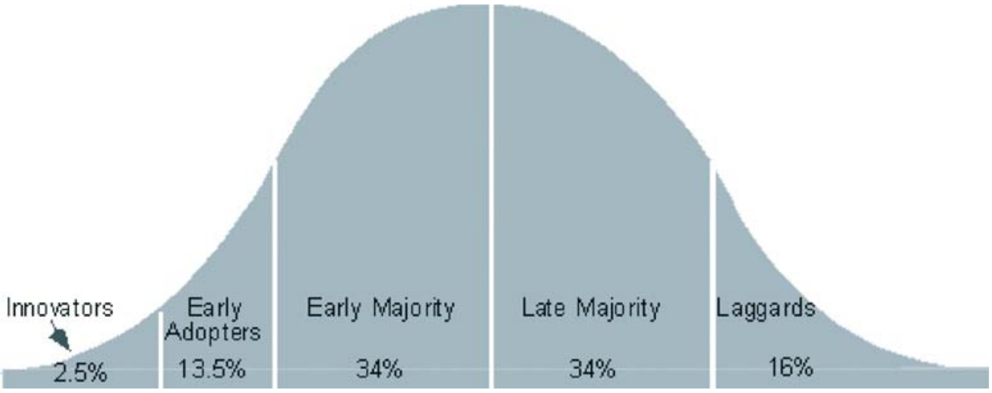
This persuasion stage is followed by an implementation stage in which the actors enact the decision. Finally, actors revaluate or confirm their decisions to adopt and/or their implementation of the decision. The result may be either continuance or discontinuance of the adoption.

Table 6-1: Phases in the development of innovation diffusion processes

PHASES	TYPOLOGY	ACTIVITIES
1	Knowledge/Awareness	People learn about the innovation
2	Persuasion	People are persuaded as to the merits
3	Decision	People decide to adopt
4	Implementation	People implement the innovation
5	Confirmation	People reaffirm or reject the decision

It is understandable that not everybody will go with the same speed through such an adoption process. Rogers has made plots of the percentage of people who adopt an innovation in relation to time. This generates a hyperbolic-form cumulative frequency distribution and on basis of this curve he subdivides a population in five general categories of people regarding their role in innovation processes (with average occurrence in a normal population in %) (See Figure 6-1):

Figure 6-1: innovation diffusion process theory[54]



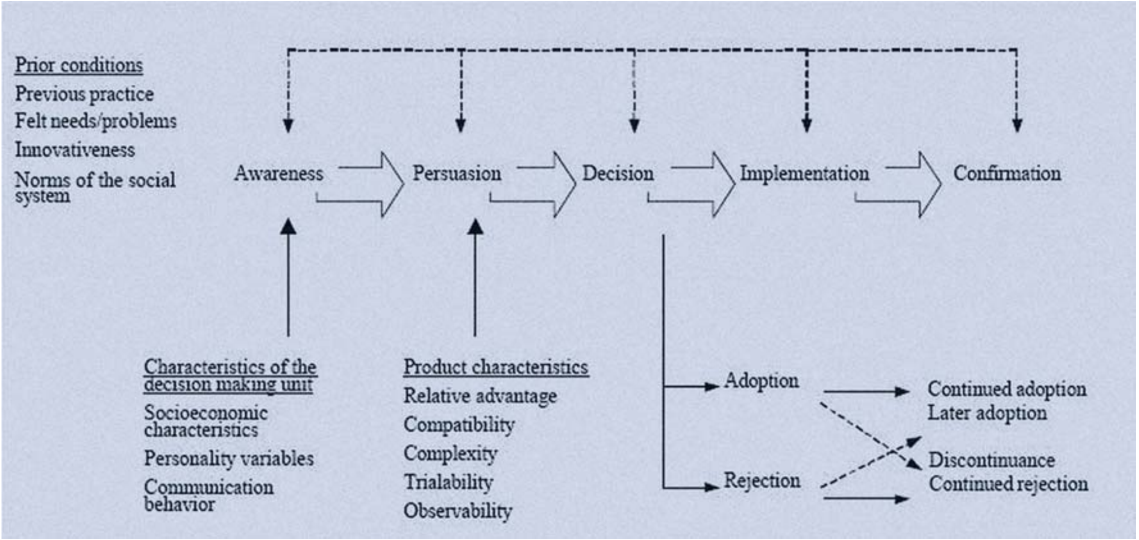
In general, supporting innovators and early adopters will give a boost to innovation processes. But the time frames for adopting an innovation can be compressed or fairly lengthy. For example, awareness of an innovation may precede the decision to adopt by months or years. Further, the decision to adopt and the implementation of the decision may be separate acts and may be separated in time (Reed, Erickson, Ford and Hall, 1996).

As an extension of the Innovation Diffusion Model, Rogers (1995) and Reed and Hall (1998) have identified some prior conditions which influence the awareness phase (see Figure 6-2). They also identified some characteristics of the decision making unit which have an influence on the course of the awareness phase. They also discovered that in the persuasion phase a number of product characteristics play an important role in the innovation diffusion process:

- Relative advantage
- Compatibility
- Complexity
- Ability to carry out trials with the product
- Ability to observe the product.

[54] Source Rogers, 1962

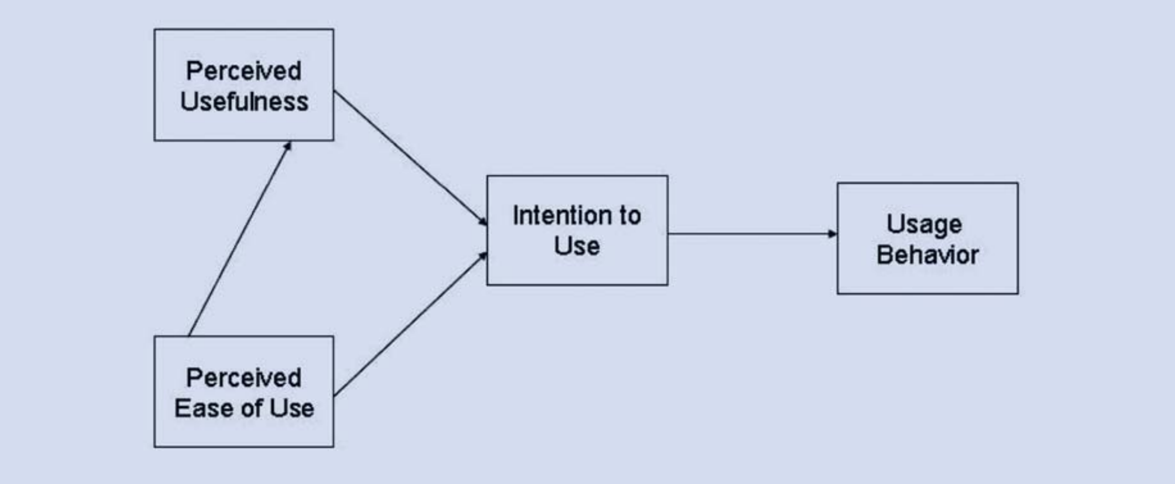
Figure 6-2: Revised innovation diffusion model[55]



6.3.3. Technology acceptance model

In studying user acceptance and use of technology, the Technology Acceptance Model (TAM), first developed by Davis in 1986, is one of the most cited models (see Figure 6-3). According to the TAM, 'perceived usefulness (PU)' and 'perceived ease of use (PEoU)' are primary motivational factors for accepting and using new technologies. PU is the degree to which a person believes that use of technology will produce better outcomes. 'Useful' refers to 'capable of being used advantageously.' In contrast, PEoU is the perception about the degree of effort needed to use a particular system. In this case, 'ease' is conceptualized as 'freedom from difficulty or great effort.' According to the TAM, if a user perceives a specific technology as useful, he will believe in a positive use-performance relationship. Since effort is a finite resource, a user is likely to accept an application when he perceives it as easier to use than another (Rander and Rothchild, 1975).

Figure 6-3: Technology acceptance model[56]



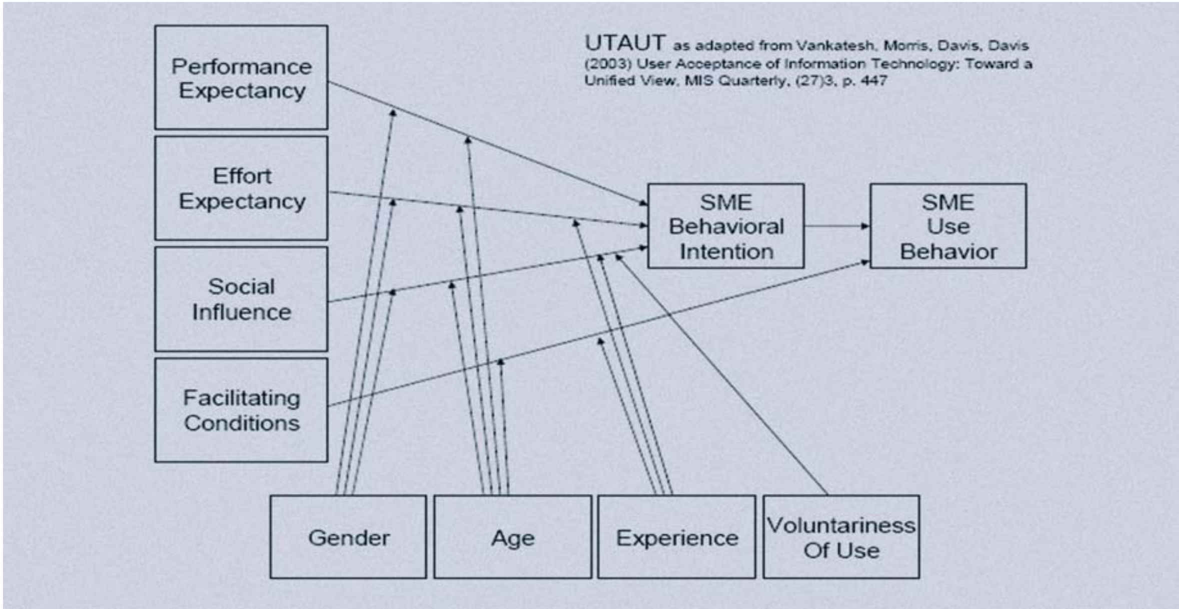
[55] Source: Rogers 1995, Reed and Hall 1998

[56] Source: Davis, 1986

6.3.4. Unified theory of acceptance and use of technology

A large number of studies have been conducted using the original Technology Acceptance Model or an extended version. In an attempt to integrate the main competing user acceptance models, Venkatesh et al. formulated the *Unified Theory of Acceptance and Use of Technology (UTAUT)*. This model (see Figure 6-4) was found to outperform each of the individual models (Venkatesh et al., 2003). In this model also social influences and facilitating conditions are taken into account as well as issues like age, gender, previous experiences and how voluntary actual use is for a user.

Figure 6-4: Unified theory of acceptance and use of technology[57]



6.4. Trust and acceptance of RFID technology

The success of a technological innovation depends heavily on the adoption by consumers. In this context the development of trust between the service provider, the consumer and the systems is of paramount importance. Therefore we analyse here the relation between trust and acceptance of RFID technology.

The concept of RFID technology has a rather broad meaning in terms of technologies applied. A main difference between various technologies is based on the kind of RFID tag classes which are used: active tags or passive tags.

Trust is an issue related to RFID technology, but in general trust will be of more importance when it is related to 'active' tags than it is for 'passive' tags because when tags become more active and are more sophisticated the implications of their actions and any errors they could make become more serious. Trust becomes very important when users may suffer physical, financial or psychological harm because of the actions of RFID technology. This section describes various aspects of trust in relation to the acceptance and adoption of RFID technology.

6.4.1. Definition of trust

Many different definitions of *trust* exist. In the general definition of Rotter (1980) trust is 'a generalized expectancy that the word, promise, oral or written statement of another individual or group can be relied upon.' In the context of RFID technology, this means that the RFID technology can be relied upon to do what it was instructed to do, meant to do and clarified to do.

But it is also necessary that people are in a situation in which they are or might be vulnerable to

[57] Source: Venkatesh et al. 2003

actions of someone else. Without this vulnerability there is no need for trust. In the context of RFID technology this means that people are no longer controlling the software directly, but that they let the process act on their behalf and that they accept the risks that this may entail.

Therefore Bickmore and Cassell (2001) have defined trust in relation to the application of technology as 'people's abstract positive expectations, that they can count on this technology to care for them and be responsive to their needs, now and in the future'.

Patrick (2002) defines trust in this context as 'user's thoughts, feeling, emotions, or behaviours that occur when they feel that technology can be relied upon to act in their best interest when they give up direct control'.

Another aspect is that trust in information systems is often seen in the tradition of cognitive psychology. While this approach has made considerable contributions to computer science and systems engineering, it is to be expected that it will not facilitate our further understanding of trust and adoption of RFID technology.

In the technical literature trust is considered as a purely cognitive process. It is often treated as a utility function that system users try to maximise for their own benefit. However, trust is a non-cognitive function that cannot always be approximated well by mathematical constructs. Approaching trust within its social context may provide a more productive alternative. Seen from this perspective, two observations are important;

Asymmetry in data collection

Collecting personal data by tracking the activities of individuals will be unacceptable for the consumer if it is not reciprocal or transparent. That is, not knowing which organisation is collecting the data, how this data will be used, how to correct errors in the data and whether to expect a return describes the relationship as non-reciprocal and not transparent and introduces asymmetry making it unacceptable for the consumer.

The fact that our profile is formed under circumstances that are well beyond our control, we cannot influence and that it is invisible to us introduces considerable stress to the relationship irrespective of whether the profile is accurate or not.

Affective aspects of interaction

The communication and interaction principle implies that rather than focusing singularly on the trustworthiness of a system, the design should also address the affective aspects of interaction between RFID supported commercial services and the consumer and addresses the emotional impact of system usage.

The term 'affect' encompasses mood, emotion and feelings. Affect is a fundamental aspect of human beings and as such influences reflex, perception, cognition and behaviour. Affective quality is the ability of an object or stimulus to cause changes in one's affect. Perceived affective quality of a system has a positive impact on users' perceived usability of the system.

Although cognition has received more attention than affect in the past decades, researchers in several disciplines have realized the importance of affect and emotion (Ping, 2005). Studies in neuropsychology and social psychology assert that affect or emotion occurs before cognition, but also intervenes with cognition. Affect and cognition can both be considered information processing systems, but with different functions and operating parameters. The affective system is judgmental, assigning positive and negative valence to the environment rapidly and efficiently. The cognitive system interprets and makes sense of the word. Although efforts exist to bring affect and emotion concepts into studies on user acceptance of technology, most of the existing studies are based on the assumption that human beings are rational and behave based on logical information-based thinking.

6.4.2. Trust-risk model of RFID success

Patrick (2002) has developed a model of acceptance of new technology (in his specific situation developed for the acceptance of intelligent agents), based on the separation of trust from perceived risk. This model is an extension of the e-commerce loyalty model developed by Lee, Kim & Moon (2000), which is used to describe user attitudes towards e-commerce applications and transactions. This model could also be applied to trust in relation to RFID technology.

The idea behind the model of Patrick is that feelings of trust and risk can be established quite independently, and together they determine the final success of the technology. Trust contributes to the acceptance of the technology in a positive direction; while risk contributes in a negative direction. The effect is that the two factors interact with each other, so that technology connected with a low degree of trust may still be successful if there is also a low perceived risk. But it is also possible that in very risky situations no amount of trust is able to offset the risk perceived by a user, and in such a situation it will become very difficult to accept the involvement of a specific technology.

It is important to stipulate that the model deals with risk *perceived by the user,* and this perception may, or may not be related to the actual risk of the technology employed in the technology system.

In the trust-risk model of technology success, developed by Patrick (2002), a number of factors are identified which *contribute to trust* and a number of factors which *contribute to perceived risk.*

In Table 6-2 various factors contributing to trust will be identified and described in short and specific recommendations will be connected with each of these factors with regard to the building of trustworthy RFID technology. In Table 6-3 the same will be done for the various factors contributing to perceived risk.

Table 6-2: Factors contributing to trust

Factors contributing to trust	Descriptions	Design recommendations
Ability to trust	People possess a basic trust as a relative stable personality characteristic, but people do not have the same baseline level of trust.	Developers should take into account that users may differ in their baseline level of trust. Some people will need more reassurance than others that the technology can be trusted. This means that interfaces must be flexible and be able to provide more information and reassurance for users that require it.
Experience	Users can change their willingness to trust based on their experiences, of their own or because of hearing about experiences of others.	Designers should support a sharing function so users can share and spread their (hopefully positive) experiences.
Predictable Performance	Systems and interfaces that perform reliably and consistently are more likely to be trusted by users. Also response times should be consistent and predictable, in stead of variable and unpredictable.	Developers should ensure that the interface is consistent and predictable. This means adopting a style guide or the use of interface guidelines in all parts of the system.
Comprehensive information	Systems that provide comprehensive information about their operation are more likely to be understood, and more trusted.	Technology systems must provide an image of their operation so that users can develop a mental model of the way the system works. This also means allowing the users to observe and track the actions performed by the technology, both in real-time and after the fact.
Shared Values	If users feel that the technology values the things that they would, they will have more trust in the agent. In interpersonal relationships, these shared values are often built through informal interactions, such as small talk conversations.	Values between technology and their users can be shared explicitly, i.e. by involving informal social dialogues between user and system
Communication	The amount and effectiveness of communication between the agent and the user also determines the amount of trust by the user. Continual feedback is important here.	The system should repeat its instructions, so that it is clear what the user understood. Error messages should indicate what was understood and what needs to be clarified. Through communications it should be made clear what the capabilities and limits of the systems are.
Interface design	The look and feel of the software that is used to control the system, including factors as appearance, functionality and operation, can contribute to trust by the user.	Most of the generic attributes of good interface design also apply to designing system interfaces.

Table 6-3: Factors contributing to perceived risk

Factors contributing to perceived risk	Descriptions	Design recommendations
Risk Perception Bias	Users have a basic or baseline level of perceived risk. Basic approaches to risk assessment are: fatalism: users feel that they have no control hierarchy: users feel that risks have to be dealt with by controls and regulation individualism: users feel that risks should be taken when appropriate for the individual enclave: users feel that risks are systemic and have to be minimised by the suppliers of the technology	System designers should design systems features that address each of these areas of risk assessment. A system may contain information to explain how users can have control over the risks they are taking.
Uncertainty	By reducing uncertainty also risk perception will be reduced.	The more users know about a system and how it operates, the less they are uncertain about the system and the less they will worry about risk taking.
Personal Details	If more personal details are being provided to the system, perceptions of risk are likely to increase.	System developers should only ask for information that is necessary to do the job, and avoid where possible asking for information that the users might consider sensitive.
Alternatives	Lack of alternative methods to perform a task can lead to feelings of risk.	Within certain limits system designers should offer alternative methods to perform a task.
Specificity	If there is a sole supplier of a service, users may feel that they are at more risk from exploitation than situations where there are multiple s uppliers and systems.	It is useful to offer more than 1 system to the user, in order to let him choose a preferred system.
Autonomy	Probably the most important factor in determining user's feelings of risk towards a technology is the degree of autonomy granted to the system	Passive tags are more trusted than acting tags. Systems can learn by monitoring what advice the user accepts or which action he undertakes, and in this way learn by example, which might lead to less risk perception by the user.

6.4.3. Evidence based analysis of acceptance and adoption of RFID technology

Consumer opinions: results of consumer surveys

According to a survey conducted in October 2003 amongst more than 1000 U.S. consumers, the majority of those polled were unfamiliar with RFID (CAP, 2004). Over three-quarter of the sample – 77% - had not heard of RFID. Confirming the general lack of knowledge about this technology, nearly half of the group aware of RFID had 'no opinion' about it.

The unfamiliarity with the concept of RFID extended even to those consumers who might be using it. Many of the survey respondents did not know that the consumer passes they were using did employ RFID technology.

Consumers who did have an opinion about RFID expressed a variety of views about whether or how this technology would affect them. Consumers were asked to rank a number of pre-programmed benefits, like improved security of prescription drugs, faster and more accurate product recalls, improved price accuracy, faster checkout times, reduced out-of-stocks etc.

When asked to rank this set off potential benefits of RFID, 70% identified recovery of stolen goods and improved food and drug safety high on the list. A majority – 66% - also placed cost savings on the top of the list of benefits, although some consumers were also concerned that RFID use would instead raise prices. Consumers placed access to marketing-related benefits, like in-aisle companion product suggestions, at the bottom of the list.

The most significant concerns expressed by consumers familiar with RFID related to privacy. In response to both open-ended and prompted questions (with pre-programmed answers), privacy emerged as a leading concern. Approximately two-third of consumers identified as top concerns the likelihood that RFID would lead to their data being shared with third parties, more targeted marketing, or the tracking of consumers via their product purchases. Main reasons for their position are the fear for increased marketing or government surveillance.

A consumer survey conducted in 2004 by two market research companies revealed similar results (BIGresearch & Artifact, 2004). Of more than 8000 individuals surveyed, fewer than 30% of consumers were aware of RFID technology. Further, nearly two-third of all consumers surveyed expressed concerns about potential privacy abuses. Their primary concerns were on RFID's ability to facilitate the tracking of consumers' shopping habits and the sharing of that information among business and with the government.

The RFID Consumer Buzz survey broke respondents into two categories: 'RFID-aware' and 'RFID non-aware' consumers. Interviewers described how RFID works to the latter group prior to asking them about perceived benefits and concerns associated with the technology.

An interesting observation is that people who were aware of RFID were more practical about balancing the positives and the negatives. Those who were not aware seemed to be surprised to learn about the technology, and they gravitated more toward the potential negative impact of RFID. A conclusion from this observation could be that it is better to inform people about the positive applications than to wait for them to discover the technology on their own.

A study carried out in 2005 by Capgemini (Capgemini, 2005) on what European Consumers think about RFID identification and the implications for business reveals in general the same results. According to this study overall just 18% of European respondents had heard of RFID, with the lowest awareness recorded in the Netherlands and the highest in the UK.

Interesting is that this study concluded that of those who have heard of the technology, perceptions were mixed, with most viewing RFID favourably or having no opinion. Only 8% of European consumers have an unfavourable perception of RFID.

The potential benefits from RFID that are most important to European consumers relate to intrinsic product improvements, such as better anti-theft measures, and improved security, safety and quality.

The possibility of savings to consumers stemming from decreased manufacturers and retailer costs was also deemed important by respondents. Of somewhat lesser importance are supply chain improvements like reduced out-of-stocks. Many consumers said that they would be willing to buy an RFID-enabled product to get the benefits that are most important to them. However, fewer would consider paying more to receive those benefits.

Privacy related issues are the most significant concern about RFID among European consumers. More than half of the respondents expressed concern about the possibility of consumer data being used by third parties, the potential for tracking consumers via their product purchased, an increase in direct marketing, and the possibility that tags could be read at a distance. Health and environmental issues were of somewhat less concern.

During the open European consultation on RFID "Your Voice in Europe" (see chapter 8.11.3), a large majority of responders see security and privacy issues as the main concern. In general one could conclude that consumer perceptions relating to RFID in the European countries were fairly similar to those identified in the U.S. research... Awareness of RFID in the U.S. was also low, but it was a bit higher than in Europe. That is not surprising given the heightened visibility of RFID in the U.S. as a result of the emphasis by the U.S. Department of Defence and large retailers such as Wal-Mart.

The importance assigned to potential benefits was similar in Europe and the U.S., although the order varied slightly. For example, European consumers rated 'Improved anti-theft capabilities" as the most important benefit, followed by 'faster recovery of stolen items". In the U.S., the order was revered.

U.S. consumers expressed somewhat greater concern than Europeans about privacy-related issues, such as the potential use of consumer data by third parties and increased direct marketing. This may be a result of the increased visibility around RFID and activity by consumer advocacy groups in the U.S.

Protection of consumers: guidelines and codes of practices

In order to deal with consumer concerns regarding the use of RFID, various organizations have developed on the basis of self-regulation guidelines and code of practices to protect consumers These guidelines and code of practices also serve as a basis for a further dialogue with consumers and consumer organizations. With the further development of RFID technology also these guidelines and code of practices might need adaptation to new ways of application of RFID.

Self regulation by the suppliers of RFID applications will help to generate trust amongst consumers and users of these applications. By publishing guidelines and code of practices the RFID applications are made transparent to the users. This gives the users the possibility to get insight in the aims and objectives of the data collection and it reveals to the user to which extend these data are used to support these aims and objectives. They also give the user the possibility to complain against misuse of the system.

Self regulation does not come instead of a proper legal system to regulate the use of RFID technology, but it has two advantages:

- It helps to generate trust amongst users, because in the eyes of the users it raises the credibility of the suppliers that the RFID technology will be used in a proper and transparent way.
- It makes it possible to develop a legal framework for RFID application which defines a basic legal regulation without a need to go into to many details, which would lead to a large amount of administrative burden, and which might block further innovation and development of RFID applications.

By comparing different guidelines and code of practices a number of issues come forward which are important for the acceptance of RFID by users i.e.:

- The RFID system and any data stored or processed within it should be used *only for the stated purpose;*
- The organisation operating *the system should be transparent* about the system's purpose, the technologies used, the locations of RFID tags and readers, and who is accountable for the proper use of the system;
- The system should be *protected by appropriate security controls*, and subject to internal and independent audits;
- RFID tags should *not be used to store or process personal information.* Any other data should be erased from the tag before it is released from the organisation's control;
- Where personal data must be associated with the system, that *personal data should be limited to that which is required for operation of the system*, and should be destroyed after use;
- No member of the public should be forced, coerced or tricked into accepting an item with an RFID tag attached. *The public should be able to remove or destroy tags, and provided with instructions on how to do so.*

6.5. Diffusion and adoption of RFID

6.5.1. Introduction

In this chapter we will see how we can apply the theoretical framework on diffusion, and adoption of technology to RFID technology.

One main observation in the model of Rogers is that awareness precedes the decision making process on RFID application and that the next step in the innovation diffusion process is acceptance and implementation of RFID technology (or rejection of the technology).

Several market research studies have revealed a very low awareness amongst consumers on the existence and meaning of RFID. One might expect that the same is true for many producers and suppliers or intermediary organisations in the supply chain. Without a certain level of awareness of the RFID technology the next phases in the innovation diffusion process (decision making, acceptance and implementation) will not take place or at least will be staggered.

So awareness creation amongst all the actors involved will be very important for a well thought decision making process on RFID implementation.

6.5.2. Stages of diffusion and adoption of RFID

The possible stages of diffusion and adoption of RFID in an ideal situation have been described by Loretto (Loretto, 2005).

This description includes both the phases of the innovation diffusion process as described by Rogers, but also the 'perceived usefulness (PU)' and 'perceived ease of use (PEoU)' of the Technology Acceptance Model of Venkatesh et al. In an ideal situation, according to Loretto, the stages of diffusion and adoption of RFID could be described as follows:

- *Stage 1:* At this stage many adopters will be applying RFID technology to their supply chain operation as a result of the requirements of key trading partners. At this stage some supply chain benefits will be realised for inventory, packing, shipping and order fulfilment, but the application of RFID will be seen as cost.
- *Stage 2:* The next stage will involve the increasing integration of RFID mature technologies into existing IT infrastructure in order to recoup investment and realise additional ROI benefits. Integration may then have immediate impacts on asset management efficiencies and order reconciliation performance.
- *Stage 3:* At the moment integration has extended RFID into existing infrastructure, it will be possible to realise further gains in supply chain efficiencies by fundamentally changing the way business is undertaken. This will require business process re-engineering to ensure that people, processes and technologies are aligned to support business objectives.
- *Stage 4:* Fully integrated systems can then be used to rapidly identify business issues and respond to those issues along the supply chain. Being able to do that will enable more effective meeting of consumer needs.

Not many RFID implementations have reached stage 4 yet; many implementations are still in stage 1 or 2.

The main reason for this is that RFID for supply chain applications and certainly for other applications is relatively new and no large-scale implementations have yet been carried out. Products are often not completely faultless and as a consequence it often takes considerable time to install and perfect the RFID hard- and software in each location.

Part of the problem to date is also that the emphasis has been on the advantages for retailers, but not on other companies in the value supply chain. The result is that many companies do not realise the potential benefits of the technology. This is not only true for the retail sector, but it is especially true for application domains in the public sector, like healthcare, public transport, governmental services.

So, RFID is still a complex technology in which little experience has been gained in most organisations. The implementation of RFID has far reaching consequences for organisations and demands fundamental preparation. The preparation time is relatively long at the moment, due to the immature technology and the limited experience with RFID.

There is also sometimes a barrier in the further development of RFID applications by negative opinions among consumers in relation to the RFID technology: privacy issues are one of the main issues here, but also other drawbacks can be stipulated by consumers.

The only way to jump the adoption barrier is through collaboration between all actors involved in the value chain for products or services: this means i.e. the involvement of IT developer, the manufacturer, retailer and consumer right from the beginning of the development of new RFID-applications.

A proven step-by-step implementation of RFID is effective and goes from study or proof of concept, pilots and small–scale projects to large-scale rollout

This process has already started by the innovators and early innovators and it is now time for the early and late majority to take the necessary initiatives to start RFID application developments.

As identified by Rogers, this development will run through different phases of a diffusion of innovation process.

6.5.3. Issues in the RFID adoption in the retail industry: advantages and disadvantages for retailers

RFID technologies has been in existence since the 1950s, but in the present situation adoption of RFID in the retail environment is mainly stimulated by large companies and to a less extend by the inherent benefits of the technology on its own.

Several factors are driving retailers to push for RFID implementation, but one of the significant advantages is the ability to remove inefficiencies from current supply chain management by using real time inventory information. We will give an overview of advantages for retailers and we will also mention some disadvantages for retailers. This information in based on findings in a study on RFID adoption in the retail industry (USA Strategies, Inc. 2005).

These advantages and disadvantages give insight into the 'perceived usefulness (PU)' and 'perceived ease of use (PEoU)' of RFID for retailers (see Table 6-4 for a summary of these advantages and disadvantages). In paragraph 6.5.4 the same overview of advantages and disadvantages is given for consumers.

Table 6-4: Overview of retailer advantages and disadvantages

Retailer advantages	Retailer disadvantages
Real time inventory information	Cost and return on investment
Decreased labour costs	Middleware issues
Prevention of theft, shrink and inventory write off	Consumer feedback
Totally integrated opportunities	

Retailer advantages:

a) *Real time inventory information*

RFID provides retailers with real-time inventory information that can help to prevent stock outs, locate stock within a store to avoid "shrinkage' of inventories, and can help to enable retailers to use more yield effective pricing strategies.

A recent study cited in the Harvard Business Review (Corsten, Daniel and Gruen, 2004) analysed what shoppers do when they face a stock out of a desired product. The results confirmed what many retailers feared. Across the entire retail industry stock outs on average, cost each retailer approximately 4% of sales. Consumers are not patient with stock outs: in fact fewer than half will purchase a replacement item, with almost a third going elsewhere to find the item.

Across the retail industry stock out levels remain near 8%, and represent a key issue that retailers hope to reduce drastically with RFID (Convert, James 2004). One manufacturer currently using RFID technology to help to reduce stock out statistics is Proctor and Gamble. Paul J. Grieger, the director of supply-chain innovation at P&G noted that if the company could reduce stock out levels from 8 to 10% to 2 to 3% of sales, the return on investment in RFID would more than pay for itself.

b) *Decreased labour costs*

RFID provides technology that practically eliminates the need for human checking of stock. Accenture estimates that effective RFID solutions can help retailers reduce a wide array of costs: receiving by 50 to 65%, stocking by 22 to 30%, checkout by 22 to 30%, cycle counting by 40 to 60% and physical counting by 90 to 100%. (Chappell, Garvin et al 2003).

c) *Prevention of theft, shrink and inventory write off*

"Shrink" is a retailing term used to describe inaccurate inventory counts as a result of customer theft, employee theft, inaccurate inventory counts due to misplaced items, and stock reordered because items are on a display shelf in another area of the store. The 2000 Retail Survey Report estimates that shrink represents 1, 69% of sales for retailers (University of Florida, 2000).

RFID technology has the potential to alert staff when items are being removed illegally, or when they have been misplaced within the store.

This can assist in theft reduction and also provide real-time accurate inventory counts automatically.

Inventory write-offs occur when goods are no longer fit for consumption, the goods are no longer in demand by consumers, or they have been damaged while in the retailer's possession. RFID technology offers solutions to track sell-by-dates of each product on the shelf.

The collection and utilization of this information will help retailers maintain a better inventory management system that can react to demand much more quickly than current systems

d) Totally integrated opportunities

In addition to improving the supply chain, *the advent of RFID technologies will offer retailers new and unlimited marketing opportunities*. Tracking a customers' purchases before they leave the store offers retailers information that can immediately be used for the cross selling of other related products. In-store suggestive selling allows retailers to communicate with shoppers while they are shopping in an effort to encourage them to buy an additional and/or complimentary item.

The implementation of RFID technology will offer retailers also the ability to change their pricing moment by moment. Real time inventory can allow for automatic price changes to maximize their yield on high-in-demand items. Yielding maximum prices for items according to store supply and demand levels will increase incidental sales for all retailers.

There are also some disadvantages for RFID adoption for retailers.

Retailer Disadvantages

a) Cost and return on investment

The introduction of RFID will lead to addition costs, while the anticipated ROI time frame is unclear, because the true cost savings are difficult to predict and the only visible benefit in the beginning of an implementation project is that the culmination of sales and inventory information can prepare retailers better to avoid stock outs and shrinkage. *It is not the cost of hardware to read RFID sensor chips that is worrying the retail industry; it is the integration of existing software with RFID information which will cost much more money.*

b) Middleware issues

RFID middleware extracts the data from RFID readers, filters it, aggregates the information, and routes the data to enterprise systems. After distilling the data, the middleware passes it along to applications like enterprise resource planning (ERP), supply chain execution (SCE), customer relationship management (CRM) and warehouse management (WM) systems. Other potential functions include monitoring and managing the RFID reader network. *Many retailers have cited issues with data quality, control and device monitoring and management problems as obstacles to the implementation of RFID middleware (Liar 2004).*

c) Consumer feedback

Metro AG's pioneering Future Store is the first entire operation to fully utilize RFID technology. The Boston Consulting Group published a report on the working of the Future Store, which showed increased customer satisfaction (The Boston Consulting Group, 2003). The share of customers that chose either fully or highly satisfied rose from 34% to 52% after the store changed from a traditional retailer to the 'Future Store' model. However not all customers are convinced. The same study showed that although 42% of customers are using the store more frequently a 20% of customers surveyed are using the store less frequently. *Not all customers will happily utilize the RFID related technologies available to them.*

6.5.4. Issues in the RFID adoption in the retail industry: advantages and disadvantages for consumers

In general, consumers in retail shops are relatively oblivious to RFID technology and capabilities. However, there are a number of consumer protection groups that are operating websites and blogs aimed at galvanizing support for legislation limiting RFID and what companies can do with the technology. To get a better insight into issues related to consumer adoption of RFID we will give an overview of consumer benefits and consumer drawbacks (see for a summary *Table 6-5*).

Table 6-5: Overview consumer benefits and drawbacks

Consumer benefits	Consumer drawbacks
Consumer savings	Hidden placement of tags
Improved security/ authenticity of prescription drugs	Unique identifiers for all objects worldwide
Efficient recalls will reduce deaths and injuries	Massive data aggregation
	Hidden readers
	Individual tagging and profiling

Consumer benefits

a) Consumer savings

RFID will allow companies to better match up supply and demand. Manufacturers will not produce vast quantities of products that will not sell and retailers will not overstock excessive amounts of products destined to sit on store shelves gathering dust. RFID will enable companies to more quickly identify goods that can or need to be discarded or replenished. This in turn will give the customer access to better and fresher products and in the long term might also lead to a decrease in pricing for the consumer

b) Improved security/authenticity of prescription drugs

RFID will be used to distinguish genuine products from counterfeit products. This is especially important for healthcare applications and medicine prescriptions. Currently, consumers have i.e. no 'fool-proof' method available which allows them to vetting their drug prescriptions, which could lead to potential health issues associated with ingesting counterfeit drugs (with i.e. wrong doses or ingredients).

c) Efficient recalls will reduce deaths and injuries

RFID can be used to identify and recall outdated products or unsafe projects. This is especially import in the food area, because it will improve food safety and enhance consumer safety.

Consumer drawbacks

a) Hidden placement of tags

RFID tags can be hidden in objects and documents without the knowledge of the individuals who purchase the items. As radio waves travel easily and silently through fabric, plastic, and other material, it is possible to read RFID tags sewn into clothing or affixed to objects contained in purses, shopping bags, suitcases etc. Not knowing if reading of RFID tags is possible or takes place is very annoying for people.

b) Unique identifiers for all objects worldwide

The Electronic Product Code (EPC) potentially enables every object on the planet to have its own unique identification code. This technology could lead to the creation of a global item registration system in which every physical object is identified and linked to its purchaser or owner at the point of sale of transfer.

This is potentially a positive aspect in some respects for the consumer, but in terms of privacy issues, it could lead to serious abuses.

c) Massive data aggregation

RFID technology requires the creation of massive databases containing unique tag data. These records could be linked with personal identifying data. The main concern here from a consumer perspective is privacy and a threat of misuse of the data.

d) Hidden readers

Readers could be placed (out of sight) into nearly any environment where consumers or products are located. RFID readers have already been experimentally embedded into floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into retail shelving and counters, making it virtually impossible for consumers to know when or if he or she is being 'scanned". Without further regulation, there is the potential threat for any number of abuses.

e) Individual tracking and profiling

If personal identity were linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent. For example, a tag embedded in a shoe could serve as an identifier for the person wearing it.

For these reasons consumer organisations both in the USA and Europe have expressed their feelings of distrust around the introduction of RFID and have asked for solutions or proposed solutions themselves. (Privacy Rights Clearinghouse, 2003; The European Consumers' Organisation).

6.5.5. Drivers and rationale in RFID adoption

Even with extensive writings on adoption and diffusion of innovations (Rogers, 1983) the adoption of new and emerging technologies with unique characteristics is still not well understood.

It is not uncommon that new technologies, as they pervade the social fabric, generate misunderstanding, mistrust, hostility or irrational fear. History is full of people and groups that fought against the introduction of new techniques or their consequences.

Today RFID technology lies at the centre of social debate because of its perceived effects on data protection and privacy, on health and safety, or also on employment and labour practices. This debate reaches a climax because RFID has left the lab and is fast entering the mainstream of business and society.

Business adoption of RFID is relatively new and therefore as with most new information technologies its true potential both independent and in conjunction with other technologies is not yet fully understood.

6.5.6. The broad landscape of RFID applications

In the previous sections we went into detail in the application of RFID in the retail sector, because a lot of knowledge concerning user acceptance and adoption has been gained in this sector. In the meantime the landscape of RFID-applications has been enlarged and we see now a rapid penetration of RFID in various other domains, both in the public sector and the private sector.

The largest number of case studies in the IDTechEx database is on pallet/case tracking and these case studies are mainly related to the retail sector. But recently also a number of item-level tagging case studies have been included in the database and they equal now the number of pallet/case studies. Especially in the item-level tagging we see many new application areas. Roughly equal to these two categories is the number of card categories, payment key fob and e-passport case studies. It is expected that a lot of new case studies on card systems will be included into the database in the near future as case studies in financial, access and other cards will be added since the world's credit, debit, account and identification cards gradually move over to RFID for convenience, reliability and reduced cost of ownership by the issuer/operator (see also Annex 8 which presents an overview of EU-US cases in categories that the IDTechEx database deals with).

Next in order is the vehicle tagging area, which is lucrative not only because of the high prices of the tags, but also the high prices of the systems.

Based on a further analysis of the IDTechEx database we can identify the following RFID-application sectors (presented in order of number of case studies in the database):

- Pallet/case
- Item Level
- Card (incl. key fob)
- Vehicle
- Ticket
- Conveyance
- Intermodal container/ULD
- Passport
- Clicker/immobiliser
- Air baggage
- People
- Animals

While the prices of the tags for pallet/chase applications can be rather low, the unit prices in general are somewhat higher. This is especially the case for applications in the medical sector, the aircraft sector and the library sector, because in these sectors a superlative performance of the tags is required. Also the prices of RFID-applications in cards and passports are high, which makes these applications very profitable for suppliers. The same is true for RFID-applications in vehicle tracking.

New applications are also seen in the textile industry, where RFID is used to raise the efficiency in textile production and distribution, but also for managing the quality control of the goods from raw material to end products.

An important new area for RFID applications is healthcare. IDTechEx predicts that the market for RFID in healthcare will grow from $ 90 million in 2006 to $2.1 billion in 2016. One of the application areas here is the authentication of drugs. By establishing a kind of electronic pedigree of every drug, it will be possible to follow the medicine through the whole distribution chain in order to authenticate the medicine at the point of dispensing. Of course the usage of medicines is highly sensitive personal information. Therefore it has to be guaranteed that the pharmaceutical industry doesn't collect any personally identifiable information of the patient during this process. So it is clear that several privacy and data protection issues are related to the RFID application in drug distribution.

At the level of the patient RFID-applications can help to record which medication was taken and in what quantity and in this way lower the percentage of errors in medicine intake. The benefits sought here are better patient compliance of drug taking. Especially with an increase of older people in our society this is an important application.

Table 6-6 shows that the larger application of RFID might generate a number of socio-economic benefits. It is obvious that the price–development of the tags is only one factor in the adoption and broad application of RFID. The development of some potential markets might be not as price-sensitive as often is believed, because of the social benefits which (also) might be realised.

Table 6-6: Potential benefits of RFID applications in various application areas[58]

	POTENTIAL BENEFITS					
APPLICATION AREA	Cost Reduction	Increased Sales	Crime Reduction	Better Service	Safety	Removal of Tedious Procedures
Laundry/Rented Textile	X			X		X
Library Books, DVD's etc.	X		X	X		X
Parts for aircraft & Other Machinery	X		X	X	X	X
Blood Bags & Samples	X			X	X	X
Military	X		X	X	X	X
Book Retail	X	X	X	X		X
Drugs Prescription	X	X	X	X	X	X
Cigarettes	X	X	X	X	X	X
Postal	X		X	X	X	X
Other Consumer Packaged Goods (CPG)	X	X	X	X	X	X

[58] Adopted from: IDTechEx, RFID in action, 2006.

6.5.7. RFID and the new consumer or the new citizen

RFID can help to reduce the inefficiencies in supply chains. This is a main advantage of RFID for suppliers of products and services. Especially in a situation where competition is growing and suppliers are forced continuously to lower profit margins.

On the other hand, there are also very significant social and market changes that directly affect consumer behaviours (we do not see a difference in the behaviour of consumers or citizens in this respect, so if we use the term ´consumer´ we also mean ´citizen´?. Socio-demographic changes such as increased number of dual-income, single-parent and technology-familiar households have significantly altered the consumer behaviour (Kim, 2002).

A core component in strategies to reach the new consumer is the development of attractive consumer experiences. The reason for this is that traditional factors of competition, such as price level, selection and location, although still important, are no longer sufficient to achieve competitive differentiation. This is because the shopping experience of the new consumer is also affected by a number of store-related factors, such as ambience (temperature, scent, music etc), service quality in the store, store perceived image and situational elements such as crowding, time and budget availability of the consumer.

This means that a shopping experience has to be driven to a maximum of efficiency and at the same time also towards a maximum of pleasure and entertainment.

The new consumer is more knowledgeable about comparable product costs and prices; more changeable in retail and brand preferences, showing little loyalty, self-sufficient, yet demanding more information. The new consumer holds high expectations of service and personal attention; and is driven by three new currencies: time, value and information

How can RFID in this context help to meet the demands of the new consumer? RFID makes it possible to use personal data associated with individual consumers. These data can be used to reconstruct their private activities at an unprecedented level of detail. Based on these data a more personal approach is possible, both for retailers but also for all kind of public services. This may cause fundamental transformations to the way consumers and citizens will be served in the near future.

6.5.8. Conclusions

A main issue in the debate around the adoption and diffusion of RFID is the privacy debate (see also chapter 8 on this aspect). This issue has yet to be concluded and needs to be taken seriously by the RFID industry and other actors involved, because if no adequate solutions are found for this issue, this could have a negative impact on the rate of implementation of RFID in society.

By focusing on the privacy debate one might however forget that also other social-economic, legal and ethical issues are involved in the adoption and diffusion of RFID. Privacy is mainly an issue which is related to consumer acceptance or lack thereof. However diffusion of innovation involves all actors in the value chain, not only the consumers, but also the suppliers and intermediary organisations.

Another main issue in all technology acceptance models is the balance between the ‘perceived usefulness (PU)’ and ‘perceived ease of use (PEoU)’. These two factors are main determinants for the acceptance and use of new technology.

In this chapter we have refrained on discussions on privacy issues (these are discussed in detail within chapter 8 of this report) but we have discussed some of these other socio-economic, legal and ethical issues we referred to. We have illustrated these issues by applying the diffusion of innovation theories to RFID in various markets.

Despite first appearing in tracking and access applications in the 1980s, the potential of RFID has only been recognised relatively recently. Using RFID tags, it is possible to identify and track objects and people without time delays, without human intervention and thus without variable costs. With even smaller, smarter and cheaper tags and readers, RFID is opening up amazing value chain possibilities. Through RFID technology companies can improve efficiency and visibility, cut costs, better utilise their assets, produce higher quality goods, reduce shrinkage or counterfeiting and increase sales by reducing out-of-stocks. And both in the private sector and the public sector RFID can gain also a number of social benefits, which makes these applications depend less on the price-elasticity of the RFID-tags.

All this, means that RFID will have a great impact on the processes and IT systems of companies and public and societal organisations.

However, it is expected that the use of RFID in the commercial sector will only take place if the financial benefits (on short or medium term) are greater than the cost of implementation.

Another observation is that for supply chain applications and certainly for other applications RFID is relatively new and no large-scale implementations have yet been carried out. Products are often not completely faultless and as a consequence it often takes considerable time to install and perfect the RFID hard- and software in each location.

All this means that it is necessary that companies and organisations that want to introduce RFID in there own environment thoroughly prepare themselves.

Part of the problem to date is also that the emphasis has been on the advantages for retailers, but not on other companies or organisations in the value chain. The result is that many organisations still do not realise the potential benefits of the technology.

So, RFID is still a complex technology in which little experience has been gained in most organisations. The implementation of RFID has far reaching consequences for organisations and demands fundamental preparation. The preparation time is relatively long at the moment, due to the immature technology and the limited experience with RFID. Therefore collaboration between manufacturers of RFID systems and IT developers in companies and organisations is necessary.

Also the users should be involved in this development. There is a risk of misconception about RFID technology among users and consumers. Privacy issues are one of the main issues here, but also other drawbacks can be stipulated by users.

As part of their RFID strategy, manufacturers and organisations which apply RFID-applications need to develop a privacy policy and communicate this to their users.

Educating all actors involved in the value chain will also be very important. This process of education is partly occurring in a natural way as a collaborative approach is allowing organisations and users to get involved in the development of RFID applications. There also needs to be a level of education to promote RFID outside its traditional stronghold or consumer retail products. This is especially important because the characteristics of specific application areas in our society, i.e. in traffic, travel, health, defence etc., create a need of specific measures to guarantee authenticity, privacy and safety in order to create trust and acceptance of these applications by the potential users.

A proven step-by-step implementation of RFID is effective and goes from study or proof of concept, pilots and small-scale projects to large-scale rollout.

6.6. RFID: Employment, training and education

6.6.1. Impact of RFID technology on the workplace and the employment market

Employment: job loss versus job creation

With the advent of RFID technology and its promise of long-term efficiency gains, several studies have been conducted to investigate the impact of RFID applications on society, to explore possible issues for public policy (OECD, 2005; Telematics Institute, 2006). These reports have a strong focus on technical aspects that might hinder the adoption of RFID such as standardization, interoperability and data security. The social aspects, on the other hand, often remain limited to privacy concerns, which dominate the discussion of social (user) acceptance. When economic aspects are included in the analyses, the emphasis is on the endless possibilities to apply RFID technology, the productivity gains that can be obtained, and the presentation of bright, future market prospects.

At the other side of this development, however, you'll find the automation process, reinforced by RFID, and inevitably leading to a reduction of labour costs. Administrative staff and jobs that involve bar code scanning such as cashiers in supermarkets or jobs in distribution centres, run the risk of becoming obsolete. A report from the US Yankee Group, published in 2004, forecasted that efficiency advantages of RFID will cost 4 million employees their jobs (Yankee Group, 2004).

The lack of attention for the impact of RFID on employment in these reports is in this respect remarkable. One could argue that this lack of attention is a reflection of the current state of development of RFID, where the focus is mainly on overcoming technological hurdles. On the other hand, as the public spotlight is on privacy concerns, other issues, such as job loss, remain underexposed. According to a UK report on RFID applications in healthcare the public's attention is mainly focused on privacy violations but job losses are a far more likely and dramatic outcome of RFID adoption.(Wireless Healthcare, 2004).

However, this view is disputable for the following reasons. Firstly, the loss of jobs is expected to be a gradual development coupled to a long transition period of at least 10 years from bar code scanning towards RFID applications (Yankee Group, 2004). Due to this long period the loss of jobs is not expected to result in a disruption of the labour market.

Secondly, there are indications that the rollout of RFID will create new jobs as well. Several analysts predict a transition towards more added-value positions such as information (data processing) and service related jobs. The RFID applications will give companies access to large amounts of data that have to be processed to generate actual, value-adding knowledge.

Thirdly, RFID could create new jobs in an indirect way, as RFID is likely to increase productivity gains across a wide range of industry sectors. This will spur economic growth, which in turn will create more jobs (IBM, 2005; Reeding, 2006). This line of thought emphasizes innovation and the development of new service products that RFID will create.

The impact of RFID on employment shows, in this respect, similarities with the impact of Information Technology (IT) on employment. Although the adoption of IT has led to job displacement in particular sectors of the industry, employment in the services sector has increased (OECD, 2004; 2005). At the same time, IT has become an essential element for economic growth which has created jobs indirectly (OECD, 2004; 2005).

However, the full benefits of IT can only be realized by improving skills of employees, by training management, by implementing organizational innovations and integrating IT in company strategies (OECD, 2004; 2005). This holds as well for RFID. One of the key challenges to fully realize the success of RFID will be education and training. This will be the focus of the following chapter.

Workplace

The WSM ('Work Standards Model', developed by The International RFID Business Association – RFIDba[59] - to assist organizations in quantifying and assessing their required workplace skills and knowledge to successfully implement RFID) gives a hint of the significant impact the implementation of RFID in business processes will have on the workplace. Employees (end-users) will need new skills to successfully work with the implemented systems. The emphasis will be, even more than before, on [real-time] processing of information that is collected from different sources, tools, and applications. This will transform the character of the new information workplace beyond that of traditional knowledge work (Forrester, 2005).

However, the actual number of studies conducted on the impact of RFID on the workplace is very limited. The few reports that have been published on this matter focus on privacy issues (RAND, 2005; NVVIR, 2005). Although employers have already many options available to them to control and monitor employee presence, the application of RFID in access and tracking systems

[59] RFIDba is a global, not-for profit, vendor-neutral, educational trade association focused on serving end-users who have a need for educational programs that will help them achieve successful implementation and deployment of RFID technologies. The Association is developing internationally accepted standards for RFID education, training, and certification based on the RFIDba WSM

will make data collection and processing on a large scale even easier. It will create new ways to monitor employee location, behaviour, and performance.

Current applications are often limited to access control systems (NVVIR, 2005). The expectation is however that RFID will be widely applied in organizations. This can have considerable consequences for employee privacy. In 2006, two workers of the US company Citywatcher were implanted with a RFID chip (MSNBC, 2006). Another example is a store of McDonalds (US) where employees are checked whether they have washed their hands after using the toilets, which was made possible by the application of RFID technology.

Whilst in these examples clients or employees have chosen themselves for the RFID chip implant, many employees are unaware of the possibilities of RFID applications and the consequences for their privacy. The ease of automatic data collection and the fact that RFID can function without direct contact between tag and reader increases the possibilities for illegal collection of data (NVVIR, 2005). Open and transparent guidelines (regulations) and open information practices are very important in the implementation of applications aimed at surveillance, control and monitoring, to guarantee employees' privacy.

6.6.2. Training requirements and training facilities in relation to the widespread adoption of RFID technologies

Skills: shortage, gap or mismatch?

A widely recognized problem is the shortage of RFID skills. A survey conducted in February 2006 by the Computer Technology Industry Association (CompTIA),[60] to gain a deeper understanding of the current RFID skills in industry, found that 75% of the respondents believe that the pool of talent in RFID is insufficient. From this 75%, 80% believes that the lack of skilled individuals in RFID will hinder adoption. This number is significantly higher than in 2005, when 53% said it would have a negative impact (CompTIA, 2006).

Using the definition of the European e-skills Forum, an analysis can be made of the kind of shortage that is currently observed for RFID. The Forum distinguishes between three types of shortages (European e-skills Forum, 2004):

- Shortage: quantitative lack of skilled personnel;
- Gap: A competence shortfall between current and needed competence levels;
- Mismatch: A difference between the competence of the trainee or graduate and employers' expected competence needs.

The results of the survey did not only show a quantitative lack of skilled RFID workers (there are not enough people that can perform RFID jobs); it also found that current RFID workers do not have the required competences. This implies that the shortage of skills is also a qualitative gap between what competences RFID workers currently have and what employers actually need. There is some debate on whether this gap is of a structural nature (that might require policy interventions). Some hold that the gap will dissolve quickly with the rollout of RFID, as the number of organizations offering special training programmes is growing significantly.

Before turning to what types of competences are required, it should be noted that the current focus of the shortage of skills is on RFID professionals, rather than end-users of RFID applications. The demand for skilled end-users is likely to become more important in the (near) future, when applications are implemented on a large scale.

Two types of skills in particular were identified as critical to the successful implementation of RFID applications: radio technology skills and software/business process/data architecture skills (CompTIA, 2006). Radio technology requires a combination of knowledge of the frequency spectrum of radio waves with RFID knowledge (such as RFID standards, air protocols, data coding, electronic product code formats, installation, maintenance and testing skills). The second type of skills requires knowledge of middleware, the functionality of software (real-time data acquisition and data filtering), integration of specific applications etc.

[60] CompTIA is an international organization with the aim to advance the growth of IT industry and those working in it. They have 20.000 members in 102 countries and offer vendor neutral certification programmes on several subjects, such as RFID (since March 2006). http://www.comptia.org

Training

In order to address the skills gap, several organizations have developed their own RFID certification programmes to train staff and overcome the differences in competences. As a result of their survey and discussions with industry experts, CompTIA started their RFID certification programme in March 2006. It is focused on radio technology and includes the following domains:

- Interrogation Zone Basics
- Testing and Troubleshooting
- Standards and Regulations
- Tag Knowledge
- Design Selection
- Installation
- Site Analysis (i.e. Before, during and after installation)
- Radio Frequency Physics
- RFID Peripherals

Training courses of other organizations such as RFID4U, RFIDSolutions and OTA Training are approved by the CompTIA Learning Alliance (CLA).

The International RFID Business Association (RFIDba)[61] has developed a 'Work Standards Model' (WSM) to assist organizations in quantifying and assessing their required workplace skills and knowledge to successfully implement RFID. The model describes all work processes, tasks and task elements, tools and equipment as well as the knowledge, skills and abilities of the workers to quantify and codify the work.. It can be used to understand how work processes, tools or knowledge might be changed due to the introduction of RFID and to identify the required level of expertise of different employees (Squires & Neary, 2006). This model, therefore, focuses mainly on end-users of RFID.

6.7. Conclusions and recommendations

The widespread application of RFID not only raises privacy and security concerns, but also far reaching implications of the application of this technology can be foreseen in the social interaction between people and in the economic transactions between actors in the market.

In this chapter the socio-economic aspects of RFID applications have been discussed, together with some legal and ethical issues. This subject also includes the human aspects related to the use and acceptance of the RFID, i.e. awareness, trust and user related issues of technology transfer.

Based on a theoretical framework it is made clear that these socio-economic aspects are important for the widespread acceptance and use of RFID Therefore technology developers and policy makers should be aware of these aspects and take appropriate measures to incorporate accepted social values in the development, application and implementation of the RFID technology.

Having said this, an important observation is that results on socio-economic research on acceptance, adoption and use of RFID are still rather scarce.

The same is true for the second topic in this chapter: the effects of RFID on the workplace and the employment market and the development of education and training in relation to RFID.

In relation to the issue of education and training one could also mention the issue of awareness, which is still lacking. As a result of consumer surveys one could conclude that RFID is still a rather unknown concept amongst consumers: only 30% of the consumers in the USA, and only 18% of the consumers in Europe are aware of the existence and application of RFID, the rest has never heard of the concept before.

This means that for consumers even the first phase of the process of diffusion of innovations, as defined by Rogers, hasn't started yet.

In this chapter we do not restrict ourselves to the analysis of consumer aspects, but we look at

[61] RFIDba is a global, not-for profit, vendor-neutral, educational trade association focused on serving end-users who have a need for educational programs that will help them achieve successful implementation and deployment of RFID technologies. The Association is developing internationally accepted standards for RFID education, training, and certification based on the RFIDba WSM.

the introduction of RFID in the whole value chain, so including manufacturers and suppliers, retailers and other intermediary organizations, and users/consumers in various sectors in our society..

Taking the retail sector as an example we have started to analyze which factors influence the acceptance and implementation of RFID and which advantages and disadvantages of RFID can be identified.

Conclusion is that for many different reasons, many companies are still in the first phases of adoption and implementation of RFID. This is even more the case in various other sectors of our society. One of the reasons is that RFID is a complex technology, in which still little experience is gained in most organizations. Further pilots and experiments around RFID implementation, with involvement of all main partners (so also the users) will overcome a lot of problems and will stimulate the learning and acceptance process. Main drivers for this development are perceived benefits, the existence of dominant supply chain pressure, and the existence and adoption of standards for intellectual property ad ownership of the data generated by the RFID systems.

In relation to the introduction of RFID not only technological and cognitive knowledge is important, but also the affective quality of the whole RFID system should be taken into consideration. Perceived affective quality of a system for instance has a positive impact on user's perceived usability of the system.

The same is true for pre-existing knowledge on the system. People who know already what RFID is are in general more positive on the effects of RFID than people who just learned about the existence of RFID. This observation also pleads for an extension of awareness activities both for the consumers and the other actors in the supply chain or value chain.

A main conclusion regarding the theoretical analysis of the issue of trust and RFID is that the basic level of trust is different for different people. Some people are very trustful, while others have a high basis level of distrust.

Another observation is that feelings of trust and risk can be established quite independently, and together they determine the final success of introduction and acceptance of RFID. Trust contributes to the acceptance of the technology in a positive direction; while risk contributes in a negative direction. The effect is that the two factors interact with each other, so that technology connected with a low degree of trust may still be successful if there is also a low perceived risk. But it is also possible that in very risky situations no amount of trust is able to offset the risk perceived by a user, and in such a situation it will become very difficult to accept the involvement of a specific technology.

In order to deal with consumer concerns regarding the use of RFID, various organizations have developed on the basis of self-regulation guidelines and code of practices to protect consumers A number of such guidelines and code of practices have been selected and are described in this report (see Annex 4).

It is also very important to note that:

Development of awareness activities is very important to make consumers, but also other actors in supply chains for products or services, aware of the existence, benefits and existing drawbacks regarding the widespread introduction and implementation of RFID. It is important to realise these awareness activities from a neutral point of view. Therefore the EC could initiate or stimulate these developments.

Pilot activities and experiments are important initiatives to learn to overcome all the pitfalls which might arise when a company or a public organisation start to implement RFID. It is important to develop such initiatives along the lines of proven step-by-step introduction of RFID: from study or proof of concept, pilots, and small-scale projects to large-scale roll outs.

It is also important to involve all relevant parties in the development and implementation process: so also potential users/consumers should be involved from the very beginning of such an initiative. The development of such a pilot projects and experiment is a main responsibility of the market itself. However, in order to disseminate the knowledge gained and the experience which has been built up, it might be helpful if the EC could give some support to these activities.

A lot of research is going on regarding the further development of hard- and software for RFID. However, most of this research is technology based and takes cognitive behaviour of the consumer as a point of departure. Emotional aspects also to a large extend influence the acceptance or rejection of the RFID technology. Therefore researchers should also analyse the affective quality and affective aspects of RFID systems into their research projects. In general we could conclude that the methodology for such research is still underdeveloped. We could not identify any specific study on these aspects in relation to RFID systems. We recommend that the EC supports such studies and stimulates the widespread application of the results of these studies.

The positive and negative implications of the widespread implementation of RFID on employment and overall work force are still unknown. The development of a conceptual model to analyses this impact and the further monitoring of these developments could be considered as an important task for the EC. Also issues related to the renovation of the work place due to the implementation of RFID need further attention.

RFID is only a part of the introduction of new information and communication technology in the retail sector and in other commercial or public sectors. It is a part of the introduction of ubiquitous computing and ambient intelligence in companies, shops and homes. This new technology will have an impact on the consumer, but at the same time, due to all kind of socio-economic developments in society, we also see the emergence of the new consumer. This new consumer will also develop – in a direct or indirect way - new demands regarding the use of new technology.

A further analysis of the role of the new consumer in relation to the development of new technology will be fruitful for the further development of the RFID systems, but also for other technology systems which have to serve the consumer or citizen of the future.

7. Privacy aspects of RFID

7.1. Introduction

The objective of this chapter is to position the various privacy consequences of RFID in a general framework that underscores the relationship of RFID with privacy on three distinct levels. To start with, we will present some results and observations that show the importance of dealing adequately with privacy in case of using RFID. This sets the scene. The by now 'classical' view on privacy will be presented, followed by an extension of this view for RFID. A distinction we introduce, is the distinction between closed and open RFID systems, i.e. systems in which data are confined within the system and systems that communicate with other systems and that exchange (personal) data. Dealing with the privacy implications of RFID can be done on the basis of one of the three following perspective: enforcement by law, self-regulation and technical measures. Referring to the first, the EU-privacy directive (95/46/EC) sets the scene and is overall still valid. Self-regulation is a means that enforces commitment by interested parties. The US Centre for Democracy and Technology has organised commitment in a set of RFID-privacy guidelines. Finally, technical measures can be used to enhance privacy. For consumer issues it is demonstrated that it is possible to adhere to the OECD Fair Information Principles by including specific forms of profiling and use specification to the tag and reader information. This elaboration shows the viability of a 'privacy by design' approach.

7.2. The sensitivity of RFID towards privacy infringements

In a recent OECD report, privacy is indicated as an important aspect of RFID-developments. The OECD states that "[W]ithout addressing privacy related issues carefully, appropriately and transparently … backlash by consumers and citizens is a potential risk that could limit long-term benefits and development." (OECD 2006a, p. 15) In the view of the OECD, privacy is an asset of RFID that needs to be taken on board, and that requires careful consideration. The OECD mentions a study done by the EU Article 29 Working Party on Data Protection, a group that has been established in accordance with article 29 of the European privacy directive 95/46/EC. (Article 29, 2005a) This study supports the findings of the OECD with regard to the privacy implications of RFID. The OECD and the Article 29 Working Party share the view that in relation to RFID, privacy and security are two sides of the same coin and require an approach in which they are both tackled together. During an OECD-workshop, held in October 2005, participants also addressed the double-sidedness of privacy and security, complementing that it might be possible to include security safeguards that may have positive implications on privacy. (OECD 2006b) The Italian member of the Data Protection Commission, Stephania Congia, stated that "the majority of basic principles are already laid down in the OECD guidelines, EU directives, the Council of Europe Convention, but that RFID technology has an impact on personal dignity and integrity as well as on freedom of movement and that personal data can be processed without the knowledge of the individual."(OECD 2006b, p. 14) The EU-workshop on RFID, held early May 2006, once more proved the importance of tackling privacy and security as two dominant aspects for successful introduction of RFID. Much of the workshop, devoted to privacy, security, health effects and employment was dedicated to underscoring how privacy and security might profit from each other in improving user acceptance of RFID. The double-sidedness of privacy and security requires attention right away, since it deals with embedding privacy regulations in the standards that are developed just now on the various aspects of the RFID system (encompassing tags, readers, middleware and the adjacent back-end information systems).

A recent study, performed by Capgemini (2005) supports the concerns that are raised by the OECD and the Article 29 Working Party. Capgemini concludes that overall awareness for RFID in Europe is low, and on average lower than in the United States (18% in Europe versus 23% in the

USA). Within Europe, awareness is highest in the UK (24%) and lowest in the Netherlands (12%). Though US consumers expressed greater concern for privacy related issues than European consumers, Europeans did put privacy issues "at the top of the list, leaving no doubt that companies must address these concerns as they communicate with their customers about the technology."[62] Overall, the higher the awareness, the higher the response to expected privacy concerns of RFID.

This indeed is an important message. The more one becomes familiar with the opportunities RFID technology offers, the higher the critical awareness that the technology may impose privacy threats. For Europeans, the highest ranked privacy threats are consumer data used by third party, tags that can be read from a distance, tracking of consumers via product purchases, and being targeted more with direct marketing (see *Table 7-1*).

Table 7-1: Consumer concerns related to RFID[63]

Issues of concern	EU [%]	USA [%]
Consumer data used by third party	59	69
Tracking of consumers via product purchases	55	65
Tags could be read from a distance	52	42
Targeted more with direct marketing	52	67
Environmental impact	44	45
Health issues stemming from RFID	35	56
RFID tags that can be eaten/dissolved	31	43

The table shows priorities in the USA to be different from the priorities in the EU, with privacy concerns in the USA overall higher. The biggest gap between the USA and Europe is in prioritising health issues (dangers from RFID radiation), where the USA prioritises these issues considerably higher than Europeans.

In a study, performed at the Humboldt University of Berlin, people were invited to indicate what they perceived as potential major privacy risks of RFID.(Spiekermann 2006) They identified the following list of threats:

1. Unauthorised access
2. Tracking of objects via data
3. Retrieving social networks
4. Technology paternalism
5. Making people responsible for objects.

The first two of these threats are related to the direct use of RFID: they relate to violation of confidentiality and security of communication and the direct use of data to monitor people, and are in line with the first four threats identified by Cap Gemini. The third threat is related to profiling specific groups on the basis of shared characteristics which make people part of social networks. The privacy threat here is, for one, the intrusion in the intimacy of the personal sphere, and for another the identification of people belonging to a network on the basis of shared characteristics (profiling), which may lead to inappropriate assumptions about individual persons. Technology paternalism relates to the enforcing power of RFID to control behaviour of persons. Examples provided are the smart shelves that raise alarm when objects are replaced wrongly, and cinema's that signal when people bring with them their own (RFID-tagged) food and drinks. The fifth issue refers to the use of RFID in linking objects to people, for instance in order to register deviant behaviour. An example is that objects can be linked to people (a can bought at a supermarket and thrown out of the car after consumption).

The Capgemini survey presented an other interesting result. Table 7-2 compares the perceived impact on privacy of RFID relative to other technologies, such as mobile phone, credit cards, smart cards, etc. Though some of the technologies

[62] CapGemini (2005). p. 4

[63] Percentage of consumers saying "concerned" or "extremely concerned. Capgemini (2005), p. 11

may have RFID embedded in them (for instance access control badges and smart cards) the technologies are rated as if they are independent from each other. RFID is rated to have a higher or equal privacy impact for all technologies that were presented. 45 and 46% respectively rated the privacy impact of RFID higher than the privacy impact of access control badges and smart cards. It is interesting to note that in all cases only 10% of consumers or less considered the privacy impact of RFID to be less than the privacy impact of the already existing technologies! This implies that RFID is considered to be a technology with a very high privacy profile.

Table 7-2: The impact on privacy from RFID vs other technologies – Europe[64]

Consumers saying RFID has …	Greater impact	Same impact	Lesser impact	Don't know
Mobile phones	36	33	10	21
Debit cards	36	29	7	26
Credit cards	41	31	8	20
ATMs	41	32	8	19
Frequent shopper/loyalty cards	42	33	7	18
Access control badges	45	31	6	18
Smart cards	46	28	6	20
Camera phones	34	32	10	24

The survey of Capgemini thus underscores the statements of the OECD and the Article 29 Working Party that privacy implications of RFID have to be taken seriously. The survey indicates that the consumer does not expect the introduction of RFID to lead to cost reductions. The consumer does however perceive potential benefits of the technology such as car anti-theft measures, faster recovery of stolen items, improved security of prescribed drugs, improved food safety and quality, and potential consumer benefits (such as faster check-out, better price accuracy, improved access to products and information). These potential consumer benefits are ranked low on the list, which is in combination with the high profile for privacy related issues, reason to start raising awareness of the consumer on benefits and potential dangers of widespread introduction of RFID.

7.3. Privacy in RFID systems

In the classical sense of the concept, privacy relates to the right of shielding off the home environment, the intimacy of life, confidential communication, and safeguarding the integrity of the body. Privacy was, and is, considered to be one of the conditions a person needs to develop and determine oneself. One needs to have the opportunity to protect oneself for the intrusion in ones private life in order to create prosperous conditions for realising autonomy and self-determination. This is part of the classical approach of privacy. It hinges on what can be labelled as 'relational privacy'. Due to the rise of information systems and the ubiquitous presence of data in digital form, the traditional concept of (relational) privacy has been extended to include 'informational privacy', privacy in which the data shadow of a person is at stake. Alan Westin's famous dictum defines informational privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated." (Westin, 1967) In Germany, one finds reference to the 'informationelle Selbstbestimmung' (self-determinacy over one's own information) in the German Constitutional Law (Article 8, Paragraph 9):

"If somebody cannot overlook with sufficient certainty which information concerning certain areas is known to his social environment … he can be significantly hindered from planning and deciding in a self-determined way … If somebody has to reckon with the registration of his participation in

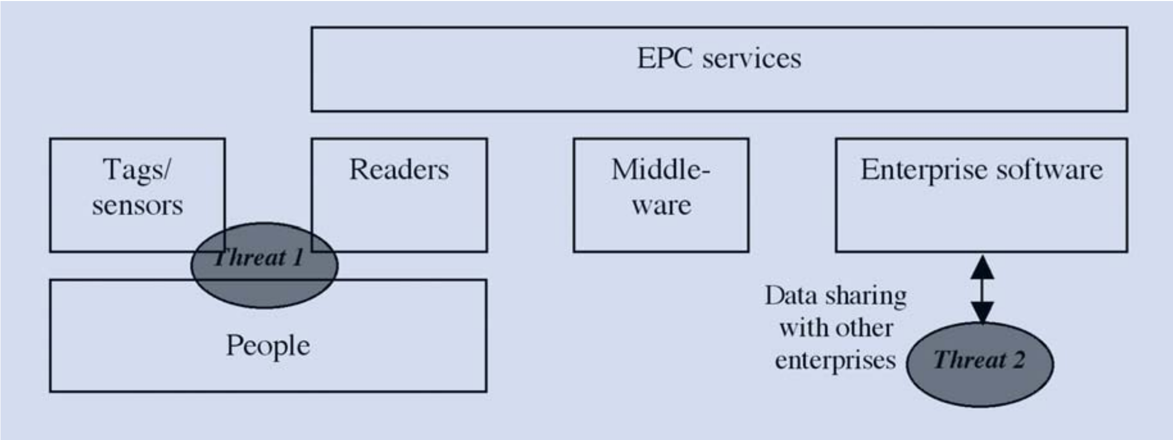
[64] Source Capgemini, 2005

a meeting or a citizens' initiative by the authorities and with the danger that risks for him are involved, he will perhaps not exercise his corresponding basic rights."[65]

RFID is a means for identification. The identification can be of products, services or persons[66] (cf. OECD, 2006b). In most cases, RFID-tags will be related to products. When however, a person is correlated to specific products by means of a token, an index or another pointer, the identified information becomes personal information (or information that enables the identification of a person). Due to the 'enabling' characteristics of RFID-tags – they can be used everywhere, in any situation for any purpose – the threat to privacy is a major concern, for the public, companies and governments alike (albeit for different reasons). As stated in the introduction, several bodies have indicated to perceive privacy as a kind of critical success factor for the widespread use of RFID. The near past has shown that trials with RFID – even trials in which the utmost care was given to privacy considerations – led to public arousal, due to perceived risks regarding the privacy.[67]

A literature review shows that authors address a broad range of privacy issues, related to several forms ('scenario's') of intrusion in the personal sphere of people.[68] The starting point for our own analysis is presented in *Figure 7-1* (adopted from (Garfunkel, 2005, p. 36). Though *Figure 7-1* refers to the EPC network, we think it is useful for more generic purposes. In *Figure 7-1*, two direct privacy threats are identified: one in relation to the tag-reader system, and one in relation to the information that is collected and disseminated outside the tag-reader system. The first kind of threat is the one that is most directly related to RFID. It focuses on the privacy implications of the tag-reader-system itself. The second kind of threat relates to the use of data collected by means of an RFID-system. The data that are disseminated by the tag-reader-system may be collected in a database, for instance to monitor pallets in a supply chain management system, in case of electronic payments, etc. This kind of threat is not uniquely determined by the RFID-system, but due to RFID the threats may be aggravated and have very specific dimensions.

Figure 7-1: Abstract view on privacy risks in EPC network[69]



[65] Quoted in: Von Locquenghien, K. (2006). p. 61-62.

[66] Distsinction made by Jeroen Terstegge, Corporate Privacy Officer, Philips.

[67] See http://www.boycottgillette.com/on the controversy surrounding Gillette using RFID to monitor buyers of Gillette razors; see http://networks.silicon.com/lans/0,39024663,39118760,00.htm for the privacy concerns surrounding the introduction of RFID in Metro; see http://www.spy.org.uk/cgi-bin/rfid.pl for an argument about the privacy implications surrounding the introduction of item-level tagging by Marks and Spencer.

[68] See (Article 29 2005a), (ECP.nl 2005), (Juels 2005), (Garfunkel 2005), (Spiekermann 2006)

[69] Adapted from Garfunkel et al.2006, p. 36. N.B.: The opaque circle identifies the direct privacy threat for the tag-reader system, the line through the tag-reader-middleware system identifies the linking of personal identity to a set of unique tags

The privacy threats will – in the end – be threats to an individual. The threat may however be a threat to a group of individuals, for instance in case of using profiling techniques to identify specific characteristics of groups of users. This leads to the following matrix, identifying the various privacy threats that will be discussed hereunder.

Table 7-3: Direct and indirect privacy threats, originating from RFID-systems

Privacy threats	Reader-tag system	Back-end
Individual	Unauthorised reading of personal information Real-time tracking of individuals	Aggregating personal information Using data for purposes other than originally specified
Collective/Group	-	Profiling and monitoring specific behaviour

7.4. Privacy threats within the tag-reader system

Privacy threats related to the tag-reader system refer to the following issues:

- The unauthorised reading of tags,
- Real-time tracking of individuals.

7.4.1. The unauthorised reading of tags

A tag may contain personal information. Identity cards and specific forms of public transport cards (seasoning tickets, for instance) will contain identifiable information. They may contain directly identifiable information on the card such as name and birth date. They also may contain data that functions as a key for a database in which personal information is stored. The privacy threat in the first case is obvious. When the data can be read out, a direct link can be made to a person. If other data is collected as well on the card (multi-purpose cards) a link may be made to these other data, thus revealing additional information about the holder of the card. In case a card holds indirectly identifiable information (a pointer that may refer to information about an identifiable person in a database), the privacy threat is indirectly present. Only when the intruder is able to link the pointer to the real person, privacy will be invaded. Within Europe, a dispute is continuing on whether all identifiable data should be considered as personal data (Article 29 WP, 2005). This is a difficult to solve issue. Private companies oppose a too strict definition; in their view pointers and tokens should not be considered as personal data.[70] General consensus exists that cards containing personal data require specific measures to prevent unauthorised persons to read the content of the card (for instance in case of loss of the card, or in case of unauthorised reading of the content of the card).

People consider the unauthorised reading of tags to be the most prominent privacy threat (Spiekermann 2006). Unauthorised reading is possible, especially in case of using UHF-based tags with reading ranges of approximately 7-10 m. EPCglobal pushes the market towards adapting UHF-based tags in order to enable multiple readings (higher bit-rate possible) and towards the introduction of smart shelves. The threat is most serious in case of item-level tagging. Implementation schemes of item-level tagging show that this will not happen on a large scale in the coming five to ten years. On the other hand field trials are occurring in which specific items are tagged. Next to the read range, it is necessary that the tag data can be read out. This presupposes that the data on the tag is not encrypted and that protocols are used which enable any reader to read out the data. Spiekermann (2006) indicates that this was the case with the EPC Generation 1 tags. When the tag can not be read out directly, read out can be attempted by means of eavesdropping. Eavesdropping is a special class of privacy threat. For this kind of threats a number of technical conditions have to be fulfilled, such as those concerning the read range and the clear availability of the data. Regarding the first aspect, one may determine a relation between read range and privacy issues. In general, there is a strict cor-

[70] This argument was spelled out in the consultation following the publication of the Article 29 Working Party report on RFID. See (Article 29 2005b).

relation between frequency used and read range; using UHF frequencies enlarges the read range to 7-10 metre, the 13.56 MHz read range (commonly in use for smart card applications) has a read range of 1.5 m and proximity cards only work at distances of approx. 10 cm. Juels (2005) discerns between different sorts of read ranges and argues that the tag-to-reader eavesdropping range and the reader-to-tag eavesdropping range outpace the nominal read range as specified in standards and product requirements. Within smart cards, which may contain personal information, the use of encryption may prevent successful eavesdropping. Authentication handshake protocols, in which the reader and the tag have to make themselves known to each other and where successful communication will only be established when they recognise each other, may be used to enhance secure communications.

7.4.2. Using tags to track persons

This is identified by Spiekermann as being the second biggest threat to privacy as identified by the people engaged in her research (Spiekermann, 2006). Tracking of persons via objects presupposes the linkage of identification data with individual track movements. Identification data can be acquired on the basis of electronic payments, loyalty cards, season cards in public transport, etc. When a person carries an object that is linked to that person (such as a wristwatch) the data of the tag attached to the wristwatch may be used as identifiable information for the person carrying the wrist watch. It is possible to track the movements of this person by surveying the movement of the object for which the tag data are known. The information can for instance be used to retrieve personal preferences. Information on specific customers in a shop can be collected on the basis of an identifiable loyalty card. The loyalty card is used to identify the customer and to follow the customer during his or her shopping sessions. Readers in the shop collect information about shopping habits of the customer, including the time spent in specific sections of the shop. One step beyond is the use of readers to identify very personal items (such as banknotes, medicines and identity cards). Information on these items, without the person knowing it, invades the privacy of the person. A person need not only be identified as a person, but s/he can also be identified as part of a group on the basis of a specific token (such as an identity card which may reveal the nationality of the individual). For this situation the Article 29 Working Party discerns specific privacy risks, including the risk that deploying this kind of technologies "will cause a boost in data to be processed by a wide variety of controllers, giving cause to concern".[71]

7.5. Privacy threats at the backend of the RFID system

The threats mentioned above, correlate directly with the RFID-reader to tag communication and the direct use of these data. Most privacy threats however refer to the collection and subsequent use of information outside the tag-reader system. Tags with unique IDs can easily be associated with a person's identity and smart cards with their own processing capacities may contain sensitive personal information. When linked to database systems, privacy threats may occur that are not unique for RFID but nevertheless pose serious problems. We have identified the following privacy threats related to the use of data outside the tag-reader system:

1. Using data for aggregating personal information,
2. Using data for purposes other than originally specified,
3. Using data to monitor specific behaviours.

7.5.1. Aggregating personal information

By means of data mining techniques it is possible to find correlations between hitherto separated objects (and subjects). When two persons exhibit similar travelling patterns and spend time together during travel, it may be assumed that they are somehow related to each other. This information can be enriched by confronting it with other information collected by other sources. When the seasoning ticket can be used as an electronic purse, shopping preferences may be added for in-

[71] Article 29 Data Protection Working Party, 2005, p. 6

stance. Data will be analysed in order to deduct social links between persons. This privacy threat was ranked third in the outcomes of Spiekermann's research. Deducting social networks may be especially interesting for intelligence agencies, for instance in trying to discover social networks of criminals: if one criminal can be traced, it is possible by datamining and pattern recognition techniques to sort out who else has a similar pattern of movement. This privacy threat is closely related to the following one.

7.5.2. Using data for purposes other than originally specified

RFID data may be collected for use in specific settings, but subsequently used in other settings. This is an example of 'function creep': though originally not perceived, data collected for a specific purpose turns out to be useful for other purposes as well. To stay with the example provided under the previous bullet: under the data retention acts that come into existence in Europe, national intelligence agencies may request the data on travel patterns in order to be able to select travellers who fulfil a specific profile. This has not been the intended use of this data. In this case one could argue that law enforces the use of data for this typical situation. The counter argument can be that with a specific design of the data system function creep may be prevented (for instance by anonymising data or by having strict rules for the period of data retention).

7.5.3. Using data to monitor specific behaviours

Monitoring can be done in real time (see point 3 above), but it also can be done on the basis of aggregated data, that are subsequently analysed in order to deduct specific patterns of behaviour. An example of using RFID technology for individual monitoring is the shop-owner who uses an identifiable token (such as a loyalty card) to collect information on shopping behaviour and uses this information to base decisions related for example on pricing without the consent of the customer. Even when the identity is not known, the shop-keeper can try to collect personal information on the basis of an identifier (such as a tag related to a personal belonging of the customer).

7.6. Open and closed RFID systems

To these privacy risks we will add the following two dimensions of RFID systems (OECD, 2006a). RFID systems are either open or closed. Closed RFID systems are systems that do not have links with an outer environment. According to the intention of the designer, data that are collected within the system do not trespass the system's boundaries and remain entirely within the system. Data from outside the system will not trespass the system's boundaries either. Open systems are systems in which data that are collected within the system may be shared with other systems.

An example of a closed system is a logistic system which uses proprietary solutions for dealing with the data it collects from its tags. The tags are used to identify pallets. Tracking the pallets is easier when using RFID since line of sight is not required and if needed, the tags can have additional functionality when combined with sensors (to measure temperature for instance). Additional information can be stored, on the level of individual pallets. In case the data collected are only used for supply chain purposes (following the supplies in transport), the system is a closed system. In case linkages are made with other systems the system may turn from closed into an open system.

An example of an open system is a public transport ticketing system which is used in conjunction with an electronic shopping system, for instance by adding e-payment functionality to the transport ticketing card for shopping at shopping malls. This functionality may be an interesting one for the passenger since for example it may give him or her benefits for shopping in shops related to railway stations. In this situation, however, the purpose of the travelling system and the purpose of the shopping system are distinct from each other. Though data sharing may be strictly bound to specific rules, set in advance by the responsible authorities, it can not be excluded that misuse of data will occur, since data collected for one purpose may be used for quite distinct purposes. Keeping track of the collected data becomes more problematic in an open situation; relations may exist with third parties outside the system who use the information collected for other purposes. This in the end will lead to a complicated mix of intertwined systems in which it becomes increasingly difficult to disentangle the various purpose specifications of each of the systems and see whether they are in line with each other. Issues as 'informed consent', 'purpose specification', 'use limitation' and the like will have become problematic.

7.7. Strategies to cope with the privacy threats

The use of RFID poses privacy threats, either directly by its tag-reader system or indirectly by the possible intrusion on personal information gathered in RFID-related databases. In attempting to safeguard privacy, different strategies may be pursued:

1. using law,
2. using self-regulation,
3. using technical solutions,

In case of RFID all three strategies are used. Much is expected of the possibility to safeguard privacy by technical means ('Privacy by design'). In the following subsections we present the three strategies in more detail.

7.8. Privacy laws

Started in 1973 with the Principles of Fair Information Practice as formulated by the US Department of Health, the OECD published in 1980 its privacy guidelines – which were based on these Principles of Fair Information Practice; the European Directive 95/46/EC in turn was based on the OECD guidelines. The European Directive formed the basis of many national data protection laws within Europe, in which national differences are of course introduced. Many of these are in effect today; they all encapsulate the same set of principles. This set of principles is summarised in *Box 7-1*

Box 7-1: 1980 OECD Guidelines on the protection of privacy and transborder flows of personal data[72]

"The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data … continue to represent international consensus on general guidance concerning the collection and management of personal data. … 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 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, complemented or amended.
8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles."

[72] OECD, 2006, p. 23

These eight principles define the information space in which legal forms of acquiring and processing data will take place. Some of the principles may be enhanced by using technical means, some of them require organisational approaches, for instance in defining roles and responsibilities concerning access to personal data. Two additional principles can be formulated that may be used to control the privacy sensitivity of the applications in which personal data are collected (Holvast, 2001):

- the principle of *subsidiarity*: the responsible agency for the data collection has the responsibility of choosing that form of data gathering, storing and processing that limits the impact on privacy most.
- the principle of *proportionality*: purpose and scope of data collection needs to be balanced with possible privacy impacts.

Overall, consensus exists that the European privacy directive (/95/46/EC) enables a proper treatment of privacy aspects related to RFID. Some issues are still contested. The consultation of the report of the Article 29 Working Party on Data Protection showed disagreement between private and public parties about the precise definition of 'personal data' (Article 29, 2005b). Private parties disagreed with the strict approach of the Working Party who defined personal data as "any information relating to an identified or identifiable person". They did not consider all RFID data to be related to a person and they considered the approach of the Working Party too restrictive. The Working Party especially warned for the broad scoping of identifiable information in stating that "account should be taken of all the means reasonable to be used either by the controller or by any other person to identify the said person." (Article 29, 2005a, p.8). The consultation revealed a difference of opinions about the question whether item level tagging based on EPC global standards will usually entail a processing of personal data. This dissensus has also been acknowledged at the recently held EU Consultation Workshop on RFID privacy implications.[73] To the immediate identification the OECD adds that identification may take place some time after having collected the data, may be by other parties than the parties originally responsible for the data collection process (OECD, 2006a). This addition increases the likelihood that RFID-data may turn out to be related to individual persons, and seems to be in line with the more stringent approach of the Article 29 Working Party.

Informed consent is another major challenge. The Article 29 Working Party stipulates the need for informed consent when this is legally required. Consent should be freely given, should be specific, should entail an indication of the individuals effective will, should be informed and should be unambiguous. The Working party provides the example of a supermarket for which informed consent is required and the example of surgery in which case there is no need to inform the patient about the data that is acquired on the tools that are used during the surgery. The practice of informed consent around RFID will have to be sorted out, especially in circumstances when third parties may use the data collected.

To enable individuals to exert their rights, the Working Party defines a number of information requirements that have to be met to comply with article 10 of the Directive. Responsible parties should provide information on:

- the identity of the controller,
- the purpose of the processing,
- the recipients (third parties),
- the existence of a right of access.

It continues by presenting the right of access by individuals (Article 12 of the EU directive). Individuals need to be able to check the accuracy of data ànd check the accuracy of the data processing.

RFID-data processing has to comply with similar requirements as other forms of data collection and processing. The European Privacy directive addresses the issues responsible parties have to be aware of. It is difficult to judge the practical consequences of a very strict interpretation of the directive. Concern is uttered by private parties who fear the RFID innovation process (and thereby economic growth) to be hindered by a too strict interpretation. The OECD

[73] EU Consultation workshop on RFID: Privacy, security, health and employment issues (16-17 May 2006, Brussels).

underscores this concern in its recent document when stating "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, while legitimate concerns that determine acceptance are identified and addressed." (OECD, 2006a, p. 6).

Except for the 95/46/EC directive another directive may bear importance for RFID applications. This is the European directive 2002/58/EC on Privacy and Electronic Communication (the 'e-Privacy directive'), which deals with issues related to personal data protection rules in case data are generated as a derivative of telecommunications traffic (for billing purposes for instance). There is some dispute about the applicability of this directive to RFID.[74] The combination of RFID with Location Based Services might turn RFID in location based data that bear a relation with subscription data and the like. The combination of RFID with a cell phone, turning the cell phone in a multifunctional device, capable of Near field Communication may be a situation in which RFID data should be considered to fall under the EU directive. This point of view was presented as a conclusion at the EU Consultation Workshop on Privacy, Security, Health and Employment effects.

7.9. Self–regulation

The private sector is willing to be engaged in a form of self-regulation. Self-regulation is in place in case legal regulations are considered to have adverse consequences one would like to prevent, in case self-regulation clearly has an added value in safe-guarding public interests and/or in case legal arrangements are not opportune given the technical state of affairs. In case of RFID one considers legal arrangements to be out of line, given the still immature technological basis of RFID. This opens the way to self-regulation. So far, a number of initiatives have taken place to stimulate self-regulation.

7.9.1. Addressing the issue by NGOs

In November 2003, civil liberty organisations in the USA (including Privacy Rights Clearing House, American Civil Liberties Union, Caspian and several academics) published a "Position Statement on the use of RFID on Consumer Products." The Statement was very critical about RFID and stated that "if used improperly, RFID has the potential to jeopardize consumer privacy, reduce or eliminate purchasing anonimity, and threaten civil liberties." (Garfinkel, 2005, p. 36). The organisations plead for a moratorium on the deployment of RFID until a formal Technology Assessment has been undertaken.

7.9.2. EPCglobal guidelines for EPC usage

EPCglobal has recently (2005) published a set of guidelines for EPC usage.[75] Components of this set are: notice, choice, security, record use, retention and consumer education. Notice is given by using marks on tagged objects and readers; choice refers to the possibility consumers may have to deactivate or remove the tag; security, record use and retention are safeguarded by EPC's statement that "the Electronic Product Code does not contain, collect or store any personally identifiable information." (quoted in OECD, 2006a, p. 25). This approach hinges on a clear separation between the tag-reader system and the use of the aggregated information in back-end systems, where product information can be combined with personal information, such as a loyalty card. Consumer education is perceived to be time consuming; they will have to be educated in order to recognise products with EPC tags.

7.9.3. Centre for democracy and technology guidelines for the deployment of RFID technology

The American Centre of Democracy and Technology has recently published a draft set of guidelines for the deployment of RFID technology (CDT, 2006). The guidelines have been discussed

[74] See for instance the Dutch position paper, written by a Dutch interest group on RFID, hosted by the Electronic Commerce Platform ECP.nl. Within this position paper, it is argued that European Directive 2002/58/EC is not applicable to RFID since no specific telecommunications infrastructure is in place for RFID and no specific operators for RFID are known (ECP, 2005).

[75] www.epcglobalinc.org/public_policy/public_policy_guidelines.html

with and are supported by a variety of important American stakeholders in the privacy dispute, such as Procter and Gamble, Microsoft, VISA USA and the National Consumers League. The guidelines are based on three general principles:

1. *Technology neutrality*: RFID technology by itself does not pose a privacy threat; privacy is threatened due to failing responsibilities in dealing with the data disseminated by RFID.
2. *Privacy and security as primary design requirements*: Users of RFID technology should address privacy and security issues as part of its initial design.
3. *Consumer transparency*: There should be no secret RFID tags or readers. The guidelines resemble the EPCglobal guidelines; the most important elements are equivalent to the EPCglobal guidelines; a few new entries are added.

The guidelines comprise: give notice; choice and consent; onward transfer, access and security (see *Box 7-2*).

Box 7-2: Privacy guidelines by centre for democracy and technology working group on RFID[77]

CDT Guidelines for deployment of RFID Technology

1. *Give notice*

Clear notice should be provided when information, including location information is collected through an RFID system and linked to a Personal Identification Information system (PII).

Consumers should be notified when entering an environment (public or private) where RFID technology is in use.

Consumers should be informed about the purposes of collection and use of the data collected.

Consumers should be informed when there is the possibility to deactivate or remove a tag; the burden of removing the tag should not be by the consumer.

Consumers should be noticed before the completion of a transaction.

The company collecting the data is responsible for providing notice.

2. *Choice and Consent*

Consumers should be notified in case they have a choice for usage or non-usage of RFID.

Consumers should be notified in case they have a choice for removing, de-activating or destroying the tag; in case consumers exercise their choice to remove, de-activate or destroy the tag, benefit from a warranty, or benefit from the protection of local law should not be compromised.[76]

In case linked information is solely used in order to facilitate a service delivered (including the functioning of a device) notice can be given, but consent or choice need not to be solicited. In other cases, consumers should be offered the opportunity to consent to such uses.

3. *Onward transfer*

In case personally identifiable information is shared with third parties, the contract with these parties should entail provisions with respect to level of protection of shared data to be equal or greater than afforded by the company collecting the data.

4. *Access*

When personal identifiable information is maintained on the tag itself, individuals should have reasonable access to their information

If an individual receives an adverse decision based on linked information about him or herself, that individual shall have reasonable access to that information.

5. *Security*

Companies should exercise reasonable and appropriate efforts to secure RFID tags, readers and any corollary information from unauthorised reading, logging and tracking.

Companies should establish and maintain an information security programme in keeping with industry standards, appropriate to the amount and sensitivity of the information stored on their system.

Companies should minimize the information stored on the tags themselves.

[76] This is fully in line with the Sydney declaration (2003) in which it is stated that "Whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags". www.privacyconference2003.org

[77] Source CDT, 2006

The various approaches towards privacy guidelines known today are all USA-based. Within Europe, discussion about appropriate guidelines and the role of guidelines vis-à-vis law enforcement has to be initiated yet. Discussing guidelines has the advantage above imposing regulations that it opens the debate, raises awareness and enables the sector to regulate the expected detrimental consequences of RFID themselves, with probably better results than when enforced by governments. Still, self-regulation will always be an add-on to formal regulation and will not replace regulation.

7.10. Technical solutions

There seems to be general consensus that privacy and security are two sides of the same coin in case of RFID. The Consultation Workshop in RFID, held 16 and 17 May 2006 in Brussels, showed a remarkable convergence on this by all participants, both from industry and academia. The OECD and the Article 29 Working Party on Data Protection endorse this view. The Article 29 Working Party "considers that technology may play a key role in ensuring compliance with the data protection principles in the context of processing personal data collected through RFID technology. For example, the design of RFID tags, RFID readers as well as RFID applications driven by standardization initiatives may have a great impact in minimising the collection and use of personal data and also in preventing any unlawful forms of processing by making it technically impossible for unauthorised persons to access personal data." (Art 29 WP, 2005, p. 12)

The OECD refers to many security researchers who argue in favour of considering both privacy and security issues that RFID raises before standards are set and implemented. According to the OECD "this 'privacy by design' approach might prove to be more efficient in the long run.", referring to the other approaches (law enforcement and self-regulation). (OECD, 2006a, p. 19).

Various solutions have been presented for tackling privacy issues by means of technologies, but most of them face practical drawbacks. Overall, these approaches should be considered as being part of Privacy Enhancing Technologies (PET). PET is based on minimising data collection that may entail personal data. The Common Criteria (part of ISO 15408) describe the following functionalities of PET:

- *Anonymity*: PET enables individuals to get services without revealing their identity.
- *Pseudo-identity*: PET enables individuals to get services without revealing their identity, by giving them a pseudo-identity; the real identity is related to the pseudo-identities in a database which only can be accessed by authorised persons.
- *Unlinkability*: individuals can use specific services while the use of the services can not be linked to each other.
- *Unobservability*: users can use services unnoticed by third parties.

Anonymity is stronger than pseudo-identity; unobservability is stronger than unlinkability (Registratiekamer/TNO, 1995). Looking at the purposes of RFID, which is identification of objects or persons and linking this to services, the four PET functionalities need to be explicitly taken into account when developing an RFID-based information system. They may serve as systems requirements that need to be fulfilled. They refer, amongst others, to using encryption techniques in case of storing personal data on a RFID tag (or smart card), to prevent unauthorised access. They also refer to introducing pseudo-identities in case the identity of persons is not strictly required. Pseudo-identities enable using the same RFID-cards for separate domains by enforcing different identities. The PET-functionalities may be used for the entire RFID-system, thus including the back-end systems where usage of the data is made and where linkages between different sources can be prepared. These approaches do not necessarily address RFID-issues, since they address more generic privacy concerns in dealing with stored and processed data.

Solutions that are more directly related to RFID are solutions that try to keep control over the data flow to the user (by means of killer and blocker tags) in order to prevent information to be disseminated against the wish of the user, and to offer the users an 'opt-in' choice. These solutions are based on the technical functioning of the RFID system, especially in the communication of RFID tag and reader. Other proposed solutions in this vein are using a Faraday cage to shield the tag from being read and reducing or removing the antenna (in first case as a means to reduce the read range, while in the last case as a means to disable the tag).

'Privacy by design' means that compliance with the privacy principles is sought by means of appropriate technical measures. Security researchers have shown that almost the full set of principles for Fair Information Practices can be met by an appropriate choice of data handling protocols. *Box 7-3* presents an overview of the approach.

Box 7-3: Enforcement of compliance of RFID with fair information principles[78]

Scanning with a purpose – Supporting the fair information principles in RFID Protocols

Openness through reader and policy identification

Today tags can not identify readers they are communicating with. It is proposed to add a unique reader policy ID (RPID) into the inventory command of the reader. This RPID can have a similar structure as the General Identifier Encoding (GID96) of EPC.

Purpose specification in inventory command

The Platform for Privacy Preferences Project (P3P) discerns twelve abstract purpose types. For RFID, fourteen purpose types have been discerned of which thirteen can be encoded as single bits. Five different profiling types can be discerned:

- ad-hoc tailoring (immediate and anonymous tailoring; example: providing recommendations on the basis of the content of a shopping basket);
- pseudo-analysis (use data to learn about preferences and characteristics of individuals; example: use information for re-arranging shelves);
- pseudo-decision (make customization decisions based on the interests of individuals without identifying them);
- individual-analysis (use collected and aggregated data to make personal profiles of individuals);
- individual-decision (use the collected information to determine individual preferences and to link them with identified data; this profile allows personal suggestions).

The latter profiles include the former.

Use limitation through collection types

Four different collection types are discerned: anonymous monitoring (collection status information without the need for actual identification); local identification (collection of unique IDs without the need for correlation of events); item tracking (monitoring item movements); and person tracking. By using collection types, boundaries are drawn between the various forms of data collection.

Collection limitation by appropriate tag selection

One can use selection masks to restrict tag ID collection. This requires the tag ID's to follow a known structure. This is the case with EPC tags.

Watchdog tag

In order to empower the user, a so-called watchdog tag can be used. A watchdog tag is an ordinary tag with a battery, a screen and a long range communication channel. It decodes commands transmitted by a reader and makes them available on screen. It can inform the user that some anonymous reader is scanning for tags in its vicinity. It can provide the operators ID, the purpose and type of data collection and the target range of tags.

The approach sketched above relates to the use of the Electronic Product Code. It is not a solution for use by more sophisticated tags, for instance in smart cards. Still, it is an interesting approach since it shows the viability of addressing privacy and security measures before standards are formulated and deployed. In practice, a number of problems still have to be overcome.[79] For one, to include issues such as air interface encryption and mutual authentication (between tag and reader) one requires readers with bi-directional communication (i.e. readers that transmit information about their status to the tag). Today, these readers are quite expensive (a few thousands of dollars per piece) which makes the deployment of these readers in environments where many of them are required, prohibitive. Another problem is the fact that low cost RFID devices do not have the com-

[78] Source Floerkemeier et al., 2005

[79] See (OECD, 2006a), (Juel 2005).

putational resources to use selected cryptographic methods. The kill tag, though appealing through its radical approach, may kill beneficial uses of the information that is hidden on the tag as well. This may be circumvented by using password driven tags, i.e. tags that can be re-activated by the user by means of a password. Using encryption may be hindered by problems of key distribution.

7.11. Conclusions

The European directive 95/46/EC and the national laws that are based upon it offer a good starting point for tackling privacy issues related to RFID. What should be questioned is the extent in which the Directive is able to deal with the reality of a situation in which RFID becomes widespread and is related to personal or identifiable information. What precisely should be considered as personal data is still an open issue. Aspects, such as how to practically organise informed consent, will have to be tackled as well.

In the future, the European e-Privacy directive (2002/58/EC) may become more important for RFID systems. This will especially be the case for the combination of RFID with location based services. For the time being, use of RFID does not seem to comply with the requirements of the e-Privacy directive.

Self-regulation is considered as having several positive effects: it creates commitment by stakeholders, it creates awareness by stakeholders and the general public, and it will contribute to coming to terms with the boundaries of existing privacy laws. Several initiatives for creating Codes of conduct are in place yet, most of them being US-based. Europe has a backward position in this respect. Codes of conduct handle such issues as notification, choice and consent, transfer to third parties, access and security.

Technical solutions to enforce privacy compliance may be of various kinds. For one, specific technical measures are possible that prevent collection of (personal) data and enhancing control by users (blocker and killer tags, ‘deep sleep mode’, using Faraday cage and destroying antenna capacity). For another, it has been shown that the Principles of Fair Information Practice can be realised by an appropriate configuration of the reader-tag communication. Privacy Enhancing Technologies enable privacy enhancing functionalities of RFID systems, such as realising anonymity, using pseudo-identities and realising unlinkability and unobservability. Technical solutions may have a drawback, in that they are costly, require managerial resources, or deny useful functionalities of RFID systems to users.

8. Security aspects of RFID

8.1. General overview of RFID security threats

This chapter will contain a general overview of security threats of an RFID system, consisting of an RFID tag and a reader. The security threats are classified as either threats for the tag, or the air interface between the tag and the reader, or the reader.

8.2. Security threats for the tag

8.2.1. Falsification of contents

Data can be falsified by unauthorized write access to the tag. This type of attack is suitable for targeted deception only if, when the attack is carried out, the ID (serial number) and any other security information that might exist (e.g. keys) remain unchanged. This way the reader continues to recognize the identity of the tag correctly. This kind of attack is possible only in the case of RFID systems which, in addition to ID and security information, store other information on the tag.

8.2.2. Falsification of tag ID

The attacker obtains the ID and any security information of a tag and uses these to deceive a reader into accepting the identity of this particular tag. This method of attack can be carried out using a device that is capable of emulating any kind of tag or by producing a new tag as a duplicate of the old one (cloning). This kind of attack results in several tags with the same identity being in circulation.

8.2.3. Deactivation

These types of attack render the tag useless through the unauthorized application of delete or kill commands (Auto-ID center). Depending on the type of deactivation, the reader can either no longer detect the identity of the tag, or it cannot even detect the presence of the tag in the reading range.

8.2.4. Physical destruction

Tags could be physically destroyed by chemical or mechanical means, or by using strong electromagnetic fields (like in a microwave oven). Active tags could also be shut down by removing or discharging the battery.

8.2.5. Detaching the tag

A tag is separated physically from the tagged item and may subsequently be associated with a different item, in the same way that price tags are "switched". Since RFID systems are completely dependent on the unambiguous identification of the tagged items by the transponders, this type of attack poses a fundamental security problem, even though it may appear trivial at first sight.

8.3. Security threats for the air interface

8.3.1. Eavesdropping

The communication between reader and transponder via the air interface is monitored by intercepting and decoding the radio signals. This is one of the most specific threats to RFID systems. The eavesdropped information could for example be used to collect privacy sensitive information about a person. It could also be used to perform a replay attack, i.e. the attacker records all communicated messages and later on can either simulate this tag towards the reader, or simulate this reader towards the tag.

8.3.2. Blocking

So-called blocker tags (Juels et al., 2003) simulate to the reader the presence of any number of tags, thereby blocking the reader. A blocker tag must be configured for the respective anti-collision protocol that is used.

8.3.3. Jamming

Jamming means a deliberate attempt to disturb the air interface between reader and tag and thereby attacking the integrity or the availability of the communication. This could be achieved by powerful transmitters at a large distance, but also through more passive means such as shielding. As the air interface is not very robust, even simple passive measures can be very effective.

8.3.4. Relay attack

A relay attack (Kfir et al, 2005) for contactless cards is similar to the well known man-in-the-middle attack. A device is placed in between the reader and the tag such that all communication between reader and tag goes through this device, while both tag and reader think they communicate directly to each other. Smartly modifying this communication could for example in payment systems lead to charging the wrong electronic wallet (a smart card with an RFID tag). To make this attack more practical one could increase the distance between the legitimate card and the victim's card by splitting the device into two components, one communicating with the reader, and one with the victim's card. The communication between these two components could be implemented by any kind of fast wireless technology.

8.4. Security threats for the reader

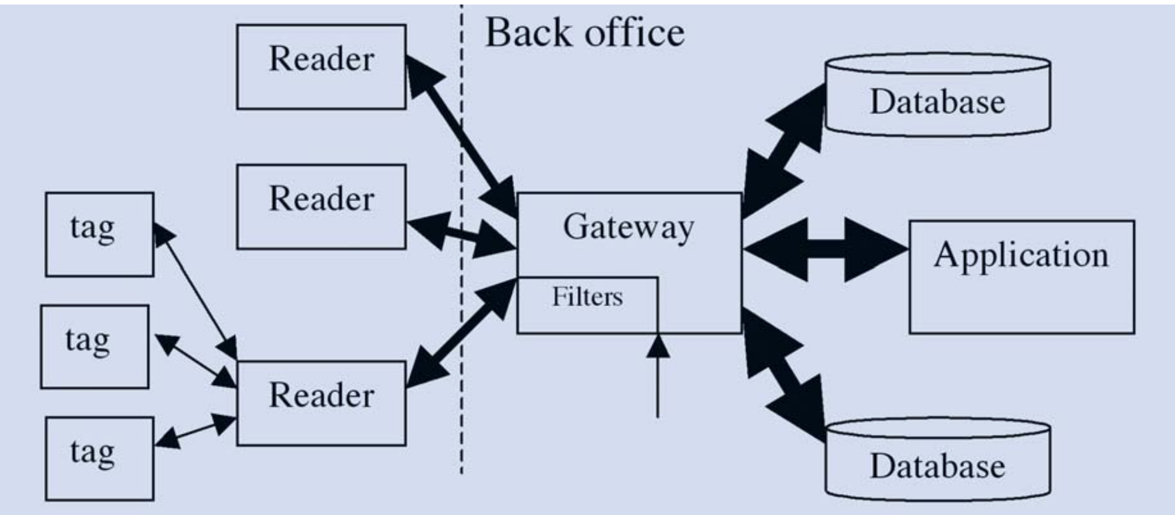
8.4.1. Falsifying reader ID

In a secure RFID system the reader must prove its authorization to the tag. If an attacker wants to read the data with his own reader, this reader must fake the identity of an authorized reader. Depending on the security measures in place, such an attack can be "very easy" to "practically impossible" to carry out. The reader might need access to the backend in order, for example, to retrieve keys that are stored there.

8.4.2. Security threats for other parts of RFID systems

When considering the security challenges of RFID in a broader perspective, one has to take into account the infrastructure including a back office where additional information of all tags is stored, and the aspect of convenience in use. A general RFID architecture is depicted in *Figure 8-1*.

Figure 8-1: A general RFID architecture



Real-life RFID deployments employ a wide variety of physically distributed RFID readers, access gateways, and databases. The middleware receives events from the RFID readers when tags are scanned. These events are passed through a number of filters, which process the events in an application-specific manner. When an event has passed through all filters, it is dispatched to the components that have registered an interest in such events. Often, one of these components will store the event in a database, for further processing.

RFID readers are generally connected to the middleware using modular drivers much like Windows uses device drivers to communicate with a graphics card. This allows different readers to be used with the middleware, without having to modify the middleware.

In addition to event-processing, the middleware handles different kinds of user interfaces. A user interface is generally provided for system-management purposes, for example to modify the series of filters through which an event is passed. There will also be user interfaces that allow regular users to access the system and use it. For example, in a supermarket distribution centre, there will be a user interface that provides information on the current stock levels.

The middleware also communicates with other software systems, which implement the application's business logic. To stay with the supermarket example, it is likely that the supermarket RFID system is connected to a stock management system, which orders new stock from suppliers before it runs out.

When considering the broader RFID architecture of *Figure 8-1*, new security risks and countermeasures come to mind:

8.4.3. Tag-borne attacks at back office[80]

One could foresee an attack at the back office through information stored at the tag, which was recently shown by PhD student Melanie Rieback, MSc student Patrick Simpson, Assistant Professor Bruno Crispo, and Professor Andrew Tanenbaum of the Vrije Universiteit in Amsterdam (Rieback et al., 2006). Basically there are three types of RFID malware which are mentioned in increasing complexity of implementation:

1. RFID exploits: Just like other software, RFID systems are vulnerable to buffer overflows, code insertion and SQL injection.
2. RFID worms: A worm is basically an RFID exploit that downloads and executes remote malware. A worm could propagate through the network or through tags.
3. RFID viruses: An RFID virus starts with malicious content of a tag. When the tag is read out, this initiates a malicious SQL query which would disturb a database in the back office. Although such an attack has not yet been performed in practice (AIM Global, 2003), such a type of threat cannot be excluded.

8.4.4. Misuse of gateway interface

The user interface to the gateway could be misused by unauthorised people to attack the integrity of the filters and to misguide the product management system.

8.4.5. Corrupted drivers

The drivers that are used by RFID readers to communicate with the middleware could be corrupted. This could be done either by modifying the driver of a legitimate reader, or by replacing the legitimate reader with a fake reader that has a corrupted driver. A corrupted driver could be used to attack and misguide the gateway.

8.4.6. Attacking the reader-gateway communication

The communication between reader and gateway could be eavesdropped or modified.

8.5. Security measures for the tag

8.5.1. Security measures to prevent unauthorized modification of tag data (contents and ID)

An obvious security measure to prevent modification of tag data is to use read-only tags for which unauthorized modification is intrinsically impossible. Another effective measure, also recommended for reasons of data management, is to shift all data except the ID to the backend. Some types of tags dispose of an authentication method (like the ISO 9798 standard), through which the

[80] We only consider attacks at the back office that are RFID related.

reader can be authenticated by the tag such that only authorized readers can modify the tag contents.

8.5.2. Security measures for deactivation

Unauthorized application of delete commands or kill commands can be prevented by using an authentication method (when available).

8.5.3. Security measures for physical destruction

A counter measure for physical destruction of the tag would be a close mechanical connection between the tag and the tagged item to make it difficult to destroy the tag without damaging the item. To prevent discharging the battery of an active tag one could implement a sleep mode in the tag.

8.5.4. Security measures for detaching the tag

A counter measure for detaching the tag from the tagged item would be a tight mechanical bond between the tag and the tagged item to ensure that removing the tag will also damage the product. In case of active tags, an alarm function is conceivable: a sensor determines that the tag has been manipulated and transmits the alarm to a reader as soon as it comes within range. For high value items an option would be to manually check whether the tag is attached to the correct item.

8.6. Security measures for the air interface

8.6.1. Security measures for eavesdropping

An effective measure to reduce the effect of eavesdropping is to shift all data to the backend. A consumer that just bought some tagged object, which tag has no legitimate use any more, could use shielding to prevent the tag from being read out by intruders. This could be established by wrapping the tag in metal foil or by placing it in an aluminium-coated bag. More advanced tags have a module to encrypt the communication with the reader which also prevents eavesdropping. Such advanced tags cannot by read out by intruders, and are still available for legitimate use. Another measure would be to design the RFID system such that tags are used with a small range which is just sufficient for the legitimate readers (and thereby shutting out a class of unauthorised readers).

8.6.2. Security measures for blocking

There are no technical measures to prevent the use of blocker tags, but a solution is to ban their use in the standard terms and conditions of business.

8.6.3. Security measures for jamming

It is possible to detect jamming transmitters by performing random measurements or by using permanently installed field detectors.

8.6.4. Security measures for relay attacks

One way to guard against relay attacks is to shield the tag when it is not used e.g. by putting the tagged card in a Faraday like cage (Kfir et al., 2005). Another way is to require an additional action by the user (push a button, type in a PIN code or use a fingerprint) to activate the tagged card, although this solution eliminates some of the convenience of the contactless system.

8.7. Security measures for the reader

8.7.1. Security measures for falsifying the reader ID

To prevent readers to falsify their ID and obtain unauthorized access to a tag, an authentication method (when available at the tag) can be used to authenticate the reader towards the tag (ISO/IEC, 1999). This risk can be further reduced when the reader has to access the backend during the authentication procedure, e.g. to retrieve cryptographic keys.

Note that these measures are designed to assure the integrity of a reader that is about to communicate with the tag. For measures like shielding which prevent an unauthorised reader from communicating at all see "Security measures for eavesdropping" (8.6.1).

8.8. Security measures for other parts of RFID systems

8.8.1. Security measures for tag-borne attacks at back office

To avoid such attacks, the content of tags should be checked by the reader, and regular security measures should be taken to protect the gateway. A typical countermeasure against RFID viruses is to improve the software in the gateway which is able to distinguish a regular tag ID from an SQL query such that these attacks can be prevented from entering a database.

8.8.2. Security measures for misuse of gateway interface

To prevent such an attack the user interface should be provided with some kind of authentication mechanism such that only authorised users are able to access the gateway. Another measure would be to place the gateway and the user interface in a physically protected room such that only authorised employees that have access to this room can access the user interface.

8.8.3. Security measures for corrupted drivers

A possible solution to this problem is to use only signed drivers, i.e. each legitimate driver should be digitally signed such that the gateway can check that communicating readers contain a legitimate driver.

The use of drivers enables the fact that different readers can be used to communicate to the gateway. From a security point of view the use of different readers should be encouraged because an attack is likely to be specific for one type of reader or one type of driver, so a diversification of types lowers the impact of a possible attack.

8.8.4. Security measures for attacking the reader-gateway communication

The communication between reader and gateway could be eavesdropped or modified.

8.8.5. Security measures against cloning

When considering one tag and one reader as a system, which has been done in the previous sections, the risk of cloning (duplication of the tag ID in a new tag) has been identified. Only in the broad view of the complete architecture, such a risk could be handled: in the database where all the different tag IDs (with respect to a specific application) are collected, a duplicate ID could be detected and in some cases even the clone could be recognized (i.e. be distinguished from the original tag).

8.9. General security evaluation of RFID

Given the security risks of an RFID system, and the available security measures, we can evaluate the security of RFID. This means incorporating (a qualitative estimate of) the costs of each security measure and on the other hand (a qualitative estimate of) the costs of performing a specific attack (FOIS, 2004). The comparison of these two types of costs will give insight into the vulnerabilities of RFID systems.

Table 8-1: Summary of security evaluation

Object	Threat	Cost of performing attack	Cost of countermeasures
Tag	Unauthorized modification of data	Medium to high	Low to medium
	Deactivation	Low to medium	Medium
	Physical destruction	Low to medium	Low to medium
	Detaching the tag	Low	Low to medium
Air interface	Eavesdropping	High	Medium
	Blocking	Low	Low
	Jamming	Medium to high	Medium to high
	Relay attack	High	Low to medium
Reader	Falsifying reader ID	Medium to high	Medium

The summary of the security evaluation is shown in *Table 8-1*. The qualitative estimates of the costs are explained in the following sections, followed by a separate section of conclusions.

8.9.1. The costs for unauthorized modification of data

To perform an unauthorized modification of data in case of re-writable tags, the attacker would have to acquire a reader that is capable of writing on the tag. Due to the short range involved the possibility of this attack is limited. The longer the range of the reader, the more expensive the attack would be.

In general, a read-only tag is less expensive than a re-writable tag, so in case the application allows, a replacement by read-only tags would be a fine countermeasure. When the tag has an authentication method available, the costs of switching it on are low, most expenses would go in the management of tags and readers which have to be loaded with cryptographic keys. To shift all data on the tag to the backend requires a new infrastructure (in the backend and for provisioning of the tags and readers) which brings high initial costs, but will fade out later.

8.9.2. The costs for deactivation

A deactivation by means of a kill command requires a dedicated device and usually a password.

When the tag has an authentication method available, the costs of switching it on are low, most expenses would go in the management of tags and readers which have to be loaded with cryptographic keys. This would prevent unauthorized usage of the kill command.

8.9.3. The costs for physical destruction

To physically deactivate a tag is easy by means of chemicals or exposure to an electromagnetic field, or to destroy the antenna.

To prevent physical deactivation one could introduce a tight mechanical bond between the tag and the tagged item to ensure that removing the tag will also damage the product.

8.9.4. The costs for detaching the tag

In general a tag can be easily detached from the tagged item, unless some mechanical bond is placed between the tag and the tagged item. Alarm functions in which tag manipulation is detected by a sensor are only available in more expensive active tags.

8.9.5. The costs for eavesdropping

To perform unauthorized reading of data, the attacker would have to acquire a suitable reader. Due to the short range involved the possibility of this attack is limited. The longer the range of the reader, the more expensive the attack would be.

A cheap and effective way to prevent eavesdropping is to use some kind of shielding of the tag, although this would have to be performed for every tag. When the tag has an encryption method available, the costs of switching it on are low; most expenses would go in the management of tags and readers which have to be loaded with cryptographic keys. To shift all data on the tag to the backend requires a new infrastructure (in the backend and for provisioning of the tags and readers) which brings high initial costs, but will fade out later.

8.9.6. The costs for blocking

A blocker tag is relatively cheap and can prevent a reader from working properly, although they only work for specific anti-collision procedures. An easy countermeasure is to ban their use in the standard terms and conditions of business.

8.9.7. The costs for jamming

A jamming transmitter has to be powerful enough to jam the tag-reader interface, and it requires some technical experience. The price of the transmitter increases with its range.

A field detector to detect possible jamming transmitters is a dedicated device, and measurements are performed by skilled engineers.

8.9.8. The costs of a relay attack

To perform a relay attack requires a special device to intercept and modify the radio signal, and especially the communication between the two main components would be sophisticated.

To place the smart card in a Faraday save holder is relatively easy to do. An extra action by the user before activating the smart card would require a more sophisticated card and/or reader.

8.9.9. The costs for falsifying the reader ID

To falsify the reader ID, an attacker would have to obtain some secret key. The difficulty for obtaining such a key depends on the implementation.

When the tag has an authentication method available, the costs of switching it on are low, most expenses would go in the management of tags and readers which have to be loaded with cryptographic keys.

8.10. RFID security challenges in a broader perspective

The security risks that are mentioned in the previous paragraphs depend of course on the type of application in which RFID is used. The seriousness of each risk will vary along the different application areas. Therefore, we will analyse the seriousness of the security risks mentioned in section 8.1 for the most relevant application areas, which will give some insight in the considerations involved.

We consider five application areas of which the first four are cases within the overall RFID study and the fifth offers an interesting case from a security perspective:

- *Healthcare*: consider the environment of a hospital or clinic. RFID in such environments is typically used for tracking and listing tagged medicines and blood bags. Also persons could be tagged. We consider two situations in which persons are tagged namely doctors that have to be tracked (in which room they are) in case of an emergency, and patients that have to remain within specific areas (e.g. an area for serious psychiatric patients). In the latter case RFID is used for access control at the borders of these areas.
- *Animal tracking*: in some situations animals are tagged (externally or internally) in order to trace them in case of an infectious disease. Currently this is only done with goats, sheep and pets.
- *Public transport*: in several cities (e.g. London, Porto) and countries (e.g. the Netherlands) an electronic ticketing system has been developed such that only people with a valid ticket can pass the gate and enter the bus, tram or train. Some tickets are anonymous, some are personalised.
- *Identity card*: some identity cards, like the new passport in the Netherlands, contain RFID chips such that the passport can be read automatically. To hinder unauthorised reading, an initial step is required before the RFID tag can be read. In this initial step an optical device will have to look into the passport and read the cryptographic key which is subsequently used to encrypt the

communication between tag and RFID reader.

- *Smart shop*: articles in a shop are tagged using Object Naming Service (ONS). The tag is not only used for logistics and identification, but also for providing extra services to the customer. The tag number leads to an Internet site where additional information about the article can be found like a warranty, the ingredients of the product, etc.

Within each application area, an estimate of the seriousness of the different security risks is made. The summary of this evaluation is shown in *Table 8-2*, where "N/A" means that this security risk is Not Applicable to (or not realistic within) this application area.

Table 8-2: Security risks per application area

Security risk	Health care	Animal tracking	Public transport	Identity card	Smart shop
Unauthorized modification of data	high impact	tags are read-only	relevant	high impact	relevant for rewritable variants
Deactivation	linking in database	N/A	frustration	N/A	privacy vs. extra service
Physical destruction	only for persons	possible by animal	procedural measures	fraud	consumer right
Detaching the tag	both persons and objects	possible by animal	leads to physical destruction	leads to physical destruction	consumer right
Eavesdropping	N/A	N/A	replay attack	relevant	privacy
Blocking	N/A	N/A	sabotage	sabotage	sabotage
Jamming	N/A	N/A	sabotage	sabotage	sabotage
Relay attack	N/A	N/A	possible free transport	ID fraud	possible
Falsifying reader ID	N/A	N/A	replay attack	relevant	privacy

For a clarification of the security risks see section 8.2. The results of *Table 8-2* are explained for each application area in the following sections.

8.10.1. Healthcare

When the tag number of medicines or blood bags could be modified by unauthorised people, the impact of such an action would be high because it might lead to patients receiving bad medicines or wrong blood types. Although the probability of occurrence and success could be low, the high impact of such an attack still justifies adequate measures to prevent it.

The deactivation of a medicine tag in a hospital environment for privacy reasons will probably be less useful since the linking between medicines and patients is usually performed in a database in the back-end.

A physical destruction of a tag on a medicine or blood bag might cause confusion but will not lead to patients receiving bad medicines or wrong blood types. A patient whose action radius is bounded by his tag however has a clear motivation for destroying the tag. A possible measure would be to require a valid tag before leaving the area, but this would also have consequences for visitors and hospital personnel. A doctor that is being traced by his tag could incidentally destroy his tag, so some alert mechanisms could be built in for this.

Detaching the tag of a medicine has the same consequence as physical destruction of the tag. The hospital should have alternative ways (e.g. etiquettes) to identify medicines. The main difference is that this tag could be (accidentally) replaced at another medicine with possible severe consequences. The same reasoning goes for detaching the tag on patients or doctors.

Other security threats like eavesdropping and jamming are possible but seem unrealistic in this application area.

8.10.2. Animal tracking

Most of the tags in this application area are read-only tags, so there is no risk of unauthorized modification of data. Since there is also no reason for having a deactivation function, this risk is hardly applicable. In case of rewritable tags, there is a risk of unauthorized modification of the tags by the owner, especially in case of fraud. This would block the goal of tracking the animals in case of infectious disease. However, since all animals are registered in a central database, this action will not be effective.

The highest risk in this application area is the risk of physical destruction or detachment of the tag by the animal. This would block the goal of tracking the animals in case of infectious disease. A measure to reduce this risk is to regularly check the presence of a valid tag on these animals.

Note that it might be in the interest of the owner to destroy tags of his animals to avoid being held liable by animal health authorities. However, as noticed before, since all animals are registered in a central database, such an action will not be effective.

8.10.3. Public transport

Unauthorized modification of the contents of a ticket is very relevant in a public transport ticketing system. The departure or arrival location in a ticket could be changed, or billing information of the ticket could be changed. Some ticketing systems incorporate an electronic purse that could be uploaded.

The tags in the tickets might have deactivation functionality for deactivating the tag during distribution to the ticket office. There is a risk that passengers will cause frustration to other passengers by deactivating their tickets during transport. This risk can be limited by using proper authentication mechanisms for the deactivation function.

Physical destruction of the tag, either accidentally or on purpose, is a clear risk of such a ticketing system. Clear procedural measures should be taken to cope with it.

The tickets are usually designed such that a possible detachment of the tag can only be done by physical destruction of the ticket. Replacement of a tag on another ticket is not a serious threat because tickets can only be used once.

By eavesdropping an RFID communication, e.g. by putting an eavesdropping device in a gate or using an illegal RFID reader, one could be able to reuse (replay attack) this communicated information to form invalid tickets.

Blocking and jamming will probably not lead to free tickets, but could severely frustrate (or even shut down) the public transport system.

A (sophisticated) relay attack could lead to public transport on the cost of other persons. Since such an attack is rather elaborate to develop, it will only be interesting when it results in a large number of free passages. A detecting mechanism in the back-office could reduce the risk of such an attack.

8.10.4. Identity card

Unauthorised modification of data is of course absolutely undesirable in case of an identity card. Therefore, in the design of the ID card, sophisticated measures are taken to reduce the risk of such an attack.

There's no reason to implement deactivation functionality into an ID card, so there's no risk for deactivation.

The ID card is designed in such a way that detachment of the tag will usually lead to physical destruction of the tag. Although the tag of an ID card could be destroyed accidentally, such destruction will usually lead to a fraud investigation.

Eavesdropping (including reading the card with a fake reader) is a very relevant threat for RFID based ID cards, so extra measures are taken in the design of the card. Think for example at the risk of a terrorist scanning passports looking for a specific nationality to attack.

Both blocking and jamming of the communication between ID card and RFID reader can be considered as sabotage and could even be prohibited by law.

A relay attack in an ID card setting makes sense and would eventually lead to ID fraud. On the other hand, the extra measures that are taken in the design of an ID card will make such an attack much tougher to complete.

8.10.5. Smart shop

For cheap articles the RFID tags used will be probably read-only, but for more expensive articles one might want to reuse the tags while at the same time becoming vulnerable to unauthorized modification of data. This might lead to wrongly priced items, extended warranties, etc.

For privacy reasons a consumer would like to deactivate (sleep mode, kill) the tag after leaving the shop. On the other hand, the producers would rather see this tag activated because it enables them to provide lots of extra services to the consumer. The debate about whether to provide deactivation functionality is still going on [7].

The consumer has the right to either physically destruct, or detach the tag to protect his privacy. Unauthorised persons could get access to privacy related information on the tag by means of either eavesdropping on a legitimate reader or by faking a legitimate reader ID. The use of fake RFID readers in a shop could be detected by suitable scanners.

Blocking and jamming are techniques that could be used to frustrate RFID readers and sabotage the legitimate use of RFID tags.

A relay attack could be possible, for example by a consumer that is paying for a cheap product while he actually bought an expensive product, although it's questionable whether such an attack would be worthwhile in practice. It might for instance be easier to just switch the tags of the cheap and the expensive product, or to use a device that fakes the tag of the cheap product (without actually communicating with the tag of the cheap product).[81]

8.11. Security aspects of RFID in EU research projects

RFID is an actual research topic in many European projects and publications, such as the formal EU research projects in the IST-programme and the (predecessors of the) CIP-programme. Besides, there are many academic researchers worldwide who are studying a broad range of security aspects of RFID. Since 2002, Gildas Avoine (a French researcher, currently working at MIT, USA) maintains a website with refereed papers published in journals and conference proceedings, as well as technical reports and theses related to security and privacy issues in RFID systems.[82] Most of these research papers concern security issues regarding the communication between tag and reader. Briefly, in this area academic research is mainly focused on the more expensive smartcard solutions (e.g. electronic ticketing in public transport, identity cards, healthcare sector) and less on the logistic process (e.g. replacement of barcodes by RFID-tags). Given the sensitivity of the data processes that are in use in these domains, the development of security mechanisms (by cryptographic techniques) is of high relevance to the overall developments within RFID. Even the less sophisticated passive and relatively simple tags will be more and more equipped with cryptographic techniques.

This section primarily focuses on RFID in the European research programmes and specifically on the security issues of RFID.

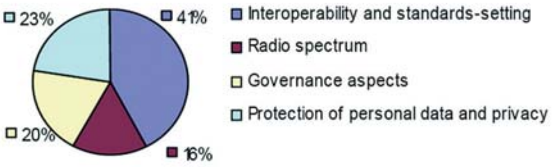
8.11.1. Research projects on RFID

A recent overview of RFID research in Europe shows a total of 40 collaborative research projects supported by European industry and research organisations. The European Commission contributes €153 million to a total investment of €312 million. These research projects are all part of the Fourth, Fifth or Sixth Framework Programme. The 40 projects cover a broad array of issues. 41% of the project funding is related to interoperability and standards-setting, 16% to research of the radio spectrum, 20% to governance aspects and 23% to protection of personal data and privacy.

[81] Although not part of this application area, a relay attack could be more useful when an RFID tag is used during payment e.g. by means of a payment card. In such cases it could be possible to pay products with payment cards of other (innocent) people (Kfir et al., 2005).

[82] http://lasecwww.epfl.ch/~gavoine/rfid/#papers

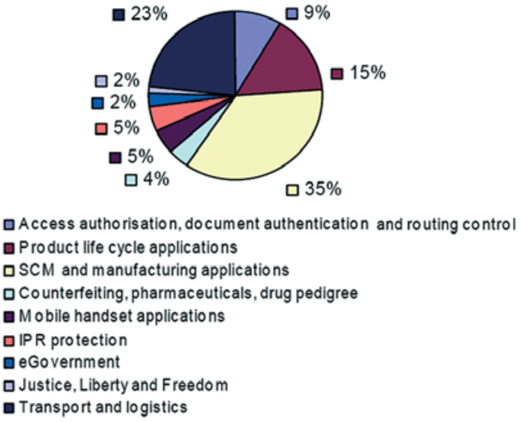
Figure 8-2: Relationship of RFID research projects to policy issues[83]



A prime example of such a research effort is the recently launched BRIDGE-project, a €7.5 Million, three year RFID-project in the Sixth Framework programme for Research and Technological Development.[84] BRIDGE ('Building RFID solutions for the Global Environment') combines research institutes, a number of GS1 offices (five from Europe and one from China), twelve solution providers and seven business end users. The focus of BRIDGE is on providing solutions for the supply chain in a number of application areas (anti-counterfeiting, healthcare, retail, textile, ...). It will study business based research, provision of information services and hardware (sensor, tags) and software development.

The potential applications for RFID are multiplying rapidly. In the figure below the extended variety of application areas have been shown.

Figure 8-3: RFID projects by application area[85]



The European funded research and related promotional activities aim at helping industry, regulators and consumers to better understand the potential benefits and potential pitfalls of RFID, removing many of the risks and uncertainties from the market and so encouraging wide scale investment (EC, 2006a).[86]

8.11.2. Security aspects of RFID in EU research projects

A wide consultation on wireless smart tags in 2004 investigated the need for further research in the technology and application domain. The consultation report presented the findings, conclusions and recommendations from the wide consultation exercise relating to the research needs for the topic of smart wireless tags, which are also known as RFID (Radio Frequency Identification) or smart tags (EC, 2006a). The consultation exercise was undertaken as part of the process for the preparation of the IST work-programme 2005-2006. In addition however, the report also included recommendations for longer-term research in the smart wireless tag area, research that naturally fits within the time scale of Framework Programme Seven, which will cover the period 2007-2013.

From this consultation report it can be concluded that the respondents considered the privacy and security of RFID tags as a fundamental enabler or a *showstopper* of smart wireless tag technology. Some research needs that were concluded in the field of security were:

- Encryption to protect the tag data.
- Finding cost-effective solutions for the expected increase of backend system costs. The increased security capabilities on tags will affect backend systems since these will require additional functionality. This will increase system costs.
- Increased demand for greater security will require tags with computation capabilities and memory. In the long-term, research is needed into the construction of highly miniaturized devices.

We looked in more detail to the coverage of security aspects of RFID in the 40 research projects

[83] Source: http://ec.europa.eu/information_society/doc/factsheets/5-1-rfid-research-portfolio.pdf

[84] See http://www.bridge-project.eu

[85] Source: http://ec.europa.eu/information_society/doc/factsheets/5-1-rfid-research-portfolio.pdf

[86] URL: http://europa.eu.int/information_society/policy/rfid/index_en.htm

(FP4, FP5 and FP6). Notwithstanding the recommendations from the consultation report of 2004, it was remarkable to find that security was not a prime area of interest. In only two research projects security aspects make part of the research objectives.

A search in the CORDIS database revealed the two projects in which security aspects are (partially) covered: *Improving airport efficiency, security and passenger flow by enhanced passenger monitoring (OPTAG)* and *Safeguards in a World of Ambient Intelligence (SWAMI)*. The projects are concisely described below, based on information from the CORDIS-database:[87]

OPTAG[88]	
Start date: 2004-03-22	End date: 2007-02-01
Duration: 34 month	
Programme type: Sixth Framework Programme	

Description:

This project aims to harness emerging passenger tracking and identification technologies with the objectives of increasing the safety of air travel whilst maximizing the utilization of existing facilities. The proposed system could form an essential component of Airline passenger identification and threat assessment systems through the automated identification of suspicious passenger movements or through the closer the closer monitoring of individuals considered to pose a risk to secure operations. The project aims to deploy networks of enhanced Closed Circuit Television (CCTV) systems coupled to local, direction based, and passenger tracking systems, using far-field RFID tags.

There are three main developments required to create the OpTag system:

- A compact far-field radio frequency identification (RFID) tag and a reader capable of reading a large quantity of tags within its range without interference.
- A high-resolution, panoramic imaging system and corresponding software to follow a target and confirm the identity of the tagged individual or item. The system will be able to work over a network and allow different operators to select different views from the same camera.
- An ergonomic user interface to facilitate augmented surveillance, monitoring and targeting of individuals who may pose an economic or security risk to effective airport operations.

The security and efficiency environment of airports will also be researched so that the Optag system can be understood in context and developed to meet real requirements and with full understanding of the legal and operational factors and IP of the design.

SWAMI	
Start date: 2005-02-01	End date: 2006-07-31
Duration: 18 month	
Programme type: Sixth Framework Programme	

Description:

This project aims to identify the social, economic, legal, technological and ethical issues related to identity, privacy, trust and security in Ambient Intelligence (AmI). The third report, entitled Threats, vulnerabilities and safeguards in a world of ambient intelligence, discussed the issues of privacy, identity, trust, security and the digital divide, followed by a chapter on threats and vulnerabilities and a chapter on safeguards. The final chapter contains the recommendations and conclusions, which were specifically addressed to the European Commission, Member States, industry, academia, civil society organisation and individuals.

RFID is discussed thoroughly in this report as one of the enabling technologies which can be used in AmI applications. The aspects of privacy, identity, security are discussed for RFID as well.

The description shows RFID-related security to play a minor role in the research projects. The review of the basic descriptions of the other 38 projects did not reveal a relation with RFID security issues at all. Though this is of course not a strict guarantee that RFID security is totally absent in these projects, at least it shows that attention for RFID-security is hardly present.

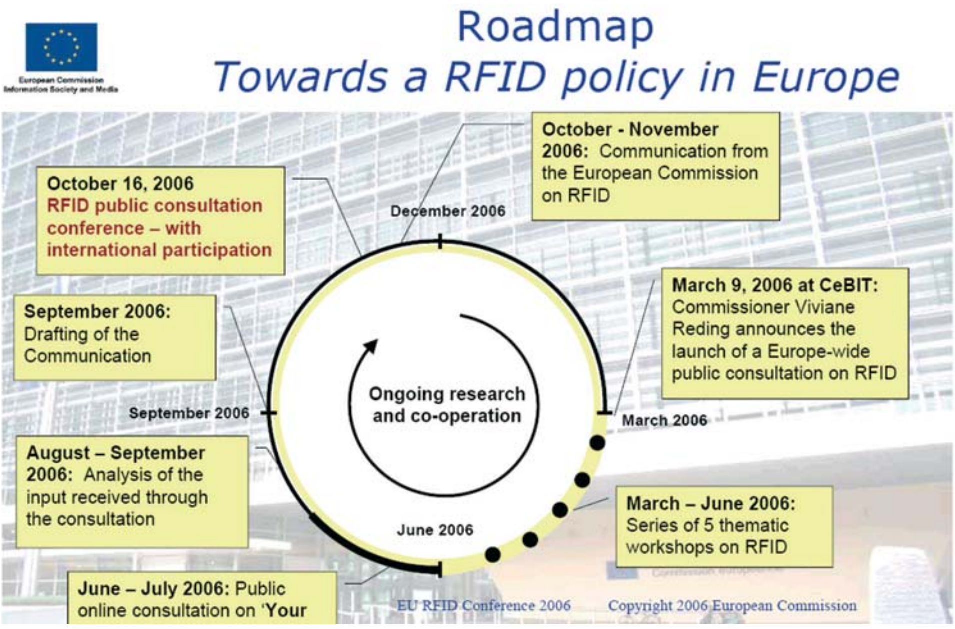
[87] URL: http:// cordis.europa.eu/search/

[88] http://ec.europa.eu/research/aeronautics/projects/article_3718_en.html

8.11.3. From research to policy

Besides these research projects in the Framework Programmes, the European Commission started a Consultation process with conferences, workshops and studies in the field of RFID in order to make a policy plan on the developments of RFID. Security is one of main topics that are investigated in these activities. A picture of the roadmap of the European Commission is shown below.

Figure 8-4: Roadmap: towards a RFID policy in Europe[89]



European Commission Information Society and Media

Roadmap

Towards a RFID policy in Europe

October - November 2006: Communication from the European Commission on RFID

October 16, 2006 RFID public consultation conference – with international participation

December 2006

March 9, 2006 at CeBIT: Commissioner Viviane Reding announces the launch of a Europe-wide public consultation on RFID

September 2006: Drafting of the Communication

Ongoing research and co-operation

September 2006

March 2006

August – September 2006: Analysis of the input received through the consultation

March – June 2006: Series of 5 thematic workshops on RFID

June 2006

June – July 2006: Public online consultation on 'Your

EU RFID Conference 2006

Copyright 2006 European Commission

This roadmap was presented on the final conference on October 16 in Brussels on RFID.

From 3 July to 30 September 2006, an online public consultation was held via "Your Voice in Europe" (EC, 2006c) on future RFID policy.[90] In total, 2,190 respondents (citizens, manufacturers, system integrators, academic and scientific institutions, public bodies and regulators, etc.), covering all the European Union Member States and a number of countries from outside the EU) answered questions about: RFID use; Privacy, Data Protection and Security; Standardisation and Interoperability; Frequency Spectrum; Research.

A large majority of all respondents (about two-thirds) have the opinion that the best solution(s) to eliminate or greatly reduce the concerns of security, data protection and privacy, which may arise from deploying applications of RFID technology, are the development of technical solutions allowing to disable RFID tags and/or awareness raising campaigns to educate consumers. More than half of the respondents report that some kind of legislation regulating RFID should be considered. A minority of respondents (14%) mention a preference for self regulation and best practices based on the 'Fair Information Principles'.

Almost half of all respondents have the opinion that privacy-enhancing technologies (PETs) should be made mandatory in RFID applications. A clear majority of respondents (61%) have the opinion that a RFID tag related to a product in a supermarket should be automatically de-activated at the point of sale. Other solutions, i.e. a removable sticker attached to the product itself and a "proximity tag" with a very short reading distance – are advocated by 46% and 40% of all respondents, respectively.

About half of the respondents regard the concept of limited distance "proximity tags" as a valuable (complementary) solution to preserve privacy.

[89] Source EC, 2006d

[90] http://ec.europa.eu/yourvoice

The strong majority of respondents consider a generic reading distance of up to 10 cm as acceptable for proximity tags. Personal data (e.g., e-passports) is generally placed in the shortest reading range. A majority of respondents see the need for appropriate security and privacy mechanisms to be taken by RFID application providers, while a large majority is concerned RFID-enabled monitoring of workers.

We may conclude that this interest as voiced by the people who contributed to the Consultation process can not be recognized in the European activities in this field up till now.

8.12. Conclusion

The security analysis of RFID delivers the following conclusions. The first set of conclusions refer to the overall risk analysis performed in section 8.1 till section 8.9. The second set of conclusions refers to the risk analysis performed for various application domains (section 8.10). The last set of conclusions refer to the attention for RFID security aspects in European programmes (section 8.11).

8.12.1. Conclusions of overall risk analysis

From a financial point of view, the most alarming risk would be the risk that has low costs for performing the threat and high costs for taking countermeasures. By analysing *Table 8-1*, this would be the risks of deactivating or detaching the tag because these are fairly easy to perform and countermeasures are more involved. Although much attention in the media is paid to eavesdropping on the air interface because of the privacy consequences of the consumer, from a security cost point of view indeed the vulnerability of the tag itself is an often overlooked aspect. Since tags are easily removed or destroyed, and countermeasures are costly, this can be seen as the weakest point of an RFID system.

At first sight it seems that a redesign of tags might be needed to overcome these risks. However, some important considerations have to be taken in mind:

- These are the results of a general security analysis and a rough cost estimate has been made. No conclusions can be drawn with respect to specific applications or scenarios. Each application or scenario would require its own more detailed and specific security analysis. The (seriousness of the) consequences of removing or destroying RFID tags depend on the application. Depending on the business case of the application, even a Common Criteria accreditation process might be worthwhile.
- The costs are not the only point of view. Also user convenience, user's acceptance, interoperability, etc. are important factors to take into account. This would require a case by case analysis.
- There is a trade-off between security and functionality. In general, the less functionality a (RFID based) system has the more secure it would be. It could be the case that certain security risks are taken for granted because the functionality involved is badly needed.

The RFID system is usually part of a larger IT system which includes the back-office. Since the security chain is as weak as the weakest link, we have to consider the entire IT system.

The security analysis shows that it is difficult to draw conclusions on the security of RFID only by observing an RFID tag and a reader. When regarding the tags and readers as part of architecture, better weighed conclusions can be drawn.

The systems that are used in the back office are not RFID specific systems. Much is known about the threats, risks, and countermeasures of such systems. The new and possibly more vulnerable systems are the RFID specific readers and tags. Especially since tags are usually less sophisticated elements that cannot contain many security mechanisms, it seems worthwhile to store the least possible vulnerable information in the tags. So from a security point of view, but also from an information management point of view, it seems right to shift as much data as possible from the tag to the backend. Only the essential elements, such as tag ID, should be stored on the tag itself. Another advantage of such an approach would be that less advanced tags can be used which are cheaper. Of course some additional investments could be necessary for the back office.

8.12.2. Conclusions of risk analysis per application domain

By considering different application areas, insight was created in the seriousness of the different security risks (Juels, 2006). Also the goal of the attacker varied over the different application areas:

- *Healthcare*: the most important risk for tagging medicines and blood bags is the risk of unauthorised modification of the tag. Not because the probability of occurrence is high, but because the impact of such an 'attack' would be immense and could lead to patients receiving wrong medicines. When RFID is used for access control of (mentally ill) patients, the most important risk would be the physical destruction or detachment of the tag which might lead to patients exceeding their allowed frontiers. When RFID is used for tracing doctors also the main risk is physical destruction or detachment of the tag, although it would probably not be the goal of the doctor to destroy it but it could be a little accident. In this case physical destruction of the tag would lead to doctors being less traceable in emergency situations.
- *Animal tracking*: the main threat in this application area is the physical destruction or detachment of the tags by the animals. The animals would then no longer be traceable in case of an infectious disease.
- *Public transport*: the most important risk within an electronic ticketing system is the chance that illegal tickets (i.e. tickets for which is paid less) are made. This could be accomplished by a replay attack after eavesdropping an RFID communication, or by unauthorized modification of the contents of a ticket.
- *Identity card*: the risk of unauthorised modification of the contents of the ID card is of course a very important risk. As with ID cards without RFID, adequate measures are taken to reduce this risk. The most important RFID specific threat for ID cards is the risk of unauthorised reading of ID cards. Therefore, an initial optical step is required before the ID card can be electronically read out.
- *Smart shop*: in this application area the most important risk is the loss of privacy of the consumer. There is an interesting debate going on about the deactivation of RFID tags when the customer leaves the shop. Producers want this tag activated in order to offer many new services, but consumers would like to have the possibility to deactivate the tag for privacy reasons.

It turns out that each specific application area has its own specific security risks. The risk of unauthorized modification of data on the tag is relevant, but (of course) only for rewritable tags. Some security risks do not pose a threat in the sense of loss of resources, but are just annoying, frustrating, or even a form of sabotaging the system. The risk of detaching the tag is an often underestimated risk, but for some application areas it's the most important risk. On the other hand, the risk of eavesdropping and consequently infringement of privacy seems to be overrated for most application areas although it's especially important in the smart shop application area (Garfinkel, 2006).

8.12.3. Conclusions on RFID security within European programmes

RFID is an actual research topic worldwide. In the academic world a broad range of security aspects of RFID is studied. However, the academic research is mainly focused on the more expensive smartcard solutions (e.g. electronic ticketing in public transport) and less on the logistic process (e.g. replacement of barcodes by RFID-tags). In the EU research projects (Framework Programmes), only two research projects (out of a total of 40 research projects addressing RFID) have a focus on RFID security aspects. This is in contrast with the results of a consultation report in 2004, in which the privacy and security aspects of RFID were considered as a fundamental enabler of smart wireless tag technology and in which various research needs were defined in the field of security. It is also in contrast with the results of the 2006 EU-consultation process on RFID which showed a primary focus on security aspects as one of the key enabling factors of RFID as well (in combination with privacy concerns).

Briefly, we conclude that Europe could further stimulate research on security of RFID, including the passive RFID tags which are less investigated in academic research, and including security architectures of RFID systems.

Part three

RFID case studies

Institute for Prospective Technological Studies

9. Searching the dynamics of RFID-practices

The broad analysis of the preceding chapters of this study has been used to enrich our understanding of the dynamics of RFID-practices. To understand drivers and barriers of RFID we have performed an in-depth study of the introduction of RFID in a number of practices. Much is already known about the use of RFID in the logistic process. Globally operating firms as Metro, Tesco and Wal*Mart all enforce the use of RFID within the logistic chain. This is not necessarily the best approach, given the investment costs suppliers have to make in realising compliance with the requirements of these firms. Firms tend to chose intermediate solutions (such as the Slap-n-Ship approach; see section 5.1) which may turn into a 'penny-wise pound-foolish' strategy: relatively cheap in terms of investments and required adaptations in the work process in the short term but probably no use in the longer term when the entire logistic process has to be revised. Though much can be said about the problems that logistic suppliers will face in introducing RFID, it was decided at the beginning of this study that the focus should be on other domains in which RFID can be used. This study should complement the view on drivers and barriers of RFID introduction by studying other application domains.

An initial survey of RFID application domains presented the following distribution of RFID activities:

Table 9-1: Distribution of cases over societal domains[91]

Domain	No. of cases
Retail, Consumer goods	400
Financial, Security and Safety	316
Passenger and Public transport	278
Leisure and Sports	228
Land and Sea Logistics, Postal	177
Healthcare	142
Manufacturing	135
Animals and Farming	81
Books, Libraries and Archiving	76
Military	43
Laundry	10
Other	4

Table 9-1 represents a broad class of cases, from initial pilots and field trials to full-fledged roll-outs of RFID. The table encompasses public and private domain applications. We used this table (and the more detailed table in Annex 8) as a starting point for the selection process.

[91] Source IDTechEx 2006 (visited 12 April 2006)

9.1. Selecting the appropriate cases

The intention of the study was to use case studies to analyse the dynamics of RFID implementation in a number of domains. We defined as overall objective that case studies should enable to identify:

- Drivers for the future RFID usage.
- Barriers to RFID introduction (technological, economic, social, legal).
- Perceived market potential for the European market.
- Distance in time to adoption.
- Stakeholders perspectives on drivers and barriers.

Moreover, the case studies should help to identify:

- Differences in stakeholder strategies due to variation in Member State markets.
- Perceived EU wide benefit.
- The role of the public sector in helping to achieve this benefit.

The first four items have been made part of the description of the case studies as these will be presented in the following chapters. The last three items have been taken up in chapter 15 (the policy evaluation).

Before choosing the final set of cases, we did a pilot study on Public transport, in which we researched the appropriateness of the following set of criteria:

1. Drivers and barriers.
2. Threats and opportunities.
3. Role of stakeholders.
4. Role of government.
5. Technology involved.
6. Role for Europe.

The next step was the identification of the remaining set of four cases. On the basis of desk research in which we studied a number of articles and reports dealing with implementation of RFID,[92] we identified a number of domains as promising from a European perspective. The analysis revealed a number of characteristics, which we present in Table 9-2.

Table 9-2: Characteristics of RFID application domains

	Technology applications	Actors	Issues
Health	Varied uses	Hospitals, patients, insurance companies	Quality, privacy, security
Cultural sector	Repository, loan, add. info	Libraries, museums, visitors	Privacy, data retention
Pharmaceuticals	Repository, logistics, counterfeiting	Pharmaceutical industry, healthcare institutions, patients, insurance companies	Counterfeiting, additional info, logistics of care-system
Digital rights management	Tracking, tracing	Variety (governments, commercial organisation of various kinds)	Appropriate use, privacy, new business models
Identity cards	Identification	Governments	(National) security, privacy, civil rights
Animal tagging	Tracking and tracing	'From farm to fork', governments, consumer organizations	Quality assurance, recall issues
ICT sector	Supplier of RFID applications	Chip developers; system integrators, consultancy firms, ...	Competitiveness of EU vs USA/Asia

[92] See (Capgemini, 2005), (Garfunkel & Rosenberg, 2005), (Gartner, 2005a), (Gartner, 2005b), (Gartner, 2005c), (IDC, 2004), (IDTechEx, 2005a), (IDTechEx, 2005c), and several issues of IDTechEx, Smart Labels Analysts, a monthly periodical to which the project team had access.

Figure 9-1: Expected diffusion of RFID tags, 2006-2016[93].

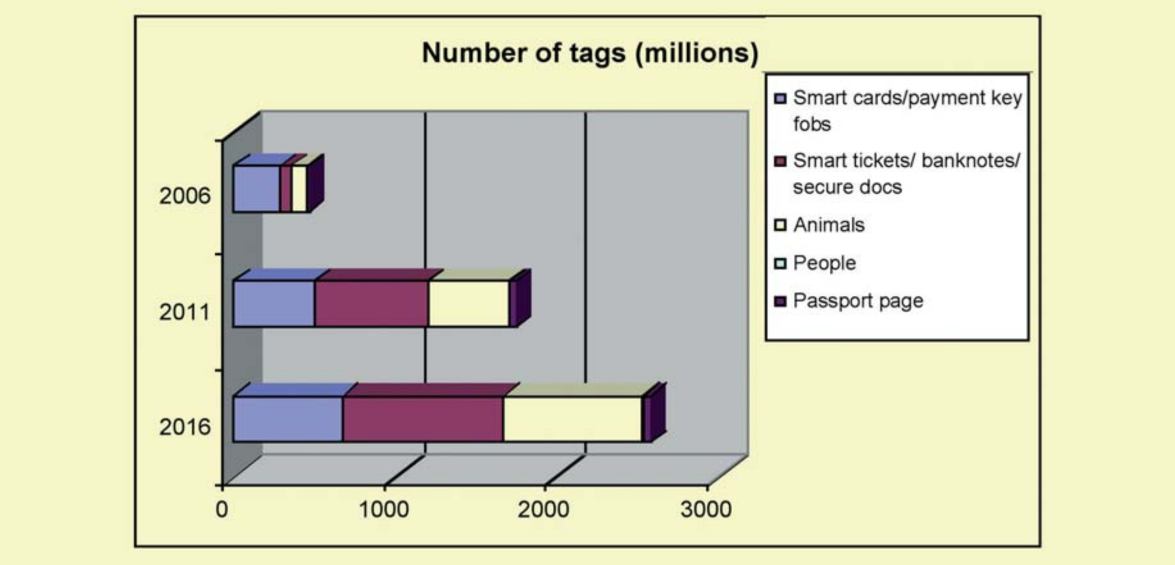
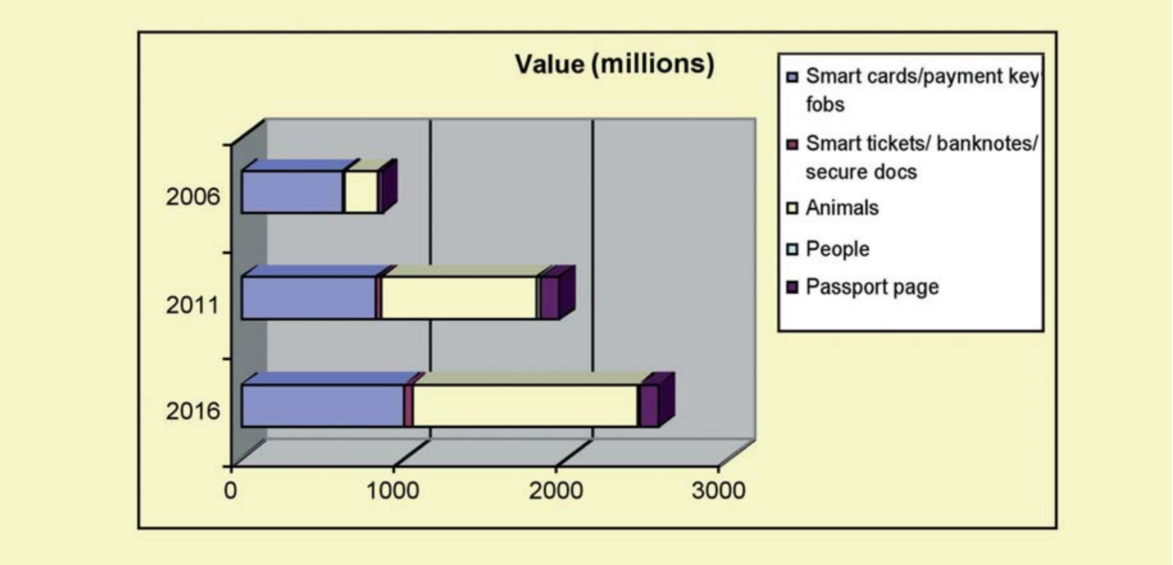


Figure 9-2: Expected value of RFID tags in different application domains[94]



From *Figure 9-1* and *Figure 9-2* we derived the importance of RFID for animal tracking and the importance of smart cards/smart ticketing. Smart cards and animal tagging represent a very interesting marketing value. Smart cards will be used in a broad array of application domains. The market value for passport tagging is less visible then for animal tagging but still offers an interesting starting point. The sources we used indicated a number of domains as niche markets (IDTechEx, 2005a):

- Prison and Parole
- Passports
- Live stock /Food traceability
- Healthcare
- Ubiquitous sensor networks
- RFID enabled cell phones

[93] Source IDTechEx, 2005a

[94] Source IDTechEx, 2005a

On the basis of this analysis we came up with the following selection of case-studies:

1. Animal tracking (major business segment, possible niche market for Europe, open market)
2. Healthcare (many small pilots, niche applications, combination of public and private investors, opportunities to follow people and items, a 'closed' market of vendors).
3. Identity cards (sensitive issue, example of law enforcement, privacy and security issues).
4. ICT industry (internal European market, innovative appeal, big European players on chips-market, leading edge firms?).
5. Public transport (major introductions; high impact, complex market, high investments).

9.2. Main conclusions from the case studies

The case-studies have been analysed bearing the following questions and issues in mind:

- What to expect from RFID: drivers and opportunities identified in pilots and projects taking place today?
- What experiences with RFID: what pitfalls and barriers can be identified?
- What (European) parties are involved; which interests do they have?
- What future issues can be discerned: what future technologies; what future drivers; what future business models?

We also paid attention to the issues presented in the previous chapters:

- What about the market potential visible in this application domain (direct benefits, return on investment, value chain, indirect benefits)?
- What about trust, user acceptance, employment aspects (reshuffling employment issues, training)?
- What about security issues (security throughout the value chain, sensitivity of the case for security issues)?
- What about privacy issues (what kind of data are collected, how are privacy issues safeguarded, compliance with privacy directives, etc.)?

The results of the case-studies are summarized in Table 9-3. In the following sections these results will be detailed.

Table 9-3: Summary of findings from the case studies

	Animal tagging	ICT sector	Identity cards	Healthcare	Public transport
Drivers	Law enforcement	Broad application area Extended functionality	Queuing time Terrorism Additional services US legislation	Efficiency Cost savings Anti-counterfeiting Improvement of care	Harmonizing ticketing system Travel information Queuing time Operational efficiency
Barriers	User acceptance High initial costs Training and education	Privacy and security Cross-platform interoperability	Role of citizens/consumer organisations Technical feasibility	Privacy (trade-off) Frequency interference (?)	Complexity of system High transition costs Complex actor environment
Opportunities	From Farm to Fork Improving animal welfare	European regulation of secure environment/ interoperable platforms	Harmonised national ID cards Extension of use Experience	Quality of healthcare New medical services	Increasing efficiency Additional services (e-purse) European experience
Threats	Alternative technologies Standardisation User interface	DRM: careful considerations not to overshoot regulations	Security Privacy Acceptance Function creep	No specific threats	Privacy Acceptance Technical failure Function creep

9.2.1. Animal tagging

Animal tagging is a potential billion Euro market. European legislation requires sheep and goat to be tagged as from 1 January 2008 onwards. Tagging is a major instrument in protecting human health and promoting animal welfare. Tagging enables a 'From Farm to Fork' approach in which all parts of the value chain are expedited with RFID tags. In case of outbreaks of infectious diseases, RFID enables a focused approach of infected animals (efficiency), prevents massive slaughtering of animals (animal welfare) and increases confidence for trading partners (economic incentives).

Drivers

The main driver for animal tagging within the European situation is legislation. Up till now only ovine animals (sheep and goat) and pets (transborder transport) require RFID identification. In case of sheep and goat RFID identification is obligatory as of 1 January 12008. Exceptions are made for countries with relatively modest sized herds of sheep and goats and for farmers with a relatively modest herd. This is the case for many of the states that have just entered the European Union and a number of Southern European countries.

Barriers

Tagging requires all farmers to be equipped with the appropriate hardware and software and expects all farmers to be skilled in working with the required computer programmes. In practice this is difficult to realise, reason to work with different modalities (such as centralised processing for a small group of farmers). Costs for providing the entire herd of one farm with RFID-tags may be high, in the light of modest revenues for the meat that sheep (especially lambs) produce. Training all professionals in the entire value chain is a costly affair, but is essential for beneficial use of RFID.

Opportunities

Having all animals equipped with RFID enables a quality improvement of the 'From Farm to Fork' approach, in which concerns of consumers and of quality control agencies can be reassured. Animal welfare can be improved (no need for massive slaughtering in case of infectious disease outbreaks). The economic risk of infectious diseases can be diminished and societal resistance against slaughtering practices can be taken away. Efficiency within the entire value chain is improved.

Threats

Animal tagging with RFID is surely not the only possibility. Though still in their infancy, DNA techniques are under development that offer similar advantages and may meet some of the problems raised against RFID tagging (loss of tags, difficult to re-use tags due to ISO agreements). The user interface of RFID equipment (readers, gates, tags) needs improvement; the readers for instance are not well suited to the practice in which they have to function, are difficult to understand, and require more than default user knowledge to deal with. The system needs to be developed in close cooperation with the user community in order to prevent massive rejection of the technology.

9.2.2. ICT sector

The ICT-sector itself has a lot of potential for introducing RFID in products, services and processes. In line with RFID developments, consortia are built to underscore the importance of two way interactive devices, in which devices function both as reader and as object to be identified. New business models emerge, such as the electronic purse with which one can order and pay for tickets simply by holding it in front of a poster. Other interesting applications refer to the possibility to enforce DRM-compliant behaviour: the RFID chip enables the authentication of appropriate uses of specific content, in whatever audio-visual format.

Drivers

A driver for RFID in ICT-products and services is the extended functionality it offers. This functionality is usually welcomed by users who consider extending the range of applications to be beneficial and who may be willing to accept the trade off with privacy and security issues that may come with these technologies.

Barriers

Notwithstanding the positive approach towards consumer attitude, privacy and security are serious concerns, especially in dedicated applications. Consumers may be deterred by possibilities of eavesdropping which might render the e-wallet vulnerable. These concerns may be difficult to counter, albeit that, as stated above, extended functionality may offer an interesting inroad. A second barrier is the difficulty of realising cross-platform interoperability. Lack of interoperability between platforms from different providers may lead to lack of sufficient use facilities for services which are based on these platforms, and to creating lock in situations.

Opportunities

Europe might take a front runner position in developing appropriate regulation to creating a secure environment in which interoperability has been taken care of. It also may position itself as a promoter of interesting novel applications that use the functionality of RFID and that promote new services, based on RFID.

Threats

Issues related to privacy and security, are a threat to the fast roll-out of RFID based services. Probably the biggest drawback is to be expected from a too rigorous arrangement of Digital Right Management issues. DRM is a delicate affair. Going for a too restrictive regulatory framework might force consumers to opt for illegal procedures. This should be prevented at the cost of diminishing returns of investment for the service providers. It is a difficult task to reconcile both perspectives in one framework.

9.2.3. Healthcare

Healthcare is a multibillion Euro market. Roadmaps indicate a market of more than 1.5 Billion Euro to be reached between 2012 and 2016. Benefits of RFID are to be expected in fighting counterfeiting of drugs. RFID may be used to tag medical assets such as blood bags and drugs, in order to prevent medical mistakes. Search for equipment, such as wheel chairs and infusion pumps, may become past history when an encompassing RFID-system is in place that indicates where medical equipment is situated. This may save many hours of unnecessary tracking down of medical objects per hospital and improve quality of service. RFID may also be used to locate personnel (doctors and nurses) in order to have the appropriate people at the right place in case of emergencies for instance, and to locate patients (for instance those suffering mental illness) and visitors (to give them access to parts of a building).

Drivers

RFID has the potential to improve efficiency, to reduce medical errors, to improve quality of care and to fight counterfeiting. Pilots project demonstrate the efficiency and quality gains which would outweigh investment costs within a few years. The business case for RFID is unambiguous positive in the case of hospital RFID systems.

Barriers

Notwithstanding the positive business case, issues of security and privacy will have to be treated with utmost care. Security is a basic asset of any medical system: no medical faults may be made due to failing technologies. Privacy could be considered as a negotiable concept in that offering personal data may improve healthcare and life saving operations considerably. Still, it needs to be treated cautiously, in order to prevent negative images. A final barrier may be the interference of RFID with medical equipment. Interference has not been indicated to be a problem yet, but with the emergence of an RFID-dense reader and tag environment, there is a need for a thorough analysis.

Opportunities

Efficiency gains in healthcare offer interesting opportunities for all European countries. The improvement of quality of medical services offers a strong incentive to invest in RFID-based applications and services. It may also offer new services, based on early and appropriate reconnaissance of needs of patients and personnel. Since healthcare still is a rather confined technological system, in which independence of countries is a basic asset, opportunities are present for all European countries. Europe should enable the dissemination of learning processes.

9.2.4. Identity cards

RFID-based identity cards form by far the biggest contract known so far: the Republic of China has ordered the production for over one billion of identity cards against a budget of more than 4.5 billion Euros. US-legislation enforces the use of biometric technologies in foreign passports of countries which are within its visa waiver programme. As of 26th October 2006 all newly issued EU passports have to be equipped with RFID tags to facilitate wireless access and authentication, thereby creating a big European market.

Drivers

An important driver for RFID based identity cards in Europe is the EU legislation which demands RFID tagged passports (e-Passports) which follow international standards. Other drivers are the increase of throughput speed at check-out points (though this speed will be reduced due to more intense control checks!) and the opportunity (in theory) to add services to the e-Passports (for instance, the combination with a driver's license or other official documents).

Barriers

Within Europe, concerns are raised against centralised database systems which would contain all data of European citizens and make these in principle easily accessible for central intelligence services. On the other hand, a centralised database would facilitate the protection of personal data: sensitive personal data would be stored centrally; an RFID would only need to contain an identifying number that refers to personal data in the database. The reversal of this argument – as brought forward by concerned citizens' organisations – is the increased opportunity to trace people via the centralised database as well as the fact that such a database would become a prime target.

Opportunities

The Europe-wide introduction of the e-Passport enables the fine-tuning of European regulation on passports, having all e-Passports provided according to the same standards. This increases the chances to create new services (such as including the driver's licence to the e-Passport) that may be implanted Europe-wide.

Threats

What may be seen as an opportunity (adding functionality to the e-Passport) is a threat as well. Extending devices with functionalities which were not foreseen is known as 'function creep'. This means that the original functionality of the e-Passport (identification and authentication of its holder) is enlarged with new functions that are not directly related to identification and authentication purposes. In combination with a centralised database, the information may be used for surveillance and surveillance functions. Though formally in line with the purposes of the e-Passport (fighting terrorism), this may be interpreted as misuse of data. Related threats are the infringement of privacy and lack of sufficient security measures to prevent unauthorised reading of the information of the e-Passport (a threat which is more realistic in case the data are on the e-Passport itself).

9.2.5. Public transport

The introduction of the Oyster card in London and the introduction of an entirely RFID-based public transport ticketing scheme in the Netherlands are both projects with an estimated value of 1.5 billion Euros. Public transport thus offers a major RFID-market. It is however a far from simple market. Public transport is usually a multi-actor game, combining the efforts of several independent public transport operators, public bodies that organise overview over the public transport market (transparency of prices, quality of services, competition) and consumer organisations. RFID-based ticketing has shown to increase boarding times in the Paris metro fourfold! There are many trials in many European cities with RFID-based ticketing schemes (Clermont Ferrand, Florence, London, Manchester, Paris, Porto, Rotterdam to mention a few). It shows that RFID-based ticketing offers value to operators.

Drivers

For public transport operators RFID-based ticketing offers an increase in operational efficiency: it enables a fine-tuning of operational processes, such as fleet management systems; it increases knowledge about travel patterns of passengers and the use of more than one transport mode (combining train and buses or metro for instance) making better alignment of services possible. Throughput of passengers in rush hours is increased considerably, as the Paris example shows. Introduction of RFID-based ticketing enables a harmonization of ticketing schemes in cities, regions or countries and between transport modalities (train, buses, metro).

Barriers

Public transport systems tend to be complex, multi-actor systems in which a variety of actors have to be aligned. Public transport is increasingly privatized, leading to pilots and trials that involves tens of organisations (in Paris the train company SNCF and the Metro-company RATF had to align 93 different private transport companies in the transition form the traditional Carte d'Orange; in Manchester 40 bus companies in 10 districts were involved). The costs to migrate from the traditional system to the new system are high, as is indicated by the size of the London and Dutch case. Arrangement of data ownership is difficult in these complex constellations.

Opportunities

RFID based ticketing offers opportunities to fight fraud (using public transport without ticket), to increase efficiency (fleet management, time schedules), to structure tariffs (alteration of old system in an economic more profitable one), and to improve services to the passenger (faster boarding times, better information provision, ease of use). Additional services can be the use of he electronic ticket as an e-purse, thus enabling extension of the scope of use to shops, rental of bicycles (in the Netherlands), special arrangements (holiday tickets all included) etc. Finally, for Europe, this domain offers possibilities to gather expertise by European vendors that can be used in pilots and trials worldwide.

Threats

Public transport is a complex system. Introducing RFID within the system implies that all actors have to be aligned and that crucial decisions about revenue sharing, tariff structures and the systems lay-out have to be made. Given the required investments, standards have to be open in order to increase competition. If these conditions can not be fulfilled, successful introduction of RFID may be threatened. Acceptance of this form of ticketing by passengers is essential. RFID increases passenger throughput considerably and is fairly easy to use. The precise lay-out of how tickets are to be priced occurs at the system backend. Questions emerge such as: will there be an entrance fee, will it be a debiting system (meaning that passengers will pay the maximum price of a ticket at the entrance and the precise price of the ticket is only calculated when they leave the train, bus or metro at some point, thus requiring action on the passengers). In the London case, the number of inquiries by the police intelligence services have multiplied since it became possible to track people on the basis of collected data about their travelling patterns. Commercial use of collected personal data may intrude privacy as well.

10. RFID in animal tagging

The market for using Radio Frequency Identification (RFID) in animal tracking is potentially huge. Alarmed by recent outbreaks of animal diseases (such as Bovine Spongiform Encephalopathy – BSE or 'mad cow' disease, Foot and Mouth Disease and the Avian influenza, of which the well-known H5N1 virus is dangerous for human beings) the call for widespread identification programmes to safeguard human health may easily be understood as an interesting business case for the adoption of RFID-based identification systems. Contemporary laws and regulations regarding the identification of animals offer the opportunity to use RFID in order to identify and register animals and to follow movements of animals (moving from one farm to the other, or from a farm to the slaughterhouse). This may function as an incentive for the introduction of RFID in animal identification. Another incentive is the pressure exerted by market parties who want to be able to trace back the origins of separate pieces of meat. This 'From Farm to Fork' approach interconnects different information networks: the information network used by farms to meet the legislative demands for full traceability of animals, and the information network used by the meat producing industries (from slaughterhouse to retail sector) The opportunities for RFID in animal tracking are identified to be huge, given for instance the outcomes of a forecast which expects in 2015 worldwide some 900 billion food items to be RFID tagged and over 800 million livestock to have more sophisticated, more expensive tags on (or in) them.[95] Within Europe, the livestock of sheep and goats exceeds the 100 million animals. Notwithstanding the opportunities RFID offers, it has to compete with traditional technologies, such as ear marking and tattoos. Bar codes on ear tags are as much an identifying technology as RFID.

As part of the overall study on 'RFID technologies: emerging options, challenges and opportunities', this case-study will answer the following research question:

"What barriers and pitfalls, and what drivers and opportunities can be discerned for the introduction and adoption of RFID in animal identification and tracking?"

Animal identification may be pursued for a variety of reasons, ranging from pure research (studying movements of animals) to economic and health reasons (being able to trace back the origins of meat when quality standards enforce this).

The case we will present below, will elaborate on the following issues:

- What to expect from RFID in animal identification and tracking: drivers and opportunities identified in pilots and projects taking place today?
- What experiences with RFID in animal identification and tracking today: what pitfalls and barriers can be identified?
- What (European) parties are involved; which interests do they have?
- What future issues can be discerned: what future technologies; what future drivers; what future business models?

In line with the issues that have been researched in a previous part of the project, we will pay specific attention to the following issues:

- what about the market potential visible in this application domain (direct benefits, return on investment, value chain, indirect benefits)?
- what about trust, user acceptance, employment aspects (reshuffling employment issues, training)?
- what about security issues (security throughout the value chain, sensitivity of the case for security issues)?
- what about privacy issues (what kind of data are collected, how are privacy issues safeguarded, compliance with privacy directives, etc.)?

[95] http://www.researchandmarkets.com/reports/c26259

This case-study will start with a short comparison of the overall distribution of RFID-cases between the EU, the USA and other regions of the world. A number of examples of animal tracking within Europe will be presented to give an indication of the kind of applications RFID is used for, the technologies used and the parties involved. We then will continue with a presentation of the European approach to RFID in animal tracking, as was formulated through the European IDEA-project (Identification Électronique des Animaux) and can be distilled from the EU-regulation on this topic. An UK pilot, commissioned by the UK Department of Environment, Food and Rural Areas, can be seen as the practical successor of the IDEA-project and delivers additional information about the European situation. A comparison with the activities in the U.S., notably the attempts to establish a National Animal Identification System, shows some interesting cultural differences between Europe and the U.S. which can be translated in drivers and barriers. The results of this case-study are presented in the last paragraph, in which the questions phrased before are dealt with.

10.1. Overview RFID in animal tagging

Table 9-1 presents an overview of the distribution of cases within the IDTechEx database. It shows that Animals and Farming ranks number eight.[96] The economic potential of Animal and Farming is considered to be high; according to IDTechEx it ranks third, after killer applications such as item level tagging and pallet tagging.[97]

In *Table 10-1* we present the distribution of the cases in Animals and Farming over Europe, the USA and a number of other regions.

Table 10-1: Distribution of cases in animals and farming over worldwide regions[98]

Region	No. of cases
Europe	24
USA	22
Australia	14
South East Asia	12
Canada	10
Africa	3
South America	3

Again, we want to emphasize that these figures only indicate an overall distribution.[99] It shows that attention for RFID in Animals and Farming is evenly divided between the EU and the USA, while Australia, South East Asia and Canada are following track.

In *Table 10-2* we present the distribution of cases within Europe. This table shows the UK to be the leading European country in terms of identified number of cases in the IDTechEx database. New Member States are absent in this table. But again, the table only presents part of the activities that are visible within Europe in the field of Animal identification and tracking.

[96] See rfid.idtechex.com/knowledgebase/en/breakdown.asp; visited 12 April 2006; IDTechEx warns to be cautious in interpreting the figures on face value. Not all cases are similar in scope and coverage. The market value of the cases differs considerably, ranging from a few thousand Euro to over a billion Euro. But overall, the table gives an idea of the relative attention that is given to RFID in the various application domains.

[97] See Figure 5-9 in section 5.4.2

[98] Source IDTechEx knowledge base, visited 22 June 2006

[99] Just to give one example: in the case-studies of Europe, we found one case that was twice registered. And we have information about a pilot in the Netherlands that started in February 2006 but is not yet included in the IDTechEx database. We have not corrected for these anomalies, but we have used the information as IDTechEx presents them.

Table 10-2: Distribution of cases in animals and farming within countries of Europe[100]

Country	No. of cases
United Kingdom	11
France	3
Portugal	3
Spain	2
Austria	1
Germany	1
Norway	1
EU	2

To get an idea of the content of the cases that are registered, we have checked all records on their relevancy for this case-study. A number of cases did not deal with animal identification but with other aspects in the logistic change (vehicles and pallets mainly). A few cases could be combined being very closely related or fully overlapping. Details on European animal identification and tracking are presented in *Table 10-3*.

10.1.1. Use cases

More than half of the identified cases deal with cattle and herds, three out of twelve are related to pets (dogs, pet passports) and three are different (keeping track of pigeons during a race and studying foraging strategies of bees and butterflies!).

10.1.2. Technologies used

Almost all cases deal with LF frequencies (125-135 KHz range), the only exception being the identification of sheep in the UK DEFRA (Department of Environmental Food and Rural Affairs, UK) which has a double frequency (LF and 13.56 MHz). The transponders used in case of the bees and the butterflies did not use an RFID-chip, but are based on reflections of radar waves (harmonic doubling) to identify the bees and butterflies.

10.1.3. Application area

Except for one, all uses are directly related to identifying an animal by means of a unique number. In one case (animal care, pets, UK) use of RFID is directed at measuring temperature.

[100] IDTechEx knowledge base; visited 22 June 2006

Table 10-3: European cases animal identification and tracking.[101]

Description	Tag	system	application	project	benefits
Animal care,	-	interrogator:	Animal	roll-out	Disease control
pets UK		Digital Angel (US)	temperature		
DEFRA, sheep UK	LF (125-135 kHz); 13.56 MHz	interrogator: various integrator: ADAS (UK)	Sheep identification	trial from 2004	Cost reduction Data capture Speed
FEVEX tracking cattle Spain	HITAG S IC 2 kbit memory, Philips	Neoris (Latin America, Spain)	Cattle	roll-out (complete)	Cost reduction Data capture Traceability
Iberian Pig Spain, Portugal	LF FDX-B glass transponder 64 bits				Cost reduction Integrity of supply Traceability
Lionor Poultry, France	TagSys	interrogator: TagSys integrator: Athelia Solutions	Meat conveyances	roll-out (complete)	Cost reduction Loss of conveyances Speed
Merial Pet, France	LF	tag+ interrogator: Digital Angel	Pet tagging	roll-out (on-going)	Safety
Pet Passport, UK			Pet Passport	roll-out (complete)	
Pigeons tracking, EU	LF	tag+interrogator +integrator: Deister Electronics	Homing pigeons	roll-out (on-going)	Accurate race timing Identification
Dogs, Portugal	-	tag+ interrogator +integrator: Digital Angel	Pet tagging	roll-out (on-going)	Legislation compliance
Bee and butterfly tracking, UK	radar transponder	Rothamsted research	Studying flight path of bees; studying foraging strategies of butterflies	roll-out (complete)	Research
RSPCA Animals, UK	LF; EM-Marin chip	tag: Sokimar			Identification
Smorfjord, Reindeer Norway	LF	tag+Interrogator: Jojo Automasjon integrator: Reinkjottspesialisten	Reindeer	trial (on-going) since 2001	Cost reduction Efficiency System automation

[101] IDTechEx knowledge database with case studies; visited 22 June 2006

10.1.4. Project

Most projects described are already in place. Only one describes a trial. All the other projects are roll-out schemes.

10.1.5. Companies involved

The US-based Digital Angel (the former Destron Fearing technologies) and its EU distribution partner Merial is present in three out of twelve cases, taking care of the entire RFID system (tags and readers). Philips as supplier of chips is mentioned once (its HITAG S IC chip) and in six cases a variety of European vendors and system integrators are mentioned (RFID system: Deister Electronics, Jojo Automasjon, Sokimar, TagSys; integrator: ADAS, Athelia Solutions, Deister Electronics, Neoris and Reinkjottspesialisten).

10.1.6. Benefits

Cost reduction is mentioned most often; other benefits are traceability, speed, efficiency, data capture and some specific benefits such as legislation compliance, disease control, accurate race timing and (reduction of) loss of conveyances.

10.2. Illustrative examples

Table 10-3 demonstrates a number of interesting examples of use of RFID. To track the homing of pigeons and enable a clear decision on racing times, Deister Electronics has developed the Unikon system.[102] Unikon consists of a clock to register the pigeons and an RFID reader and tag system to identify and register departure and arrival times of pigeons. The RFID reader can detect two pigeons per second, and can be connected to the clock module (the base station) by a cable or can be read out at a distance (up to 300 m). Deister claims to be market leader in the time racing equipment for pigeons and has selling points for Unikon in 25 countries world wide.

Rothamsted Research in Hertforshire, UK has used radar transponders to enlarge the distance to track butterflies and bees in their foraging strategies.[103] The transponders were tiny, did not weight more than 12 mg and enabled the researchers to track the motions of the bees and butterflies over a distance of approximately 900 metres. It enabled to study the imitation behaviour of recruit bees who were informed by a scout bee about places to go to and the strategies butterflies used for identifying foraging hot spots. These experiments were based on the reflective capacities of small transponders to identify and track separate bees and butterflies.[104]

An example of a different kind is formed by Lionor Poultry, a French specialist in poultry slaughter.[105] Lionor Poultry changed from cardboard containers to more expensive plastic crates. Crates were identified by bar code technology. Loss of the plastic crates exceeded 25 per cent per year and rotation time was very high with 21 days. Lionor decided to replace the barcode with smart labels which were moulded into the crates. The approach was robust and showed clear benefits: the rate of loss dropped from 25 per cent to less than 2 per cent, and the rotation rate went down to 11 days. Lionor claims that return on investment was achieved in less than two years.

10.3. EU activities in animal tracking

A number of European research projects have been undertaken that were directed at studying the specific requirements of an RFID-based identification scheme. The first research project mentioned is the FEOGA-project on “Electronic Identification of Farm Animals Using Implantable Transponders” (CCAM 93-342).[106] This was a one-year project carried out in 1993-1994 by institutes in Spain, Italy and Portugal. Its objective was to evaluate the possibility to use existing technologies for electronic identification in livestock species that received subsidies from the EC. The project focused

[102] http://www.deister.com/content/english/ident/sports/unikon/index.htm (visited 29 June 2006)

[103] *http://www.rothamsted.ac.uk/corporate/PressReleases/WaggleDance.html; http://oldweb.northampton.ac.uk/aps/env/lbrg/journals/papers/TrackingButterfliesCant2005.pdf#search=%22radar%20transponder%20rothamsted%22* (visited 6 September 2006)

[104] Communication with Mr. Alan David Smith, Rothamsted Research, Harpenden, Herts (29 June 2006)

[105] http://rfid.idtechex.com/knowledgebase/en/printcs.asp?casestudyid=157 (visited 22 June 2006)

[106] See: http://idea.jrc.it/pdf%20report/2%20antecedents.pdf, p. 1

on where to insert glass-encapsulated transponders subcutaneously and the consequences of the insertion (breakage, losses, migration distance, easiness of injection, animal welfare). A total of 5 000 sheep, 3 000 cattle and 2 000 goats were injected. The study showed the promise of an electronic identification system and recommended a follow-up for a large scale field trial. Due to the possible migration of the electronic identifier in the food chain, the armpit was not pursued anymore as a body-site to be used for the insertion of the RFID chips. The ruminal bolus[107] and ear tags showed to offer sufficiently safe alternatives.

The second project was the AIR2304 research project on 'Coupling active and passive telemetric data collection for monitoring, control and management of animal production at farm and sectoral level" (1995-98). Ten research teams of six European countries participated (Belgium, Germany, The Netherlands, Portugal, Spain and the United Kingdom) in a four year research effort. Main objectives were

- to complete and validate the findings of the FEOGA-project,
- to design a protocol for a large-scale experiment not only testing technologies but also elaborating an improved animal identification and registration system.

A total of 25 000 cattle, sheep and goats were followed. The results were promising. A cost-benefit analysis showed that net savings of 17% could be realised compared with plastic ear tags. The costs per animal were estimated at 5 Euro per year (presupposing the tagging of one million animals).

10.3.1. The IDEA project

The IDEA[108] project was launched in 1998 with a duration of 4 years (until 2001). It was part of a Commission Decision (98/562) which stated that "the IDEA project is designed to verify in real-life situations the reliability and advantages offered by an electronic identification system for the purposes of managing premiums and the veterinary monitoring of animals." To these objectives the utilisation of electronic identification for livestock management by farmers and Breeders Associations can be added.[109] The results of the IDEA project should empower decision making over an integral implementation of a European identification system on livestock. The IDEA project was coordinated by DG Agri, while JRC IPSC (Institute for the Protection and Security of Citizen) had formulated the tender proposal. Ten out of fourteen submitted proposals were selected, comprising a total of 370 000 cattle, 500 000 sheep, 29 000 goats and 15 000 buffalo. Six countries participated: France (three projects), Germany, Italy (3 projects) Netherlands, Spain and Portugal. Three different tags were used: ruminal boluses (620.000), electronic ear tags (230.000) and injectable tags (30.000).

Table 10-4: Overview of electronic identification devices used in IDEA project[110]

	Electronic ear tag	Ruminal bolus	Injectable transponder	Total identified
Buffalo		15 715		15 715
Cattle	139 807	159 430	29 982	329 219
Sheep	92 503	414 043		506 546
Goat	-	30 531		30 531
Total Identified	232 310	619 719	29 982	882 011

All devices had to pass specific tests developed and maintained by JRC-IPSC to receive the 'Certificate of Laboratory Acceptance'. The project developed specific guidelines for the various components of the information system: electronic identifiers and reading devices, tagging procedures, recording and exchange of administrative data, recovery of electronic identifiers, quality control of tagging and reading devices. Quality and performance criteria were formulated for the electronic devices. A total of 96 different devices (tags and readers) were certified during the trial.

[107] A ruminal bolus is a – usually glass – encapsulated RFID tag that is inserted in the stomach of an animal and that will remain seated there.

[108] Identification Electronique des Animaux

[109] See http://idea.jrc.it/pdf%20report/3%20IDEA%20project.pdf, p. 1 (visited 29 June 2006)

[110] Source: IDEA project results, chapter 4 table 4.1.2.1.1

The technologies used were HDX and FDX-B[111], compliant with ISO standards 11784 (specifying the information coding structure) and 11785 (specifying the reader-tag transmission protocols).[112]

The IDEA project resulted in a high number of detailed recommendations, in which the experiences with the tagging procedure, the information system, the recovery of IDs in the slaughterhouse, the possible losses of tags (which – in case of ear tags – increases over time and is significant), etc. are dealt with. We will focus on a number of interesting observations:

- IDEA considers training to be essential, especially for the application of ruminal boluses (death percentage of less than 0.02% at one hand shows ruminal boluses can be applied to animals at a very young age - younger than 20 days – but shows at the other hand that training is needed to lower the death rate which is still high compared to other tags – ear tagging and injectable transponders).
- Reading failures for electronic ear tags are highest with initially 0,63% but increasing to 2,3% after 14 months for cattle; in case of sheep and goats reading failures are close to 0,2% with a slight increase 1 month after tagging; injectable transponders and ruminal boluses show reading failures of – in the end – 0,3%, both for cattle and sheep and goats.
- Slaughterhouse Recovery of tags is high: 93% of electronic ear tags and 100% of ruminal boluses were read or recovered in case of cattle; in case of sheep and goats recovery was 100%; for injectable transponders only 80% was recovered while only 52% was successfully read after recovery for cattle.
- The IDEA project recommends a coding structure compatible with ISO standard 11784, which defines four digits for the country code, followed by a serial Individual Animal Code of 12 digits. This last part of the code may pose problems:
  - no differentiation is made between species; if different Authorities are responsible for distributing unique identification codes, this might cause problems;
  - the suggestion to include the local authority, responsible for the assignment and distribution of identifiers, into the code may pose problems; this requires the involvement of the ISO working group;
- Other issues to be dealt with is whether in case of re-tagging the same or another unique code has to be used; using the same means that the procedure is not ISO compliant; using different codes poses severe constraints to the database used.

The following overall conclusions were drawn from the IDEA project:

"The IDEA project has demonstrated that a substantial improvement can be reached for livestock identification by using electronic identifiers. It is the proper time to introduce electronic identification for cattle, buffalo, sheep and goats in view of establishing an improved livestock identification, registration and management system in the EU."[113]

A number of conditions to realise this conclusion have to be fulfilled:

- A clear and unambiguous legislation needs to be available taking into account the capabilities and constraints of the new technology.
- Guidelines and specifications need to be available at the EU level for implementation and use of electronic identification devices.
- A data dictionary and communication standards need to be available.
- Member States and the European Union need to develop proper technical standards for the exchange of data and the preparation, review and improvement (if needed) of the accompanying measures.

[111] HDX: half duplex, i.e. one-way; FDX-B: full duplex, i.e. two way

[112] These ISO standards are contested, also in the domain of animal tagging. See for instance the discussion on http://www.rfidnews.com/iso_11784short.html (visited 29 June 2006). The paper describes three flaws of ISO 11784/11785: 1) Inability to ensure unique ID codes; (2) Lack of manufacturers' accountability; (3) The problem of transponder performance.

[113] http://idea.jrc.it/pdf%20report/8%20conclusive.pdf, p. 1 (visited 29 June 2006)

10.3.2. DEFRA sheep identification

The UK Government of Environment Food and Rural Affairs (DEFRA) decided in 2004 to start a pilot with the electronic identification of sheep by means of using RFID. The contract for the three years pilot was awarded to the UK based ADAS, a consultancy organisation active in environmental and rural issues. ADAS has engaged two EID systems integrators, Allflex Europe Ltd and Earlsmere ID Ltd, as sub-contractors. The UK has launched a program to have the entire process of labelling and identification of sheep in compliance with EU regulations. According to these regulations, a strict information system has to be used in which sheep are tracked from birth to death by means of various tags. Movement of sheep over a distance more than five miles has to be registered. The EU regulation determines that[114]:

- double identification before six months of age has to be used; double identification may comprise of two ear tags or one ear tag and a tattoo, a mark on the pastern (for goats only) or electronic identifiers; as of 2008, one of the identifiers has to be RFID (if decided so by the EC in 2006)
- each holding needs to maintain an up-to-date register;
- each movement of groups of animals (herds or flocks) has to be accompanied by a moving document;
- a central register of all holdings or a computer database at national level is required.

The regulation is in force since 1 July 2005. From 2008 onwards, electronic identifiers are required (Commission decision was taken in December 2006[115]).

By starting a pilot DEFRA wants to assess what it means to start widespread tagging of sheep with RFID, in terms of user-friendliness of the equipment to be used, the kind of tags to be used, how to attach the tags to the animals (part of the ear tag, implanted or embedded in the stomach - ‘boluses’), the information architecture to be used, and what training and support requirements for electronic identification and electronic tracking systems is required. The pilot thus was much broader staged than many other trials which usually only focus on technology requirements. A total of 69 participants were chosen out of a list of 278 potential applicants (DEFRA/ADAS, 2005). The 69 participants were divided over a number of categories, depending on the kind of information to be collected and the network facilities provided to the participants: most of them (51) simply collected the minimum information to be compliant with EU directive; eight collected on top of the minimum information additional management information; three were fully paper-based and two provided a reference scheme for ADAS. The last five simulated a data collection bureau that might be active for a bundle of farms (third party provider of e-services).

More than 122 000 devices were used for tagging purposes over the range of possible technologies (FDX-B, HDX, boluses and tags). The pilot showed a rather low percentage of boluses to be applied. The European IDEA project had shown that boluses are to be preferred in terms of readability and recovery above ear tags.[116] These findings of the IDEA project did not lead to a preferred position for boluses in the UK trial. The reason probably was due to the fact that in case a bolus was used, an ear tag was required as well, to indicate that a bolus was used (DEFRA/ADAS, 2005, p7)! During the trial, the percentage of non-reading devices in case of boluses and in case of electronic ear tags was rather similar and ranged from 0.15 to 0.78% (and thus showed improvement over the IDEA figures). Reading equipment functioned pretty well during the trial and met market requirements (accuracy, speed of read, ability to segregate non-read or non-EID animals). As the report states “the results of the market trials were encouraging … and indicated the potential application of EID in market environments” (DEFRA/ADAS, 2005, p.8). Commercially available, ISO compliant equipment is available but the robustness of equipment needs to be improved.

[114] http://ec.europa.eu/food/animal/identification/ovine/index_en.htm (visited 22 June 2006)

[115] Implementing Council Regulation 21/2004, Council Regulation 968/2006 of 15 December 2006.

[116] Results of the IDEA project were that reading failures of boluses are 0,35% and constant over time, while reading failures of electronic ear tags are 0,63% and tend to increase over time to 2,3% after 14 months. Recovery and reading of boluses was 100% in the slaughterhouse and 93% for electronic ear tags.See previous section. http://idea.jrc.it/pages%20idea/index%20of%20final%20report.htm (visited 29 June 2006)

The internet-based applications, needed for the data transfer of the farmer's PC to a central database showed to be sensitive to failure, leading to a possible compromise of the farm's database. The comparison with the paper-based approach showed the paper-based approach to work pretty well as long as only overall figures had to be registered (the four digit management number and not the full twelve digit individual number) while experienced workers were just as fast with a paper-based read out as with an electronically moderated read-out. In more complicated situations (high number of cattle to be registered in a short period of time) the project team expects electronic reading to be superior. The vulnerability of a paper-based system was demonstrated during heavy rain fall!

Contrary to the IDEA project, recovery rates of boluses in the slaughterhouse were only 81% overall (with differences between big and medium boluses). Abattoirs are very much aware of the costs that will have to be made to meet EU regulations (the costs of adding safety measures that have to be taken in order to prevent boluses to enter the food chain, for instance). They are a bit hesitant in adopting the EU regulations to the full and want to comply at the lowest costs possible. These concerns are shared by the Livestock Auction Association. This association points at the costs that have to be made to taking care for both EID and non-EID animals in one and the same market. This will evidently lead to higher overall costs for the auctioneers. Accuracy of reading and speed of reading showed to be fine in a proof of principle test of reading 1.200 sheep within an hour.

The user friendliness of the systems were scored as being unsatisfactory: too complicated, too slow, too unreliable. Most of the comments concerned the back end database system; the evaluation of the RFID equipment (tags and readers) was more satisfactory. Notwithstanding this judgement, it was generally accepted that a paper based system was not a real alternative. A big percentage of the farmers felt however that one should not attempt to create a system in which sheep are tagged individually but instead should focus on herd identification and movement. After all, sheep are often treated as a flock, not seldom from cradle to the grave.

The assessment of the cost-benefit ratio is very much dependent on the position in the value chain. Many actors in the value chain expect to be confronted with higher costs (farmers, auctioneers, slaughterhouses) which will be very difficult to pass on to the consumer. Farmers have to invest in equipment, in training, in transferring data to control institutes. Auctioneers and slaughterhouses will have to invest as well, while it remains uncertain whether the additional individual information will lead to any additional advantages. Advantages may be the opportunity for streamlining digital reports to public authorities. Information on individual sheep (or lambs) may be interesting in specific niche markets and of course when the information is needed in case of disease outbreaks. But it will be very difficult to make money with the data collected on individual sheep and lambs, while EU regulations will require sophisticated level of registering.

On the basis of the two year pilot, ADAS formulates a number of recommendations concerning the introduction of RFID in tracking sheep within the UK:

- Main conclusion is that the full roll-out of a complete, integrated EID system for every sheep producer in the UK in 2008 is not a realistic target. Still, important progress can be made if timely actions are taken.
- All engaged in the value chain 'From Farm to Fork' are served with clear guidance on how the European regulations will be applied, to be provided at the earliest opportunity.
- A level playing field needs to be realised in which none of the main actors has a disproportional disadvantage due to the introduction of EID.
- Government and industry need to cooperate closely to put structures in place to meet the Regulation under conditions of sufficient flexibility in order suit a range of circumstances.
- EU officials should be aware that no attempt should be made to introduce a 'gold plate' approach to the Regulation; this may lead to declined cooperation of sheep industry, and to sheep farmers given up sheep farming.

- The legislative framework set should be as basic as possible to comply with the regulation.

- Industry considers 2008 to be too early for a fully operational and effective National Register Database. A more extended approach covering periods of five years with realistic ambitions and milestones is recommended.

- Though in the end a paper-based system will have to abolished, in the intermediate period one should look for fruitful combinations between electronic and paper-based record keeping. This might give non-literate sheep farmer some time to get acquainted with the requested IT-skills. Given the age profile of sheep farmers, this is considered to be a particular concern.

- Industry needs to be informed about the implications of the Regulation at greater cost and with greater intensity than today. A survey showed knowledge with the new Regulation to be only modestly available: half of the sheep industry did not know what was going to change. Given the prevailing scepticism regarding the full traceability of all individual sheep special attention needs to be given to the rationale behind the regulation.

10.4. European legislation

Within Europe, several regulations are in place to promote animal health (and subsequently health of European citizens) by means of a strict system of identification and registration of bovine animals (cattle and buffaloes), ovine and caprine animals (sheep and goats), equine animals (horses, donkeys, zebras and their crossings), porcine animals (pigs) and pets. *Table 10-5* summarizes the main findings concerning these regulations.

Table 10-5: European regulations and directives on (electronic) identification

Animals	Regulation/Directive	RFID
Bovine animals	Regulations EC 911/2004; EC 1082/2003; EC 1760/2000	No electronic identification prescribed
Ovine and caprine animals	Regulation EC 21/2004	Electronic identification obligatory as of 1 January 2008
Equine animals	Commission Decision 2000/68/EEC	No electronic identification prescribed
Porcine animals	Council Directive 92/102/EEC	Reference to electronic identification is made
Pets	Regulation EC 998/2003	RFID is linked to Pet passport

10.4.1. Bovine animals

For bovine animals the Commission Regulation no. 911/2004 deals with ear tags, passports and holding registers for bovine animals. Objective for the identification and registration of bovine animals is[117]:

- “Localisation and tracing of animals for veterinary purposes, which is of crucial importance for the control of infectious diseases;

- The traceability of beef for public health reasons;

- The management and supervision of livestock premiums as part of the common organisation of the market in beef and veal.”

With respect to ear tags, the regulation states there should be two ear tags. The first ear tag is fully described, both in information content and in materials to be used for the ear tag, the second ear tag is relatively free, given specific requirements. No mention is made to electronic identification techniques. Each bovine animal needs to have a passport that enables the tracking of the cattle in case of diseases (BSE, for instance). Specific articles deal with very young bovine animals (calves) and with the position of the New Member States. No mention is made of the specific forms in which the passport should be available. Each holding has to keep a register that contain a specific list of information (minimum requirements). The register is an electronic register that registers information on

[117] http://ec.europa.eu/food/animal/identificaiton/bovine/index_en.htm

the animals (date of birth, name of holding, movement of cattle transport date, information concerning the competitive authority checking the register).

A previous directive (1760/2000) mentions in article 4.7 that the European Parliament and the European Council shall decide on the possibility of introducing electronic identification arrangements, on the basis of a Report from the Commission. Notwithstanding the positive results of IDEA, the Parliament and the Council have apparently decided not to make electronic identification obligatory in cases of bovines. Regulation 644/2005 on Bovines kept for cultural and historical purposes on approved premises opens the door for an electronic identifier, either in the form of a ruminal bolus (article 3.1.d), or in the form of an injectable transponder "provided the animals identified in this manner do not enter the food chain." (article 3.2).

10.4.2. Ovine and caprine animals

The Commission Regulation no 21/2004 explicitly mentions the use of RFID for identification of sheep and goats. Similar to the identification procedure with bovine animals, each holding has to use two distinct methods of registration for goats and sheep. One means of identification is a traditional ear tag, containing an identification number of the member state where the animal was first identified (ISO 3166 compliant) and an individual code of no more than 13 digits. This individual code may bear reference to the holding of the animal and the animal itself. The second means of identification is an ear tag, a tattoo, a mark on the pastern (solely in the case of goats) or an electronic transponder, compliant with ISO11784 and 11785. Article 9.3 from the Regulation reads that "as from 1 January 2008, electronic identification (…) shall be obligatory for all animals".[118] A few exceptions to the electronic identification are made, for Member States in which the total number of ovine and caprine animals is 600.000 or less, or in which the total number of caprine animals is 160.000 or less, electronic identification may be optional for (caprine) animals not involved in Intra-Community trade.

Next to the introduction of electronic identification, the Regulation describes the characteristics of the holding register, the movement document and the computer database for each holding.

10.4.3. Equine animals

According to Commission Decision 2000/68/EEC horses, donkeys, zebras and their crossings do not require an electronic form of identification. The decision deals with the use of a lifetime number for equine animals, for veterinary purposes and in case these animals are used for food production.

10.4.4. Porcine animals

The Regulations for porcine animals (pigs) are roughly equivalent to the regulations for bovine animals. Ear tags and tattoos are the accepted modes of identification, each holding (farm, market, slaughterhouse) is obliged to maintain a register, and each of the Member Sates needs a computerised database at national level. Exceptions are made for holdings with no more than one pig.

10.4.5. Pets

The basic regulation for pets is EC 998/2003. Reference is made to public and animal health as objective for introducing this Regulation. It is especially the concern for rabies that has given rise to this Regulation. Article 4 regulates the use of electronic identifiers. It states that after a transition period of eight years, electronic identification will be the sole means of identifying pets. Important elements of the Regulation are the articles dealing with the movement of pets from third countries outside the European Union into the European Union. The struggle against rabies has profited much from the oral vaccination of foxes in the past decades, reason why countries such as England and Sweden have lessened their protective measures of keeping pet animals for 6 months in quarantine.

[118] Council regulation (EC) 21/2004. Establishing a system for the identification and registration of ovine and caprine animals and amending Regulation (EC) No 1782/2003 and Directives 92/102/EEC and 64/432/EEC.

10.5. Discussion of EU approach

Following the IDEA project there has been modest progress in Europe regarding the electronic identification of animals. Only in the case of sheep and goats and in the case of pets has the European Union decided to accept electronic identification as a means of identifying animals and keeping track of their movements, within European Member States and to regions outside Europe. The electronic identification and registration of sheep has added value above ear tags with bar codes or tattoos, due to the high agility of sheep and goats and large size of the herd (contrary to bovine animals which are very docile and are (in the EU) held in smaller herds). The electronic registration of bovine animals is yet in place and serves health and identification purposes.[119] Sheep and goats thus are classes of animals to which use of RFID may offer substantial advantages. The ear tags of pigs and bovine animals, which contain information on the Member State of birth, the farm to which it has been moved and identification information about the specific animal 'at stake', are considered to be sufficient identifiers for following the pigs and the cows 'from farm to fork'. The European-wide 'pilot' with the electronic identification of sheep and goats to have a very strong all-European spread (totalling to over 100 million individual sheep and goats) and to disseminate diseases more rapidly and more vehemently than pigs and cows may provide additional legitimacy for the transition towards a full electronic system. Philips expected in 2003 a transition period of three years to the obligatory introduction of RFID. With hindsight, this vision has shown to be too optimistic.

10.6. US approach to electronic identification

Within the United States the US Department of Agriculture wants to introduce a National Animal Identification System. The NAIS should contain references to the holdings that keep animals and to the animals themselves. The rationale for the NAIS is the economic damage that was incurred by recent outbreaks of animal diseases such as the Foot and Mouth Disease and BSE. This last disease, which recently manifested itself first in Canada in May 2003, let to a demand of Japan to have proof that beef shipped from the United States was not of Canadian origin (Becker, 2006; p. 8-9). Japan had been an important importer of US beef, purchasing over 35% of all US beef exports in years preceding 2003. This requirement of Japan complicated the deliberations of the US with Canada to open their own borders for Canadian meat. The attempt to introduce a separate document, upon request of the exporters, to guarantee the origin of the meat and cattle, showed to be in vein when the USDA[120] found the first case of a US BSE cow. Japan immediately suspended imports of US cattle, beef and related products. Only after two years of "often difficult" negotiations, the Japanese market briefly reopened in late 2005 for US beef from certified US farms. An international team examining the Canadian BSE response emphasized the need for mandatory ID. The absence of such a system contributes to extended destruction of animals. The U.S. cow with BSE was, by means of its ear tag, traced back to a herd in Alberta, Canada. Notwithstanding this successful tracing back, the U.S. did not succeed in finding the origins of 52 out of the 80 cows that, together with the BSE cow, had entered the United States. The risks that one of these 52 cows was also a bearer of BSE was considered to be extremely small. This was acknowledged by an international panel (Becker, 2006, p9).

A year before the BSE-case in the United States, the National Food Animal Identification Task Force was formed in 2002 to prepare a work plan for the development of a detailed animal identification system. In December 2003 the "U.S. Animal Identification Plan" (USAIP) was published. Key goal of the plan is "the ability to identify all animals and premises potentially exposed to a foreign animal disease within 48 hours of its discovery."(Becker, 2006, p. 5; Smith, 2005). According to the planning, in July 2006 all animals (cattle, sheep and goats, swine, small ruminants) should have been provided with a unique ID number. Shortly after the publication of the USAIP, the

[119] Personal communication Peter Laloli, project manager System Pilot Electronic I&R sheep and goats, Department of Food Quality and Animal Health, The Netherlands.

[120] United States Department of Agriculture

first case of U.S. BSE was discovered. This gave an extra impetus to the plan. The initial budget of the plan was approximately $30 million for each of the successive FY 2004-2006.

Notwithstanding this financial support, implementation of the National Animal Identification System (NAIS) has been "difficult and controversial". According to USDA, as of early 2006, 50 states, two territories and five tribal organizations were able to register premises, nearly 205.000 (approximately 10%) premises had been registered. In May 2005 USDA published a strategic plan for implementation of NAIS. This plan aimed at having NAIS standards accepted by stakeholders by January 2008 and required recording of animal movements by January 2009. Since then, the Government attitude towards the plan has changed considerably. The ultimate goal of the plan – recovery within 48 hours of all animals that might be involved in an outbreak of animal disease – remained as it was. The system should however be a privately owned system, with minimal interference by the U.S. government. Government should be able to access the database with information only on a 'need to know' basis.

The most recent developments are that U.S. government is opting for a federated system, in which U.S. government only has access to two so-called 'meta-databases'. One database contains a list of animals with their ID and the private data company or organization with information about the animal. The other database contains a list of premises with their ID and the private data company or organization with information about the premises (Pape et al, 2006). The architecture of the NAIS would enable a rapid response, by knowing which private organizations have to be contacted in case of an emergency. According to Pape and Smith, a rapid response is possible within the timeframe of less than 30 minutes and, in case of fully independent databases, no more than two hours, clearly within the limit of 48 hours, posed as one of the design criteria. To meet these rapid response requirements, an infrastructure has to be in place in which fully automated requests and responses can be sent around. This is not yet the situation in the U.S.

The approach of the U.S. Department of Agriculture has been a very cautious one, trying to avoid the suggestion the government wants to get a hold on private data. However, in May 2006 the House of Representatives still voted down a bill of $33 million which was requested for the implementation of the NAIS for financial year 2007 (Clap, 2006). Before agreeing on the expenses, the House wanted "a complete and detailed plan, including but not limited to proposed legislative changes, cost estimates and means of program evaluation." Since the main part of the NAIS will be hosted by private organisations, USDA is very reluctant in estimating the costs associated with having the databases developed and implemented. The National Cattlemen's Beef Association, which has declared being willing to host the private databases, supports the actions of the House of Representatives, referring to having the highest possible transparency in the construction of the NAIS as possible.

According to Pape and Smith, much of the recent turmoil is due to the confusion about the plans of the USDA. They view that – contrary to what is commonly believed – the NAIS is based on guarding the privacy of farmers and other private organisations. The U.S. government is only able to gather information in case of emergencies by setting out requests for more detailed information at the companies or organisations which keep track of the data on birth, movements and deceases of the individual animals.

Regarding the use of RFID as means of electronic identifier, the NAIS does not require having the information available through RFID. Though USDA considers RFID to be a technology that might speed up the process of registering and getting all data in the database, it is not prerequisite.

Many issues still are open for debate. Even very basic ones, such as which cattle should be registered. Should it be all kinds of species (cattle, sheep and goat, poultry), should it be only the more higher risk animals (dairy cows, breeding animals, older livestock)?

According to the original objective the scope of he NAIS is primarily the ability to trace back the origins of animal diseases such as BSE and FMD. In case a connection will be made to food safety, the NAIS should be mandatory and should be more extensive in its registration.

Costs are an important asset, in combination with the question who should bear them. A fully deployed NAIS is expected to cost $120 million yearly, of which tags account for almost $100 million! Opinions differ as to who should bear the costs. The Canadian cattle ID programme shows that RFID-based tags are approximately C$2,- each, while bar coded tags range for C$0,80 to C$1,60 (Becker, 2006, p. 6). With an extension of traceability, the costs will also likely rise. Coupling the yet separate systems of animal ID before slaughter and product tracking after slaughter might be beneficial from a consumer perspective but is costly.

10.7. Discussion

10.7.1. Pitfalls and barriers, drivers and opportunities

The overarching incentive for the introduction of animal ID is the ability to respond quickly on crises of animal diseases, such as an outbreak of Foot and Mouth Disease, the occurrence of BSE or the outbreak of Avian influenza. Destruction costs are high, and animal welfare is challenged in these instances. In combination with food safety, there is a need for a system that couples animal ID tracking with product tracking after slaughter. Such a system is not in place yet, neither in Europe nor in the USA. Incentives for such a system come from consumers and consumer organisations who are willing to pay for animal welfare and safe food. Within Europe, an extensive system of legislation by means of European directives and regulations is in place, regulating identification of the various species of animals. National computerised database systems are mandatory, adding up to a federated animal ID system in which each nation bears responsibility for its own national database system, including the inference of costs. Each holding is required to have its own database system, registering data such as birth and movement of animals. This database system enables back-tracking the location of animals and the possible routes of infectious and contagious diseases. A more extensive registration is required to enable back-tracking the food that is produced for animals (which might be important in case of BSE cases). This system is not in place yet.

RFID only plays a minor role in these registration systems. Within Europe, RFID is only obligatory in the registration of sheep and goats as from 1 January 2008 onwards, with a few notable exceptions meant among others to relieve the burden of a too fast transition for the new member states. Pets that will be moved from one country to another are also required to have RFID as means of identification.[121] The positive experiences with RFID, stemming from the IDEA project, have not led to a broad implementation and deployment plan for RFID in European livestock. For most livestock species (cattle, pigs, horses) identification is obligatory (usually in a redundant mode) but electronic identification is not mentioned as one of the means of identification. For sheep and goats the use of RFID offers added value due to the high agility and size of flocks and herds of sheep and goats, rendering traditional techniques such as bar codes much more difficult to exploit. RFID enables farmers to set up an identification and registration system comparable to those already in place with bovine and equine animals.

So, while opportunities are indicated – in terms of added value to the existing information systems, and in terms of market size of over 1 billion tags yearly for Europe – these opportunities are only seized in the case of sheep and goats. Larger farmers perceive opportunities to use electronic registration as means to improve their business processes and to increase efficiency and software vendors see opportunities to explain market share in this market segment and are thus eager to participate as well. Law enforcement supports and enhances this opportunity. We have found no incentives to introduce RFID within the next few years in other livestock species.

Barriers for the introduction of RFID in livestock are the relatively high costs of tags (a few Euro against a price of sheep and goats of a few Euro per kilogram meat produced), the absence of mature reading products leading to resistance at a user group who is relatively unknown to high tech ICT, and the absence of uniform and standardised information coding practices by software vendors and integrators, leading to lock in and to problems of standardization. Other problems relate to the fact that national Identification and Registration

[121] Of course, other motives may play a role as well to inject an electronic transponder, such as identification in case of pets getting lost.

systems are not compatible to each other, thus hindering transborder cooperation and communication.

A final pitfall that can be mentioned is the fragmented market of hardware vendors which obscures the possibilities for end-users and which, due to low volumes, puts up serious price barriers in reading equipment for the majority of smaller farmers.[122]

10.7.2. Actors

The IDTechEx database shows that Europe-based Philips is one of the producers of the animal RFID tags. In general, European companies act as system integrators. Producers of reader equipment can be found in Europe and the U.S. (Digital Angel being a major one). On the basis of available data it is hard to tell what the position of European vendors on this market is. Given the probable size of the market (many hundreds of millions of cattle, sheep and goats and pigs within Europe) specialisation in animal tracking may offer an interesting business proposition, given mandatory electronic identification techniques. In the Netherlands, for instance, management software vendors are the system integrators and act on behalf of the farmers with respect to ICT-related issues.

10.7.3. Costs

Due to the relatively high costs of the RFID system compared to the more traditional methods (especially bar-codes in ear tags) prescribing electronic tags requires clear added value to the traditional methods. Added value may be a better and water tight system which enables a better focused reaction to outbreak of animal diseases. Using ruminal boluses might be a way to diminish losses of tags or damaging tags that thus can not be read out anymore. Costs are spread all over the value chain: the farm, the market auctioneers and the slaughterhouse. Costs are expected to be high and may have consequences for the market position of farmers, auctioneers and slaughterhouses. The US case identifies costs for the tags to be over 80% of total system costs (including readers, systems and services). Identification issues may arise if Electronic Identification means are not taken care of, once the animal deceases. Due to the high cost of eID-tags/boluses with respect to the profit per animal, businesses will tend to resell these tags to be used in other animals, thus obscuring the identification purpose of the tag/bolus. Lifecycle policies for EID means have to be adopted to prevent this from happening.

10.7.4. Training requirements

The DEFRA study pays explicit attention to the need to train farmers and personnel of slaughterhouses and auctioneers in dealing with RFID. Training encompasses the ability to insert or inject transponders and skills needed to handle the electronic register. DEFRA has searched for a number of different solutions, for instance combining a number of small farms and having them served by a service provider. The study noticed that 90% of farmers required IT training. IT-skills varied widely over the farmers' population. The average age within the population is rather high, which is an additional reason for concern. It showed to be possible to train the farmers to handle the ID data and handle the farm-based PC. Transferring the data to the central database through Internet showed to be a major obstacle. The intensity of the training was high; in a complete roll-out of the RFID-system over the entire farmer population costs for this intense form of training would be prohibitively high.

10.7.5. Security and privacy issues

Animal tracking shows privacy issues to have decisive cultural dimensions. Within the European Union the introduction of RFID for animal tracking is mostly phrased in business economic and farm economic terms. Though smaller farmers, active on the grey market as well, oppose state interference and extended inspection capabilities of public authorities, overall the issue of having a national identification system is not questioned. Within the United States, state interference is suspect. The suspicion against too much government interference has led to a delay in initiating and installing a nation wide animal identification system.

[122] Personal communication Peter Laloli and Micheael van Beckum, two TNO-researchers involved in a recent RFID-tagging trial in the Netherlands.

Private companies (including farmers) do not want the government to get an insight in their private belongings. The reserve, shown by the U.S. department of agriculture by opting for a federated system in which the national government only creates a 'meta-database' and is dependent on the co-operation of the private data companies and organizations to collect the required information in case of emergency, has not led to a more beneficial attitude of farmers and meat organisations. These kinds of disputes have not been found to determine the deployment of identification systems within Europe. A much more cooperative attitude is found. We have not found any reference to privacy concerns for the European situation.

Security is not considered to be a major issue. Fraud with identification systems has to be ruled out. RFID may offer advantages over barcode systems that over time tend to become unreadable. Especially ruminal boluses may offer advantages: they are long lasting and are difficult to loose.

10.7.6. Future technologies

RFID by means of chips is not the only means of advanced technological identification. Alternatives are chipless RFID systems as have been demonstrated at the end of 2006. By means of conducive tattoos on the skin of cattle it is possible to identify them on the basis of radio frequency.[123] Other emerging alternatives are biometric identification techniques (iris scans) and DNA-markers. They may offer added value, for instance in identifying kinship relations and in providing information on quality characteristics of the meat of production cattle (DNA-markers). Though DNA markers are not as widespread as RFID, several companies develop DNA technologies to be used for identification of cattle and for providing additional information. DNA markers could create the bridge between animal identification and tracking and food safety.

[123] See http://www.theregister.co.uk/2007/01/16/rfid_tattoo/ (visited 24 January 2007)

11. RFID in healthcare

The widespread adoption of RFID technology covers almost every possible sphere of human endeavour. The analysis of the distribution of the various applications that are at the moment at an advanced stage (executive, pilot, technical trial) shows that most of the applications are in the Service sectors (60%), which also include healthcare (Politecnica Milano, 2006). One of the reasons which justify the adoption of such technology is the simplicity of use.

According to Gartner forecasts, healthcare and pharmaceutical industries will adopt RFID faster than other application domains: pharmaceutical industries are also encouraged by the Food and Drug Administration (USA) to adopt this technology in order to combat medicine counterfeiting. It is expected that this will result into a fast widespread tagging by 2007 (IDTechEx, 2005a).

According to the IDTechEx study "RFID in Healthcare 2006-2016" the global market for RFID tags is now around $90 million and due to the fact that object and people tagging will be more and more diffused in order to improve efficiency and safety, this market is expected to grow up to $2.1 billion by 2016. In the following *Table 11-1* the main uses of RFID technology in healthcare area in the next years are presented.

Table 11-1: Evolution of RFID use in healthcare[124]

Years	Up to 2004	2005-2010	2011 Onwards
Main uses	Error prevention of products (drug do se, corrects blood and treatm ent, mother/baby mismatch etc.). Patient tagging for error prevention. Locating staff/staff alarms. Locating assets	Error prevention of products now including autorejection of wrong luer connections and parts. Patient tagging for error prevention. Locating staff/staff alarms/tags that record incidents. Locating assets/speedy, acourate stock taking. Theft prevention. Cost control. Recording procedures (eg for defence of lawsuits). Drug trials compliance monitoring/prompting. Behavioural studies to optimise operation. Phamaceutica anticounterfeiting.	Error prevention of products. Patient tagging for error prevention Locating staff/staff alarms Locating visitors/visitor alarms virtual queuing Locating assets/speedy, accurate stocktaking Theft prevention Cost control Recording procedures (eg for defence of lawsuits) Drug trials compliance monitoring/prompting (taking drugs) Behavioural studies to optimise operations Pharmaceutical anti-counterfeiting Track and trace of most medicines, consumables and assets.

11.1. Description of cases

In this document a few cases will be reported to understand the issues that are addressed in the area of healthcare applications. One source of information is the IDTechEx Data base which collects a number of cases on this matter. In *Table 11-2* the distribution of the cases in Healthcare over Europe, the USA and a number of other regions is shown.

[124] Source: IDTechEx, 2005c

Table 11-2: Distribution of cases of RFID in healthcare[125]

Region	Number of cases
Europe	40
USA	86
Australia	1
South East Asia	18
Canada	2
Africa	2
South America	1

According to this table most of the pilots are carried out in USA, followed by Europe (UK is among the countries in Europe with more case studies).

Other cases are taken from a study carried out by the Milan Polytechic, Department of Managing Engineering, published in June 2006 (Polytecnic di Milano, 2006).[126]

RFID technologies have been used in a wide variety of cases; one distinction that can be made is that of considering the use of RFID applied to people and to things or animals. This distinction allows a better understanding of the characteristics of RFID technology to be used and the pros and cons of the adoption.

Among the several forms of RFID applications there is an emergent one which combines objects identification with people identification functionalities. This allows an optimization of project costs as well as new types of functionalities. As an example: tags are applied on trees in parks for monitoring the evolution, maintenance and status of the trees but at the same time they provide information services to users. In case of hospitals, RFID technologies allow the identification of patients and the identification of medical instruments or medications associated to the patient.

The description of case studies in healthcare in the document is done by grouping applications according to the following structure:

RFID applied to objects

1. Medication and equipment traceability
2. Service operation support

RFID applied to persons

3. Person identification in hospital environment; patients/elders localization/monitoring

11.2. RFID applied to objects: medication and equipment traceability

One of the most important issues that are currently studied everywhere and for which RFID technology seems to be a good solution is the **tracking of hospital assets**, instruments and medicines. It has been estimated that the costs of theft of equipment and supplies in US hospitals are about $4000 per bed each year.[127] This implies a total potential loss of $3.9 billions considering that there are more than 975 000 staffed beds. The traceability of medication is a big issue as well, relating to on one side the risk that patients get the wrong drug or the wrong dose and on the other side the problem of drug theft.

Another issue is that of *leaving objects in the body* after a surgical operation. Every 10.000 surgeries one object is left in the body, totalling to 1500 objects every year: This causes an increase of hospitals stays (four days added), with related costs, and risks of deaths (57 US deaths in the year 2000 were associated to this kind of problems).

11.2.1. Locating and tracking hospital equipment, US hospitals

Several US hospitals joined an asset tag trial with eXI Wireless, now part of the VeriChip Corpo-

[125] Source : IDTechEx 2005c

[126] http:// www.osservatori.net/

[127] http://www.rfidnews.org/weblog/2004/02/13/rfid-asset-tags-tested-in-22-us-hospitals/

ration, starting from February 2004, with the aim of finding a way of protecting, locating and tracking hospital equipment.

The project's objective was testing the Assetrac system[128], in order to reduce high costs due to both loss of hospital equipments and to loss of time spent by hospital personnel in looking for medical equipment.

RFID tags are supposed to be fixed to medical equipment in order to trigger an alarm whenever they are brought outside the designated perimeter or when the tag has been removed from the equipment itself. The Assetrac system has a graphical interface that includes the facility's floor plan. The system can direct staff to the vicinity of the asset they are looking for.

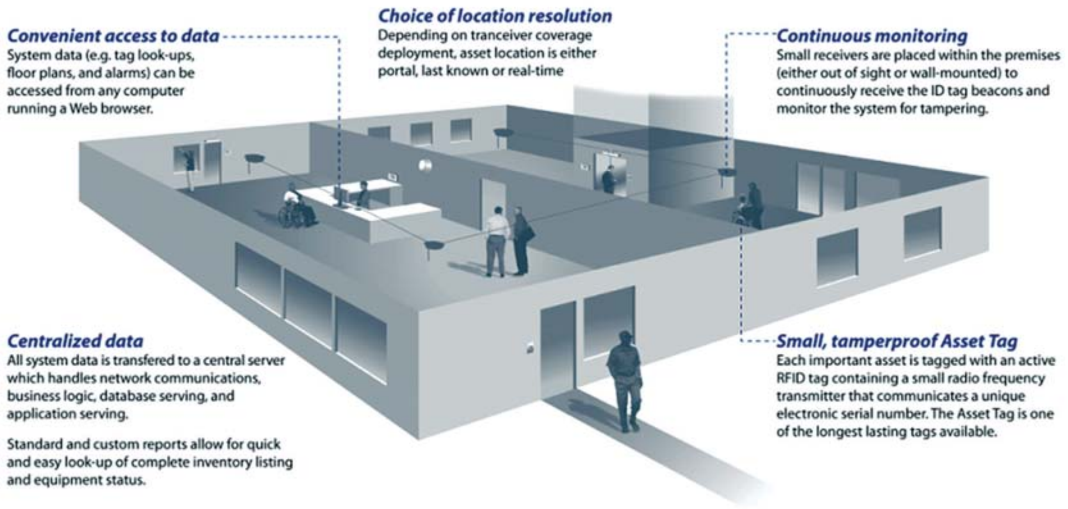
The Assetrac system is composed of two packages:

- ProtecPoint, which protects high value assets from loss by providing an individual, secure zone around doors where only authorized personnel can transport tagged assets without triggering an alarm.
- Assetrac Control 4.0, which can be used to manage assets as well as tracking them, creating custom reports for scheduled maintenance, asset utilization or inventory control.

In the following *Figure 11-1*, an example of the functionality of the Assetrac system, is presented:

1. Each medical equipment that needs to be tracked is tagged
2. A centralized server contains all the information about the actual status of the medical equipment and provides immediate inventory look-up
3. Information about tagged items is accessible through a web browser by any computer in the hospital
4. Small receivers are placed within the premises to locate the tagged equipments, to monitor the system and to update the centralised database.
5. Depending on transceiver coverage, information communicated about asset location is portal (that is the communication is done when the tagged element crosses a doorway), last-known (the object has been located after it crosses a doorway and enters a specific area in the department) or real time (transceiver coverage together with the triangulation provide exact location of the object).

Figure 11-1: Functionality of the Assetrac system[129]


Convenient access to data
System data (e.g. tag look-ups, floor plans, and alarms) can be accessed from any computer running a Web browser.
Choice of location resolution
Depending on tranceiver coverage deployment, asset location is either portal, last known or real-time
Continuous monitoring
Small receivers are placed within the premises (either out of sight or wall-mounted) to continuously receive the ID tag beacons and monitor the system for tampering.
Centralized data
All system data is transfered to a central server which handles network communications, business logic, database serving, and application serving.
Standard and custom reports allow for quick and easy look-up of complete inventory listing and equipment status.
Small, tamperproof Asset Tag
Each important asset is tagged with an active RFID tag containing a small radio frequency transmitter that communicates a unique electronic serial number. The Asset Tag is one of the longest lasting tags available.

[128] http://www.verichipcorp.com/content/solutions/asset_tracking

[129] Source *www.verichipcorp.com/content/solutions/assetrac*

Technology

The Assetrac uses active RFID tags that are able to generate alarms themselves.

11.2.2. Avoid leaving objects in the patient body, Stanford University Medical Center[130] (USA)

Funded by the National Institutes of Health and by a grant from the Small Business Innovation Research Program, a study has been carried out in Stanford using RFID technology to tag surgical objects such as tools or sponges in the operated patient's body. Although procedures are in place to track objects during surgery, such as counting objects before and at the end of a surgery procedure , occasionally supplemented with X-ray, errors do still occur and sponges or instruments are sometimes left in the patient's body (two-thirds of all objects left in the body are sponges). The risk significantly increases in emergencies, with unplanned changes in procedure and with patients that have a higher body-mass index, according to specialists.

In the Stanford study some patients allowed doctors to insert objects (tagged sponges) in their body. These were similar to those used in stores to prevent thefts. One surgeon was appointed to use a prototype interrogator to detect the sponges. It never failed to find them and the time needed was less then three seconds. So, in the trial the results seem interesting. The only problem was the size of the chips used: 20 millimetres. This size is too large and would need to be reduced to be practical on sponges and surgical instruments.

11.2.3. Tracking medication from pharmacy to patient, Jena University Hospital[131] (Germany, June 2006)

Jena University Hospital has started to test a system together with SAP and Intel to track medication from the hospital's pharmacy to patients in intensive care. In the first phase 24 people are involved in the trial; another 65 people may join in the next phase. The RFID technology enhances an already existing system; when electronic control of drug dispensing was deployed the medication errors were reduced; the use of RFID is meant to eliminate the remaining errors. Statistics show that one in 20 patients suffers from adverse drug effects and many of these cases could actually be avoided: by using patient data stored and recovered through RFID system it would be possible to discover drugs incompatibilities.

Technology

The RFID passive tag is placed on the individual dose of medication when still in the pharmacy; an RFID tag is also placed on boxes containing bottles of medications. All these data are read and stored in the computer system before the medications leave the pharmacy, together with patient information. Upon arrival at the destined hospital unit, the medicines are scanned again and information is updated in the computer servers before they are delivered to the patient. When the medication is given to a patient, information about the nurse administering it and type of medication given is stored in the patient wristband. This way medications and patient ID can be cross-checked every time instead of using paper lists like in currently used procedures.

11.3. RFID applied to objects: services operation support

The services operation support includes all the activities related to the use of RFID for improving operating processes in various application fields such as Public Transportation, Libraries and Hospitals. In case of healthcare the more interesting projects are related to cross-checked identification of patients and material/medications; tracking the patient at every stage of their treatment could help to avoid the risk of contributing to indirectly 72 000 deaths and to directly 40 000 deaths yearly (data relating to the UK, Dr Foster healthcare research group). In general the more frequent errors problems relate to:

- Giving wrong medication,

[130] *http://mednews.stanford.edu/releases/2006/july/sponge.html*

[131] *http://www.uniklinikum-jena.de/Willkommen.html*

- Administering wrong blood type,
- Mix up pathology sample,
- Operating/removing wrong parts of the body during surgery.

11.3.1. Blood transfusion monitoring at San Raffaele Hospital, Milan[132] (Italy)

The San Raffaele Hospital, situated near Milan, has about 1100 beds available. Its 'Transfusion medicine operation unit', which delivers over 15 000 blood transfusions per annum, has already developed three RFID projects. One project addresses *errors in the blood transfusion and handling process.* The risk of problems caused by an erroneous transfusion is estimated to be around 1 in 12 000 transfusions but experts estimate that the error rate may be much higher since many "near-miss" incidents are not even reported. Furthermore, nearly 80% of blood transfusion errors are due to bedside errors or labelling errors and many of those errors are human errors caused by staff people often busy carrying out multiple tasks simultaneously.

The project focus was on autologous transfusion, which is blood that is taken and then returned to the same donor; this choice was driven by the fact that in this case the blood bags remain within the same hospital thus allowing a better control of the entire process before applying it to a more extensive case.

The main objectives of the project were:

- eliminate labelling and bedside errors,
- eliminate paper forms as much as possible
- procedure (and introducing other potential sources of errors),
- provide a way to trace blood bags throughout the entire process.

Technology

HF technology (13.56 MHz) has been used: RFID tags were applied both on patients' wristband and on the blood bag. The patient was supposed to be equipped with a wristband (16 KB of memory) upon arrival at the Transfusion Unit.

The wristband tag contained information about the patient including a picture of the patient; the same information is recorded in the computer system. Before the patient's blood is put into the blood bag, the hospital staff member reads the wristband and copies the same information on a tag to be put on the bag. A cross check between the wristband and the blood bag is also done. Staff's badges information are then scanned to allow a third verification of the procedure. Reading and storing procedures are made through PDA (wireless enabled RFID reader) and through laptop PCs.

The transfusion is made possible only after all tags associated to patient and blood bags are read and all cross checks are made.

The use of bar codes in this case has proved to offer less performance quality for the following reasons:

- difficulty to read bar-coded wristband when dirty or wet;
- difficulty in reading bar codes hidden under sleeping patient, or a patient laying on an operating table.

Stakeholders

The actors involved in this project were: the technology providers, Intel, Autentica and Cisco Systems providing the computer systems, RFID tags and Wireless LAN and the users, which are the hospital personnel and the patients.

11.4. RFID for people identification and localization in healthcare

RFID technology is applied to people to manage the following situations:

1. identification of people within hospitals or care centres: in this case different situations using either passive or active tags are considered;

[132] http://www.cisco.com/global/IT/local_offices/case_history/rfid_in_blood_transfusions_final.pdf

2. identification and localization of sick people or elderly people at home: in this case usually active tags are used.

In the first situation passive tags are normally used to associate patients with specific medications, blood bags, surgical operations and so on; nurses or authorised personnel read the passive tag associated to the patient and cross check data with those stored into the computer system before performing any specific action. Active tags are used to monitor patients in limited areas (such as emergency department): normally patients wear a necklace with an RFID tag on it able to send real time information to doctors on the patient situation.

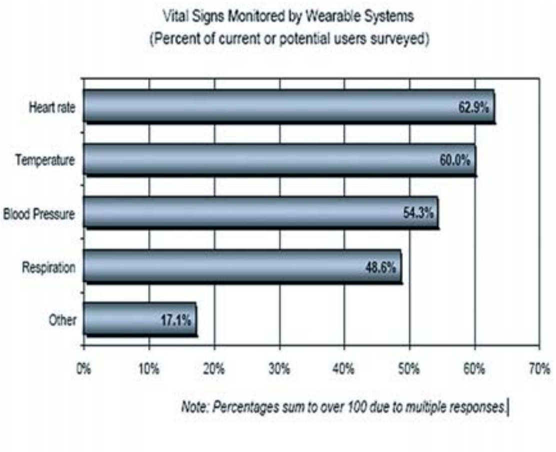
In the second situation, RFID tags can be used to localize and reach people who need help. Experiments have also been carried out during the Torino 2006 Olympic Games by CEFRIEL[133] to localize people with health problems in a crowd.[134]

The platform designed, called Mentor Me, provides a way to identify the position of a person in a given space. For example, a woman with a heart disease, wearing an UWB RFID tag can be localised while she is watching a hockey game in a crowded stadium. The tag continuously provides the coordinates of the person who can easily be localised on a map created for this purpose. If the person needs help, she presses a button on the sensor she has with her and immediately the position (chair number and row) is provided to the emergency staff together with the health files related to the person.

The application of tags or any other types of monitoring equipment to people encounters scepticism with the users who feel controlled and do not accept it easily. Besides, privacy issues have to be managed as well as the risk that monitored data could be captured by non-authorised people.

Research shows that willingness of people to be monitored increases since people realise that remote monitoring of specific vital parameters can actually save lives. A study from Venture Development Corporation (see Figure 11-2) shows the willingness of people to have some vital functions monitored.

Figure 11-2: Attitude of patients towards monitoring vital functions[135]



11.4.1. Monitoring chronically ill patients, Hackensack University Medical Center (USA)

A two-year collaboration between the Hackensack University Medical Center and the Horizon Blue Cross Blue Shield of New Jersey, the state's oldest and largest health insurer, starting in July 2006 will allow doctors to monitor chronically ill patients enabling emergency room physicians to access those patients' medical record electronically. FDA-approved microchips (provided by VeriChip Corporation) will be implanted under the patient's skin and provide immediate access to family contact information and information about the patients' medical histories.

The participants agree to having an implantable RFID-chip, the size of a grain of rice, placed under their skin. VeriChip calls the RFID-chip a personal health record module. The information on the module will include medical information from insurance company Horizon BCBSNJ's claim records, such as lab test data and pharmacy prescription information. This module emits a 16-digit number that links the patient to their electronic medical record when a special hand-held scanner is waved over it.

[133] http://www.cefriel.it/index.html?lang=en

[134] Innovation Gazette, February 2006 http://www.cefriel.it/contents/pages/attach/434/innovationGazette_n01_feb06_eng.pdf#search=%22torino%202006%20cefriel%20rfid%22

[135] Source: Venture Development Corporation

The pilot program will give Hackensack Medical Center physicians access to the member's electronic medical records and other vital information when response by the chronically ill patient, for instance in case of an emergency, is lacking. The content of the electronic medical records will be approved by each participant and include information about their condition, family contact information as well as lab test data and pharmacy information maintained by Horizon BCBSNJ.

Stakeholders

Technology provider: VeriChip Corporation[136] develops, markets and sells RFID systems used to identify, locate and protect people and assets. VeriChip recently began to market its VeriMed(TM) Patient Identification System, which is used to rapidly and accurately identify people who arrive in an emergency room and are unable to communicate. This system uses the first human-implantable passive RFID microchip, the implantable VeriChip(TM), cleared for medical use in October 2004 by the United States Food and Drug Administration:

- Service provider: Insurance company Horizon Blue Cross Blue Shield of New Jersey,
- The users: Hackensack University Medical Center.

Technology

The technology used is a microchip about the size of a grain of rice, containing a 16-digit identifier. The passive RFID can be implanted under the skin and personal medical information about the patient are then accessible through the tag ID in a password protected database.

11.5. Lessons to learn

In the following we present a few reflections drawn from the above described case studies.

11.5.1. Technological issues and problems

One of the issues which has been dealt with in healthcare case studies is that of *comparing the use of bar codes with that of RFID*. In general, it shows the use of RFID to be preferred over bar codes; data stored in RFID tags can be read much quicker and using RFID at system level is more cost effective even though barcodes are much cheaper than RFID. Concerns about using RFID relate to possible *interference* of radio waves with hospital equipment.

Considering the use of RFID in operating rooms as shown in the "Operating room of the future" (Massachusetts General Hospital[137]) one problem that has been highlighted by doctors and medical staff is related to what happens *if the computer system goes down*. In this kind of operating rooms information about the patient (name, weight, age, and procedure he/she is undergoing, body temperature, allergies, special needs, etc.) is displayed on digital screens; together with present medical staff, instruments and so on. But if the system goes down, an information technology expert is needed which complicates surgery.

RFID technology is considered to offer a good solution for tagging objects in the operating room to avoid leaving gauze sponges or other instruments in the patient body; the solution looks interesting but many small objects that are used for surgical operation still cannot be tagged due to the dimensions of tags.

11.5.2. Market issues

RFID is becoming a strategic weapon in reducing costs in the healthcare industry. The technology is easily integrated into a hospital's wireless infrastructure. With an RFID system in place, healthcare facilities can easily track mobile assets as well as staff and patients.

Healthcare facilities lose thousands of dollars worth of equipment each year and staff members spend countless hours searching for mobile assets such as infusion pumps, X-Ray machines, wheelchairs and patient monitoring devices. Furthermore also the high cost of renting expensive medical equipment is to be mentioned; it often happens that hospitals own more infusion pumps than licensed beds and normally rent more than needed to be sure that a nurse can immediately

[136] http://www.verichipcorp.com/

[137] *http://news.com.com/Tomorrows+operating+room+to+harness+Net,+RFID/2100-1008_3-5900990.html*

find one when it is needed, even if much of the equipment is left idle.

As a result, many hospitals are turning to RFID technology to keep track of pumps, as well as other expensive mobile equipment, including wheelchairs and patient monitors. According to a report by Spyglass Consulting, the number of hospitals using RFID tags to track assets will skyrocket from 10 percent in mid-2005 to 45 percent by the end of 2007[138]. Such programs promise to cut not only costs, but also the time that clinicians and engineers spend searching for equipment, and the time patients spend waiting for it[139].

11.5.3. Privacy issue

Privacy in case of healthcare is certainly an important issue to be considered. In case of use of RFID, privacy is mainly related to frequency transmission and to unauthorised access to people data stored in databases. UHF tags which can be read at a distance of ten meters are more subjects to unauthorised reading then HF tags readable from a distance of less than one meter. Tags normally used in this environment are passive and contain only an ID.

RFID technology can be used in hospitals to provide fast access to patients' records and a more secure delivery of medications avoiding provision of wrong medicines to people.

Even if privacy issues are well known and addressed some people are worried about the accessibility of their private data for instance because the tags associated to their person (wristband, implanted or other) can be read from a distance in a manner that does not allow them to know when this is actually happening or by whom.

11.6. Recommendations for European policy

In case of healthcare, RFID technology has been adopted for a variety of reasons including that of improving the care itself. It is in fact a *communis opinio* in the Healthcare environment that good improvements to healthcare can be provided by technology rather than by medicine.

RFID has been considered as the suitable technology for tracing products along the entire supply chain. The Ministry of Health in Italy has issued a decree-law which imposes every single medicine unit to be traceable starting from the production lines up to the pharmacy desk (through all the intermediate distributors). Other technologies have been considered to be more expensive than RFID.

A useful way to exploit RFID potentiality in healthcare could be that of providing European citizens with an RFID card containing medical information (blood group, allergies, etc). The time needed to acquire this information when a patient enters the emergency room or has to be immediately treated after a car accident could be limited. If ambulances and hospitals use a small wand to read the card, time to help patient will be substantially reduced.

Work has to be done to make RFID technology better known to people. The privacy issue is certainly a concern but when the advantages of the technology are clear and patients understand that RFID can save lives there is a chance that RFID will be more accepted. Of course this is not a problem to be solved by the technology provider or by the healthcare facilities. This knowledge is to be delivered by the government, and people must know that a tag might be associated to them as a standard procedure of the healthcare service.

Not all privacy issues are deemed to be as serious as others. For instance, in many situations access to a secure database is required (protected by tokens and other technical means) to be able to access personal data of patients registered in the database. The reader reads the ID registered on the tag and then accesses a database only if an authorised access is provided (IEEE, 2006). This approach prevents unauthorised people to accessing personal data (except for the person's ID number which is associated to the tag).

[138] http://www.extremenano.com/print_article/Hospitals+Save+Costs+Time+with+Wireless+Tags/162772.aspx

[139] http://www.extremenano.com/article/Survey+RFID+Use+in+Hospitals+to+Rise+Despite+Obstacles/158591_1.aspx

12. RFID in the ICT sector

ICT is a pervasive technology with information at its core and enabling communication processes anywhere, at any time with anyone (who has access). RFID is a technology, a product, and a service as well, that will become a pivotal component of ICT bridging the gap between atoms and information.

By providing a unique identifier to any physical object (it is foreseen that within the next decade any object resulting from a manufacturing process will be equipped with a tag as part of its production process, most likely based on RFID technology), and by allowing its readability at a distance, an information universe parallel to the physical one can be defined so allowing the creation of the so called "Internet of Things" (ITU, 2005).

The exploitation of the RFID in its various application fields, as already shown in other deliverables and in the literature, will create a significant explosion of IT platforms and basic applications (from main companies such as SAP, IBM, HP, Google, Amazon, WalMart, BT, Telecom Italia…).

The features provided by these platforms and applications – although leveraging on the RFID characteristics – are quite open to support any kind of identification technology. This will result in a booming of other identification systems, in their connection to these platforms and through them to the virtual world of the Internet of things.

BioIdentification (by proximity, by markers, at a distance through image recognition) will bring human beings into this universe (with related privacy concerns as well as the possibility to use advanced services). Soft tagging, associated to information (tags on software and on bits) will bring content into this universe. This content will be produced by the service providers but also, and even more importantly, by every individual.

Short Range bi-directional wireless transmission, the new NFC, will revolutionize our everyday life and will lead to using cellular phones not only for making phone calls but also for booking tickets for the theatre, for paying buses and parking, for sharing information and so on.

Having this in mind this document aims at describing some case studies related to RFID applications in the ICT world, although this will be by no means exhaustive. Basically any application of RFID (and functionally similar techniques) is intertwined with ICT. Therefore only a few examples are hereafter reported.

Some of the results presented in this document are taken from a study carried out by the Politecnico di Milano, Department of Managing Engineering, published in June 2006 (Politecnico di Milano, 2006). Case study examples are also taken from the IDTechEx Knowledgebase to which we had access during the course of the project.

12.1. Description of cases

Among the various application cases that could be mentioned related to RFID in the ICT area, we have selected the following examples: RFID used to monitor ICT assets such as data servers (section 12.1.1), cellular phones equipped with RFID capabilities (section 12.1.2) and DRM/PRM (section 12.1.3). In the following these are described and analysed aiming at highlighting issues considered to be important in the European perspective.

In particular, actions needed to accelerate the exploitation of the resulting information infrastructure built by the RFID will be indicated as well as ways to shepherd evolution in such a way that the adoption of RFID by individual players does not create disjointed subsets that would not allow exploitation.

12.1.1. RFID for asset management

Many companies are starting to explore ways to manage and track assets in the ICT department in order to optimize professional work. Among the work-related problems is that of having updated physical configuration information always available as well as the possibility to access updated information remotely so avoiding professionals' trips to the IT department just for the sake of checking that everything is on place.

RFID technology allows to automatically store and access all the information needed related to IT assets. It has been used by HP for the monitoring of its own data centres and now, once engineered, it is being sold to external companies. Some departments of Telecom Italia are also planning to implement a similar solution to keep track of the switching office modules.

Data center asset tracking (Palo Alto, USA)[140]

Hewlett-Packard announced that it has completed a successful test using radio-frequency identification to track servers in the data centre of Meijer, a supermarket chain with almost 200 retail and grocery stores. The HP solution was able to maintain an up-to-date configuration of all the hundreds of company's servers knowing when computers were moved from one location to another even within the same rack. The technology that HP used was then able to create a high-resolution view of devices in the data centre and provide historical information related to additions or changes of servers or other assets.

Modern data centres are built with hundreds of computing modules that can be easily substituted in case of failure as if they were drawers in a cabinet. The personnel that perform these operations should take care of recording each operation but, under pressure, the control is not optimal and the inventory and tracking of these modules becomes a nightmare. If the data centre is capable of automatically knowing which modules are slotted in which rack, then every movement can be recorded in configuration management systems.

This allows for a greater control over the ICT assets. In addition to automatic inventory, maintenance operations can be logged for each specific module identifiable with the tag. When a fault occurs in the rack, , it is possible to check for previous maintenance operations by knowing exactly which modules are in the rack and to easily spot the problem.

12.1.2. RFID in mobile phones

Mobile phone companies have started to equip cellular phones with the necessary technology to allow several types of payments[141]. Industry analysts predict that there will be almost 40 million contactless payment devices in use in the US by the end of 2006.

According to the information collected by IDTechEx, presented in *Table 12-1*, the number of cases only related to service payments (up to September 2006), divided by region, are:

Table 12-1: Distribution of RFID cases over worldwide region[142]

Region	Number of cases
Europe	13
USA and Canada	29
Australia	1
South East Asia, Japan	28

Applications that have started to become popular in Europe are those used within closed circuit; for example to pay drinks or services within resorts, or fitness centres, or for paying services (photocopies) in the library. Also payments on highways are considered within this area. Hereafter a few examples will be described.

When speaking of RFID applied and used through mobile phones, it is necessary to speak of Near Field Communication technology (see chapter 5.1 and 5.2). Jointly developed by Philips and Sony, NFC is a combination of contactless identification and interconnection technologies that enables wireless short-range communication between mobile devices, consumer electronics, PCs and smart objects.[143]

An NFC device can work under both active and passive mode. For active mode it acts as a reader and generates its own radio frequency field to identify and read smart card and tag

[140] *http://www.eweek.com/article2/0,1895,2035266,00.asp*

[141] *http://www.tml.tkk.fi/Opinnot/T-109.551/2005/reports/RFID.doc*

[142] Source IDTechEx knowledge database

[143] A brief description of NFC technology can be found in section 4.2.2.

while for passive mode it emulates a card or tag to be read.

To drive development and adoption of NFC, Philips, Sony and Nokia established the NFC Forum, a non-profit industry association which promotes implementation and standardization of NFC technology to ensure interoperability between devices and services. The NFC Forum has currently more than 50 members around the globe including MasterCard International, Matsushita Electronic Industrial Co, Ltd, (Panasonic), Microsoft, Motorola, NEC Corporation, Renesas Technology Corp., Samsung, Texas Instruments and Visa International.

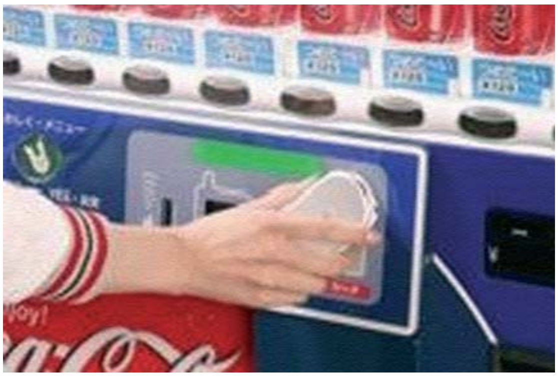
A number of trials around the world have been carried out to test NFC technology, also from the perspective of the user. It looks like the users are very positive: the idea of using the telephone also for many other functions seems well accepted by those who have tried it.[144] According to analysts AC-Nielson, for example, mobile payment is one of the most welcomed emerging mobile applications in China where over 80% of consumers are interested in the functional integration of city transportation cards and bank payment cards into a mobile phone.

CocaCola contactless payment (USA, Japan)

On the 27th of June 2006 the Philadelphia CocaCola Bottling Co, Master Card and USA technologies have decided to team together in order to equip 1000 CocaCola vending machines with payless terminals able to read RFID-enabled payment devices[145]. The payment terminals are the Generation Six (G6) e-Port terminals produced by USA Technologies. G6 terminal and access to the USA Technologies payment network will cost to Philadelphia Coca-Cola Bottling a monthly service fee of $140 each, plus a processing fee for each purchase made at each machine regardless of whether a mag-stripe or RFID card is used to make the payment. Consumers only need to put their Master Card PayPass-enabled card on the payment terminal to purchase the drink (see *Figure 12-1*).

Coca Cola Japan has planned to deploy 1000 CMOD2 vending machine by the end of the year and equipe 20% of their one million vending machines in Japan by 2008. The CMOD2 vending machines accept RFID-chipped wallet-phones payments and also collect data to be used by the company for CRM services. Machine can also be dynamically programmed to charge less in case of special offers.

Figure 12-1: CocaCola RIFD equipped automate, ready for NFC use



Nokia and Philips in NFC mobile phone trial (Xiamen City, China)[146]

Philips has launched China's first near field communication (NFC) trial together with Nokia, China Mobile's Xiamen Office and Xiamen e-Tong Card. The same type of commercial trials have already been completed successfully in the U.S.A., Germany, and Malaysia. Objective of the trial is to provide customers with secure electronic payments in restaurants, transportation buses, ferryboats, movie theatre or convenience store that accepts the Xiamen e-Tong card (contactless transportation card already used by 800,000 people).

Trial participants can conduct transactions with the swipe of their NFC equipped mobile phones (Nokia 3220) and, in addition to the standard E-Tong Card function, consumers can check their card balance and the last nine transaction records on their mobile phone display, access a built-in, WAP-based website to find out stores and venues that accept E-Tong Card. For all these reasons and for being perceived as a fashionable payment instrument, the NFC mobile phone has been well accepted by the trial participants who gave a positive impression.

[144] http://corporate.visa.com/md/nr/press291.jsp

[145] *http://www.usatech.com/company_info/news/usa_2006_06_27.php*

[146] *http://www.nokia.com/A4136002?newsid=1060346*

NFC technology is compatible with current contactless smart card infrastructure, so there is no need for significant upfront investment on NFC technology.

NTT DoCoMo Mobile Wallet (Japan)

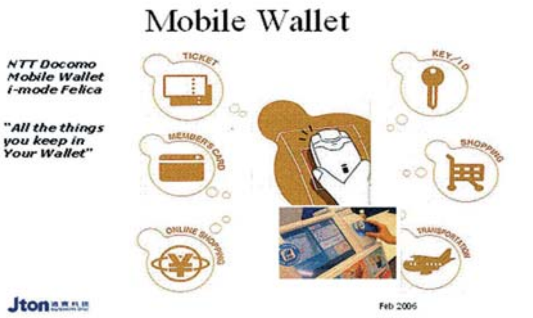
As of the 1st of April 2005 about 20,000 stores in Japan offer mobile wallet services: NTT DoCoMo already launched in 2004 new cellular models equipped with RFID Felica (by Sony) to provide this type of service. In May 2005 they announced the development of the 3G FOMA® 901iS series, five handsets equipped for mobile-wallet e-money, ticketing and other handy mobile smart-card functions.

The 901iS phones are equipped with security features that allow the phone to be blocked remotely by the owner. This series of handsets is expected to further boost the popularity of handsets equipped with FeliCa® IC card technology, which have sold more than 3.34 million units to date.

JTON MobiWallet(worldwide)[147]

The solution proposed by JTON, see *Figure 12-2*, consists of a combination of the SIM card contained in any cellular phone with a refillable RFID debit card. Normally in other solutions (see previous section on the NTT DoCoMo Mobile Wallet) the debit is done through the telephone bill tied to a specific telephone number; in this case the mechanism works differently. The RFID card is used to pay and a minimum amount of money is always to be maintained in the card. The cellular is in charge to keep this amount always available. Once the money is spent, the cellular phone is in charge of recharging automatically the card (with the pre-configured amount of refill) without any intervention from the owner of the phone.

Figure 12-2: Functionalities of JTON Mobile Wallet



Services accessible through NFC mobile phone (city of Caen, France)[148]

In the city of Caen a pilot has been carried out in order to test Philips semiconductor NFC chips applied to the Samsung D500 mobile phone. 200 people were supposed to use services accessible through the Samsung mobile phone and try RFID-enabled services. The services, developed by France Telecom's R&D include safe payments at shops (at the Galeries Lafayette, and other main stores in the centre of Caen) as well as parking. To make a purchase the customer simply waves the telephone in front of the shop terminal once the cashier has activated the reader.

Using the mobile terminal in its reader mode it was also possible to access tourist information in the historical part of the town as well as to get practical information such as the bus time table and film trailers.

Wine bottles tagging (Arnaldo Caprai Smart-Corq, Italy)[149]

A totally different application using RFID technology is the one carried out by the wine-maker Arnaldo Caprai. The pilot consists in using special polymer corks for wine bottles (Sangiovese di Montafalco) equipped with 13.56 MHz Philips transponders containing information (in the 1024 bit memory capacity) about the wine. Clients may visualize the information about the wine by using RFID readers such as those contained in mobile phones. There are still some problems at the moment, related to the bottling of the wine which may damage the transponder in the cork.

[147] http://www.jtonsys.com/

[148] http://www.rfidjournal.com/article/articleview/1943/1/1/

[149] Only references in Italian: http://www.contemporare.it/home.htm

12.1.3. RFID for DRM (Digital Rights Management) and PRM (Property Rights Management)

The problems related to digital rights protection over produced content, software, services and products are starting to be addressed by using RFID technology. Motion Picture Association of America estimates the money loss of US movie industry due to piracy at $3 billion annually (worldwide revenue).

Many companies consider the placement of tags on material to prevent unauthorized access as one possibility to protect their revenues. The issue is however not easily solved: the more complicated it becomes to make content legitimately accessible, due to protection procedures, the more motivated are people to crack the systems.

Another associated problem is considered dangerous by some field experts. RFID technology can be used for protecting products (Property Rights Management) so to be sure that products of a specific brand only function if equipped with original suppliers. An example is EM Microelectronic which plans to introduce RFID-enabled cartridges able to communicate identities and parameters to the printer in order to re-configure the printer accordingly.[150]

This mechanisms may be useful but – if not well regulated – run the risk that consumers buying a specific product suffer lock-in by a specific company forcing them to buy the whole set of accessories produced by the same company.[151] This could in principle lead to the situation in which we have to use a specific detergent in our washing machines; otherwise the machine will not wash our clothes.

DVD piracy protection (UCLA, USA)[152]

UCLA's Wireless Internet for the Mobile Enterprise Consortium (WINMEC), a research group based at UCLA, is working on a project, RF-DVD, aiming at developing software and hardware components for the digital right management of DVDs.[153]

The system, which is at the moment in a prototyping status, would embed DVDs with an RFID tag and DVD players with an RFID reader so that the tagged DVDs would play only in RFID-enabled players and only if the reader could authenticate the DVD's tag. In order to authenticate, the player would also need to link to some type of online network, similar to the EPCglobal Network, that would associate the DVD with a legal sale.

12.2. Drivers and barriers: lessons to learn for Europe

According to ABI research, there has been an important growth in the diffusion of RFID integrated circuits mainly due to contactless payment services, personal identification documents and so on: more than 565 million RFID integrated circuits were shipped in 2005[154] and the trend is not going to stop.[155]

We have not met strong barriers in the use of RFID tags in cellulars, either. RFID tagged cellulars are in general perceived by customers as an extension of the functionalities available in the mobile phone; customers do not react negatively to this asset in contrast to their reaction when discussing tagging people and therefore accessing to their personal private data. Contactless payments made possible by associating RFID to cards or mobile phones are nevertheless perceived by some customers risky since it may look like payments could be activated from a distance without the direct intervention of the owner of the card or mobile phone.[156] Even if this may seem a possible barrier for the diffusion of such a service, the technical approach might offer a starting point into explaining how the charging mechanism will allow an even more secure transaction.

On the other side the added value of having a device that enables people to make payments,

[150] http://www.emmicroelectronic.com/DetailNews.asp?IdNews=106

[151] http://www.freedom-to-tinker.com/?p=1052

[152] http://www.wireless.ucla.edu/rfid/research/

[153] http://www.rfidjournal.com/article/articleview/1589

[154] http://www.vnunet.com/vnunet/news/2163160/565-million-rfid-tags-shipped

[155] http://www.mtbeurope.info/content/ft608001.htm

[156] http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=1578&display=RFID

access theatres and cinema tickets or store an electronic flight boarding pass, may help in promoting the widespread diffusion of these applications.

European level action may be instrumental in this area, by promoting a *secure environment for sharing information*, and drafting regulation to disclose certain types of information that eventually would make the disclosure of production data more cost effective. In this area there is a mixture of ICT-related technology issues and the regulatory environment.

Proactive initiatives to explain to the public the benefits, and substantiating them, are most important to win the hearts of the consumers so that they can become a driving force towards the manufacturers to deliver information rich products. As far as DRM issues are concerned the problem is delicate: rights have to be protected but producers should be aware that complicated procedures might have the adverse effect consumers may be are encouraged not to follow the legal way and prefer the way of "buying" an unauthorised copy instead. Offering services at modest prices might be a better inroad to convincing consumers to behave legally than pricing the content. People are concerned about DRM and about PRM above all[157] since the freedom of buying our preferred products starts being threaten.

Europe is, and rightly so, very concerned on privacy and ownership issues, but should not lose sight from exclusion issues either. The former are the ones that can slow the evolution of services and adoption, the latter is the one that may swing biz one side of the Ocean or the other.

Google founders have declared in a meeting with investors in 2006 that they see their company as leading to dominate in Internet of Things in terms of searching capabilities. However this might be an understatement: whoever is going to control, or have pervasive visibility on this virtual universe will also have a platform that can be offered (at a price) to all businesses.

This scenario has to be seen under two opposite but colliding views.

The Google objective, if fulfilled, will lead to a situation where who has visibility, control and capability to offer services based on that virtual world will have a tremendous leverage on the market. In this situation it will be very probable that dominant parties (not just Google but also another few who will have managed to establish a set of indexing services) can lead to a lock-in of the market (the value proposition is so strong that the market will naturally tend to stay with these leaders).

At the same time we can expect that those enterprises, specially the smaller ones, that do not have the process capabilities and IT support to create products with an effective embedding of RFID (or functionally similar identification device) will not be able to become part of the virtual universe and since more and more business will be played at that level (to turn to the physical one only at the end of the value chain) these players will be emarginated from the global market.

A parallel issue is the one of fostering individual business and enterprises to adopt the specific technology that best suits their needs but, at the same time, to stimulate development of cross platform interoperability and the availability of terminals able to access the different technology since at the European level significant gains can only be made through a common reference environment where all goods and services can be indexed.

The availability of services leveraging on information provided by or pointed to RFID and the possibility of embedding them into proprietary offering ensuring the sharing of ownership rights (and related revenue) can prove a strong motivation for companies to adhere to open interfaces, and to enable other companies to access proprietary information made available through these open interfaces.

Examples supporting the soundness of this approach abound. Many products today, be it from Microsoft or Adobe, SAP (to a limited extent) or Apple/Nokia, open up their information interfaces to let other parties develop value added services. This in turns creates a higher value perception by end users who will flock onto adopting that product as much for the product itself as for the constellation of goodies that can be associated to it by accessing the supporting platforms.

[157] *http://www.freedom-to-tinker.com/?p=1052*

13. RFID in identity cards

The application of RFID in identity cards has to be analysed in relation to overall discussions around identity management. There has always been a demand for identity management. In the past, various techniques have been used to verify the identity of an individual in relation to specific actions, transactions, events or other purposes. Also the use of a biometric identification is not new. It has been used in history already for a very long time.

So, what is new in the discussion on RFID in identity cards then? New is the increasingly pervasive nature of identity management in our modern society and the motivations behind the application of these new forms of identity management. Also the fact that the technology is new and is not fully worked out in all its aspects raises problems.

On the one hand we have the discussion on the user benefits of identity management. Because this discussion is partly fed by those who have a vested interest in developing, implementing and maintaining applications, it is necessary to critically analyse the arguments which are used in this discussion.

On the other hand there are claims about defeating terrorism and organised crime. The terrorist events on 11th of September have of course brought this aspect to the foreground, but at the same time we should perhaps be realistic and see whether or not the claims are too ambitious.

Looking at the main actors in the debate, a push in the direction of the widespread introduction of identity management and identity management applications can be noted both from the political and the commercial sector. But also consumer privacy protection organisations play an important role here; some of the large consumer privacy protection organisations in Europe and the USA put large question marks on the necessity of the large scale introduction of identity management or at least on the conditions of implementing these identity management applications. They consider the wide scale introduction of identity management as a threat for vested democratic values in our society like person identity, personal freedom, privacy and protection against the misuse of information.

The application of RFID in identity cards should be placed in the context of the aforementioned discussion in order to understand the whole picture.

In this report we will describe initiatives around the introduction of RFID in identity cards. The main issue here is the introduction of RFID and biometrics in the electronic passport. We will describe the actual developments in Europe and the USA. But we will also look at the application of RFID in other kinds of identity cards, like consumer fidelity cards.

We will start with presenting an overview of RFID in identity cards (section 13.1), followed by a detailed description of the application of RFID in e-passports (section 13.2). Next we will describe the state-of-the-art of the development of RFID applications in the e-passport and other ID-cards in the USA (section 13.2.4), followed by a description of the situation in Europe (section 13.3). We have chosen this sequence of description because of two reasons:

Development of an e-passport has become top priority in the USA in late 2001, and hence in the past five years a lot of experience has been built in the USA around the development of an e-passport;

The Visa Waver Program of the USA has a direct influence on the development of the e-passport in Europe.

13.1. Overview of RFID in identity cards

13.1.1. Analysis of cases

Table 13-1 presents an overview of cases within the IDTechEX database in relation to the application of RFID in identity cards management and divided per continent. The main application of RFID in identity management is in the e-passport.

But also all kind of other identity documents may include RFID-applications, i.e. national ID-cards or ID-cards which are used by large organisations i.e. NASA, governmental departments, multinationals, universities etc. In general these ID-cards also permit access to buildings or facilities of these organisations. A few cases are dealing with RFID in drivers licenses. There are a lot of small access control applications with RFID (i.e. for access to company buildings, sport clubs etc.) but no such cases are described in the IDTechEX database.

Table 13-1: Applications domains for RFID in identity cards.[158]

Domain	America	Europe	Asia	Africa	Australia	TOTAL
E-Passport	2	12	6	1	1	22
National ID-cards	0	1	2	1	0	4
ID-cards	6	0	1	0	0	7
Drivers license	1	0	1	0	0	2
Access control	3	3	0	0	0	6
TOTAL	12	16	10	2	1	41

In every continent, cases were identified, but most cases came from the USA and Europe. A lot of the cases in Europe are related to the introduction of national e-passports. The cases in the USA and Canada are related to the introduction of country-wide e-passports, but a number of cases also have to do with the introduction of RFID in other ID-cards.

The cases in the IDTechEx database do not include all the activities on RFID applications which are going on in the various continents, but the number of cases gives a fair representation of activities in this area.

Some of the cases describe planned RFID-applications (2), others describe pilots or trials (5), some of the RFID-applications are ordered (10) and most of them are already rolled-out (18). We could not identify the actual status of the RFID-application in six cases.

In as far as it is known from the case descriptions all the RFID-tags used in the cases belong to the group of High Frequency tags (13.56 MHz). All the applied tags are also passive tags. Another observation is that most of the tags are able to both read and write. The distance range for sending and receiving information is mostly a few centimetres, according to ISO 14443 or ISO proximity.

13.1.2. Contact versus contactless cards

In the overall discussion on identity management a main issue is the discussion on the use of contact versus contactless cards. Card identity systems can be considered as a simple facility to increase security and efficiency. Card identity systems can be used for physical and logical access control, but also other functions could be included in such systems such as:

- employee and visitor identification
- time and attendance registration
- micro-payments

Various smart card systems exist for identity management. Smart cards are small and tamper-resistant. They hold, transmit and encrypt massive amounts of data. And they fit neatly within the surface of a digital ID card.

In an age with increasing security threats and data-transmission privacy requirements, smart card hardware, software, systems and solutions are fast emerging as the preferred technologies and applications around the world. The International Card Marketing Association states that the smart card market is growing at an annual rate of 28%.

A primary distinction between types of smart cards is whether they are "contact" or "contact-

[158] Source: IDTechEx, 2006

less". When using a contact card, the cardholder swipes or inserts the card into a card reader. When inserted properly, a metallic pad or contact plate on the smart card aligns with the electronic contacts inside the reader, where data is transferred. In contrast, contactless card systems update through antennas located in the smart card and the reader without physical contact.

Maintenance costs of contactless cards are lower since the components can be shielded in a protective casing, and the reader and cards are therefore not subject to wear and tear caused by friction when inserting the card into the reader. This allows operations in harsh environments and longer lifespan. Additionally, the cards can vary widely in sizes and shapes such as key chains, tags, stickers and wristwatches.

13.1.3. Various types of ID-cards

Powerful technologies are used nowadays to converge and transform the efficiency, functionality and security of ID-cards. This generates a number of new types of ID-cards:

- *RFID cards*
  This technology brings keyless convenience to physical access control security systems. RFID cards use an internal antenna that cardholders wave within a few inches of a reader to be granted or denied access.

- *"Combi" proximity cards*
  These cards integrate photo ID, proximity, magnetic stripe and even smart card technology into a single card, eliminating the need to carry multiple cards for different purposes.

- *Hybrid smart cards*
  A hybrid smart card has two chips embedded into a card's surface — one contact and one contactless — each with its own interface. This effectively doubles the functionality and security of every card issued.

- *"Combi" smart cards*
  Combi smart cards allow a single smart chip to securely interface with both contact and contactless readers. The Smart Card Alliance forecasts that the transportation and banking industries will adopt this technology first.

- *Optical laser cards*
  These cutting-edge cards transform CD-ROM technology into a credit card form, capable of securely storing megabytes of personal information. For example, a patient ID could hold an image, healthcare history, vaccination record, X-rays and more.

13.2. RFID in e-passports

Major initiatives by European and American governments aim to fuse RFID and biometric technologies in a new generation of identity cards, and the main application is in next generation passports, sometimes called e-passports.

The next generation of passports are supposed to contain personal information and some biometric data in digital form. This information can range from names over passport photographs to iris attributes and fingerprints. All this information is to be accommodated in a chip, which is then embedded in a RFID tag into the passport. This information stored on the RFID tag can later be read out by a reader, for example in airports to gain access control to security relevant areas.

In combination the RFID and biometric technologies promise to reduce fraud, easy identity checks, and enhance security. At the same time the combination of these technologies raises new risks, because they might have far reaching privacy and security implications.

13.2.1 Goals of e-passports

The goal of the e-passport is to provide strong authentication through documents that unmistakably identify their bearers. Therefore it is not only important to take care that the document is resistant to tampering, but also to take care of data integrity. So both data integrity and physical integrity are vital to the security of passports as authenticators and strong authenticated document.

Protecting e-Passport data against unauthorized access is a crucial part of the security of the entire identification system. Data confidentiality, i.e. secrecy of data stored on e-passports, is also critical. Protecting biometric and biographical data is essential to the value and integrity of an authentication system. In particular, data secrecy needs an important form of protection against forgery and hacking. So the question emerges how we can permanently protect these highly privacy-sensitive data against unauthorized access and data tampering, because, if no protection of this personal information exists, it will be very easy to scan those sensitive data with a (portable) reader. Any kind of data, which is stored on a RFID tag, is to be considered either as publicly accessible or must be provided with access control, no matter in which concrete form.

Therefore, RFID tags in e-passports have to be protected against any obtrusive attack or any attempt to track the bearer of the e-passport.

13.2.2. Security and privacy threats to e-passports

What are the threats of the RFID application in e-passports in view of the security and privacy aspects?

Molnar (2005) gives a detailed overview of the main security and privacy threats to e-passports:

1. Clandestine scanning

It is well known that RFID tags are subject to clandestine scanning. Baseline ICAO guidelines[159] do not require authenticated or encrypted communications between passports and readers. Consequently, an unprotected e-passport chip is subject to clandestine scanning, with attendant leakage of sensitive personal information, including date of birth and place of birth.

2. Clandestine tracking

The standard for e-passport RFID chips (ISO 14443) stipulates the emission (without authentication) of a chip ID on protocol initiation. If this ID is different for every passport, it could enable tracking the movements of the passport holder by unauthorized parties.

Tracking is possible even if the data on the chip cannot be read. The ICAO Active Authentication feature enables also tracking even when used with public key cryptosystems, like RSA[160] or Rabin-Williams signatures.[161]

3. Skimming and cloning

Baseline ICAO regulations require digital signatures on e-passport data. In principle, such signatures allow the reader to verify that the data came from the correct passport-issuing authority. The digital signatures used in the baseline ICAO standard do not, however, bind the data to a particular passport or chip, so they offer no defence against passport cloning.

4. Eavesdropping

"Faraday cages" are an often discussed countermeasure to clandestine RFID scanning. In an e-passport, a Faraday cage would take the form of metallic material in the cover or holder that prevents the penetration of RFID signals. Passports equipped with Faraday cages would be subject to scanning only when expressly opened by their holders, and would seem in first instance to allay most privacy concerns. Faraday cages, however, do not prevent eavesdropping on legitimate passport-to-reader communications, like those taking place in airports. Eavesdropping is particularly problematic for three reasons.

- Function creep: As envisioned in the ICAO guidelines, e-passports will likely see use not just in airports, but in new areas like e-commerce; thus eavesdropping will be possible in a variety of circumstances.

[159] See *http:// www.icao.int/fsix/regulations.cfm*

[160] RSA is a public-key encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique. The RSA algorithm is based on the fact that there is no efficient way to factor very large numbers. Deducing an RSA key, therefore, requires an extraordinary amount of computer processing power and time. The RSA algorithm has become the de facto standard for industrial-strength encryption, especially for data sent over the Internet. It is built into many software products, including Microsoft Internet Explorer. The technology is so powerful that the US government has restricted exporting it to foreign countries.

[161] The Rabin-Williams signature is an example of a Rabin cryptosystem, which is an asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of factorization. However the Rabin cryptosystem has the advantage that the problem on which it relies has been proved to be as hard as integer factorization, which is not currently known to be true of the RSA problem. As with all asymmetric cryptosystems, the Rabin system uses both a public and a private key. The public key is necessary for later decoding and can be published, while the private key must be possessed only by the sender of the message. The process was published in January 1979 by Michael O. Rabin.

- Feasibility: Unlike clandestine scanning, eavesdropping may be feasible at a longer distance, given that eavesdropping is a passive operation.
- Detection difficulty: As it is purely passive and does not involve signal emission by the owner, eavesdropping is difficult to detect (unlike clandestine scanning).

5. Biometric data-leakage

Among other data, e-passports will include digital photos. In accordance with the ICAO standard, these will initially be digitized full-face picture, although some countries also use fingerprints. These images would not need to be secret to support authentication if the physical environment were strictly controlled. Existing and proposed deployments of e-passports, however, will facilitate automation, and therefore a weakening of human oversight. This makes secrecy of biometric data important.

6. Cryptographic weaknesses

ICAO guidelines include an optional mechanism called “Basic Access Control” (BAC) for authenticating and encrypting passport-to-reader communications. The idea is that a reader initially makes optical contact with a passport, and scans the date of issue of the passport, date of birth of the owner of the passport, and the passport number to derive a cryptographic key K with two functions:

- The key K allows the passport to establish that it is talking to a legitimate reader before releasing RFID tag information.
- The key K is used to encrypt all data transmitted between the passport and the reader. Once a reader knows the key K, however, there is no mechanism for revoking access. A passport holder travelling to a foreign country gives that country’s Customs agents the ability to scan his or her passport in perpetuity.

A general cryptographic weakness is the use of too short keys or keys which are issues in structured series or which are interrelated in one way or another. For this reason it was possible i.e. to crack Dutch passports in about 2 hours.

13.2.3. Safeguard solutions for threats of privacy misuse

Apparent solutions for the threat of privacy seem to be found in the encryption of the content which is stored on the tags. Strong encryption procedures can provide reliable protection against eavesdropping.

The effectiveness of cryptography is based upon its key bits length. However, further research on hacking has revealed that the cryptographic protection afforded by a RFID device is not completely satisfactory. Therefore three instances of the encryption approach have been proposed which are more suited for protection. These approaches are: the hash-lock method, the re-encryption method (in several forms) and silent tree-walking. However, there are severe cost complaints in relation to the application of these methods.

Hash-Lock

In this approach a tag may be ‘locked’ so that it refuses to reveal its ID until it is ‘unlocked’. In such a situation it is necessary for a reader to query a tag to find its meta-ID, so that the reader knows how to unlock the tag.

Of course it is still possible in such a situation to track the tags via their meta-IDs.

The Faraday Cage approach

A solution to prevent skimming is to put a sort of shielding material on the passport front cover. This front cover contains an anti-skimming material that blocks the radio waves that could pick up the data. This shielding material is based on the Faraday cage principle and makes the e-passport RFID tag unreadable as long as its cover is closed or nearly closed.

In combination with other prevention methods, i.e. access control lists, this approach could be a good solution for preventing the tracking of a person and eavesdropping for the communication between the reader and the tag of the e-passport. It is not a complete prevention, because a hacker could even in the short time of communication between the reader and the tag access the data stream. Sometimes a solution is sought in a procedure, where the open e-passport should be placed on a flat reading device.

Shifting data to the backend

The most effective measure against an attack involving eavesdropping at the air interface is, however, not to store any contents on the tag itself, but instead of this to read only the ID of the tag. The data associated with the tag are retrieved from a backend database. This approach offers the additional advantages that less expensive tags can be used and memory for the associated data in the backend is practically unlimited and the used procedures for data management and IT security can be employed.

However, there are also some disadvantages of this solution i.e. the existence of user's objection against a central database (because this might bring all data under control of one body) and of course also the existence of general threats of database hacking.

13.2.4. RFID and identity cards in the USA

By the end of 2006 all new passports issued in the USA are supposed to have biometric information incorporated into RFID tags. The biometric passport is usually referred to as the 'electronic passport' or 'e-passport'

Background E-passport developments in the USA

A high level of security became a top priority in late 2001 for the United States. This tightened security required border control to take steps in cracking down on counterfeit paper passports.

In October 2004, the production stages of this high-tech passport commenced as the U.S. Government Printing Office (GPO) issued awards to the top bidders of the programme. The awards totalled to roughly $1 000 000 for start up, development, and testing. The driving force of the initiative is the US Enhanced Border Security and Visa Entry Reform Act of 2002 (also known as the "Border Security Act"), which states that such smartcard IDs will be able to replace visas. As for foreigners travelling to the US, if they wish to enter US visa-free under the Visa Waiver Program (VWP), they are now required to possess machine-readable passports that comply with international standards. Additionally, for travellers holding a valid passport issued on or after 26 October 2006, such a passport must be a biometric passport if used to enter the US visa-free under the VWP.

More specifically, as part of its US-VISIT program, the US government has mandated adoption by October 2006 of biometrically-enabled passports by the twenty-seven nations in its Visa-Waiver Program, among them Japan, most of the countries of Western Europe, and a handful others. The deadline for adoption was originally October 2005, but this date was not feasible, mainly because of the concern of US citizens over privacy protection.

The US version of the e-passport will only have full-face digital image placed onto the contactless chip. This provides a valuable increased level of security, but not as complex as the European version (see section 13.3). However, the chip used in the US passport will be large enough (64 Kbytes) to allow it to contain additional biometric identifiers should the need arise in the future.

On January 2006 e-passport trials have started in several US airports, including San Francisco International Airport. The US Department of State began issuing biometric passports to government officials and diplomats in early 2006. It began issuing regular biometric passports at its Colorado Passport Agency on August 14, 2006; though they still expect that nearly all new or renewed passports issued by the department to American citizens will be biometric by the end of 2006, other sources say this will not happen until mid-2007.

Characteristics US e-passport

The U.S. e-passports are based on guidelines issued by the International Civil Aviation Organisation (ICAO), a body run by the United Nations with a mandate for setting international passport standards. The ICAO guidelines, detailed in ICAO Document 9303, call for incorporation of RFID chips into passports.

Reasons for choosing RFID for this application are that it can provide better document security (passports become harder to counterfeit), it can facilitate the inclusion of biometric data, and many of the ICAO member countries are adopting it. One also should not forget that there was intense lobbying by the RFID smartcard industry.

Initially, the only biometric data included in passport RFID tags will be a scan of a passport photo, but it is expected that fingerprints and other biometric data are to be added in the future. The US-VISIT program in fact requires visitors to provide two fingerprints images in addition to a headshot. The ICAO standard also envisions that e-passports will someday include a write capability for storage of information like digital visas. All the e-passports which are in use now, contain passive RFID tags, which do not allow writing to the RFID tag after the production phase.

The original specifications for the project were that the RFID chip contains all the data of the ID page of a passport, and to be digitally signed, but not encrypted. This is one point of controversy, as many privacy advocates would prefer to see this data securely encrypted. The tags in passports are to conform to the ISO 14443 RFID specification, which specifies the radio frequency power and signal interface (13.56 MHz) and the initialization, anti-collision, and transmission protocols to be used.

Security threats and chosen solutions

The security vulnerabilities that have raised the most concerns are the possibility of eavesdropping and "skimming" RFID-enabled passports, the surreptitiously reading of data off a passport in a public place. Many people have expressed concern that this ability to possibly identify U.S. citizens in hostile countries could be a scary security issue for Americans. This issue received much media attention and caused a huge public outcry. Combined with the State Department's realization that these tags could be read from greater distances than originally thought, the decision was made to redesign the proposed system mid-project in order to make it less susceptible to eavesdropping and skimming.

The changes the State Department made to e-passports was to include anti-skimming material in the new passport covers and adding some basic access control to the data, so that a PIN number that is generated from the machine-readable portion of the passport is required to communicate with the RFID chip. This is considered a significant improvement to the security of e-passports.

Opposition against the US e-passport

Privacy activists in the USA and many other countries question and protest the lack of information about exactly what the passports' chip will contain, and whether it will have an impact on civil liberties. The main problem they point out is that data on the passports are transferred with RFID technology.

On one hand this will allow ID-check computers to obtain a person's information without a physical connection; on the other hand it may also allow anyone with the necessary equipment to perform the same task. If the personal information and passport numbers on the chip are not encrypted or if no other security measures are made, the information might wind up in the wrong hands.

To protect against such unauthorized reading, or "skimming", in addition to employing encryption, the U.S. has undertaken the additional step of integrating a very thin metal mesh into the passport's cover to act as a shield to make it even more difficult (the State Department claims "nearly impossible") to read the passport's chip when the passport is closed.

However, research students from Vrije University in the Netherlands, speaking at the August 2006 Black Hat conference in Las Vegas, showed that RFID passports can be cloned relatively easily, and can be remotely spied upon despite the radio-blocking shields included in US designs. They found they could read the passports from 60 centimetres away if they are opened by just 1 cm, using a device which can be used to hijack radio signals that manufacturers have touted as unreadable by anything other than proprietary scanners (Rieback, 2005).

At the same conference the German security expert Lukas Grunwald demonstrated that it is possible to clone the information on a biometric passport to create a false passport using equipment costing less than 200 Euro.

A group of German privacy hackers have come up with a portable device that can wipe a passive RFID-tag permanently, called the RFID-Zapper.

Additional concerns have been raised about the technical feasibility of biometrics in large-scale, real-world applications.

13.2.5. Other Identity cards developments

Another U.S. government implementation of RFID even gets more critics from several directions. The US-VISIT RFID programme is attaching RFID chips to i-94 documents, in an effort to better track when people leave the country via some means other than air travel. The i-94 document determines how long a person is allowed to stay in the U.S.A. A person receives the i-94 document when he has entered the USA with a VISA or when the Immigration and Naturalization Service (INS) has approved his extension. However, a common way for many people to enter or to leave the country is by car and since cars are large metal boxes, they act as Faraday cages, and make the reading of RFID signals very problematic. Unless a user in a car holds the document up to the window, it likely won't be read by an RFID reader. This is a pretty flawed implementation of RFID, as any system that depends heavily on users "doing the right thing" is unlikely to work well.

Another next-generation ID card slated for deployment in the near future in the USA is the Personal Identity Verification (PIV) card. This card will serve as ID badge and access card for employees and contractors of the federal government in the United States. The National Institute of Standards and Technology (NIST) is developing a standard for government ID cards, which is called FIPS 2001. It is to be expected that the government ID card also will include a combination of RFID and biometrics. The biometrics of choice for PIV cards will probably be fingerprint recognition.

The USA House of Representatives passed in 2006 a bill called the Real ID Act: this seems a likely impetus for States in the USA to issue drivers' licenses containing biometrics, and probably RFID tags as well.

The Real ID Act mandates that every state overhauls its driver's license ID card system by 2008. It requires real-time authentication for documents such as birth certificates and Social Security cards—which would require a massive electronic, interoperable network—and the creation of a national database to store the electronic data gathered at the state level.

13.2.6. Serious questions in the USA concerning the use of RFID in e-passports and National Identity Cards

In an article in eWEEK.com's Government Center of December 15th 2006, Renee Boucher Ferguson states that the separate initiatives put forth by the U.S. State Department and the US Department of Homeland Security to utilize RFID in passports, identification cards and driver's licenses are coming under fire from various directions. Perhaps, based on this, on December 12th 2006, two senators—a Democrat and a Republican—said they would propose legislation to repeal the Real ID Act of 2005 if the Department of Homeland Security does not change the act to include more personal privacy provisions and less of a financial burden on states.

The Emerging Applications and Technology Subcommittee, part of the Data Privacy and Integrity Committee that advises DHS, toned down its harsh criticisms of RFID technology used to identify individuals (in e-passports and PASScard ID cards) in a report released Dec. 13 2006. The report states that "RFID, standing alone, may not be best suited for purposes of identifying individuals.", while in an earlier version it said that RFID should not be used at all.

On December 4th 2006, the Smart Card Alliance, an industry group that works to foster the adoption of sensor-based technology used in all types of industry and consumer applications, such as credit cards and cell phones, issued a statement urging the federal government to reconsider its use of vicinity-read RFID technology in the proposed PASScard ID card that would be used by U.S. citizens crossing into nearby countries. Long-range RFID tag technology, according to the Alliance and other industry watchers, should be used for tracking products, not people.

In its report the Alliance listed a number of concerns, including a lack of security safeguards, the potential for tracking to inspire citizen distrust, the duplication of required border infrastructure to accept this ID technology in addition to e-passports, a reliance on central databases and real-time access to networks to read the data stored on cards, and potential operational issues with multiple vicinity-read RFID tags in vehicles.

In the meantime the U.S. government has planned to take various measures to improve the security of various identity cards (see also section 13.2.5). To prevent skimming and eavesdropping of data from the e-passports—and likely the PASS-card and electronic driver's license as well—the government has added BAC (Basic Access Control) and a shielding material to the passport. Furthermore, the RFID chip will not store any personal information—it will simply store a code or number used by a reader to call up information in a database. That is done in an effort to prevent skimming.

13.3. RFID and identity cards in EU

In summary the aims and objectives of the eID approach in Europe are:

- To provide support of eServices for the mobile citizen (building block for trust, security, easy access, convenience, service providing only to entitled persons);
- To build a more global (including a EU) information society (enhancing sense of community, offering trust, making persons aware to be a –relevant- part of society by offering a seamless e-services experience);
- To support combating of ID fraud and ID theft;
- To support preventing illegal work and illegal immigration;
- To support measures of anti-terrorism and combating organised crime.

Another issue is the extent to which Europe has to comply with US requirements, considering the fact that US requirements are a driver for e-passport deployment in Europe.

A declaration of European ministers was approved unanimously on 24 November 2005 in Manchester, UK. This declaration formulates two statements:

- *By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations. Such means shall be made available under the responsibility of the Member States but recognised across the EU.*
- *By 2010 Member States will have agreed a framework for reference to and where appropriate the use of authenticated electronic documents across the EU, as appropriate in terms of necessity and applicable law.*

In the Communication from the Commission on the i2010 eGovernment Action Plan, which was approved on 25 April 2006, the following legal aspects are presented:

- eGovernment has reached a critical juncture. Further significant progress requires certain key enablers to be in place, particularly for high impact services to be effective. Among those, interoperable electronic identity management (eIDM) for access to public services, electronic document authentication and electronic archiving are considered critical key enablers.
- Harmonised national ID cards might be one specific means to implement public service eIDM, but this is a national choice. Biometric national ID cards and eIDM for public services are markedly different: national ID cards serve public security, for example by facilitating integrated border management and supporting fight against terrorism, whereas electronic identification for public services is intended to ease access and offer personalised and smarter services.
- Member States recognise the importance of eIDM for ensuring that by 2010 European citizens and businesses will be able to benefit from secure and convenient electronic means, issued at local, regional or national levels and complying with data protection regulations, to identify themselves to public services in their own or in any other Member State.

The Commission will also consider if regulatory measures are needed for the development of electronic identification and authentication for public services.

13.3.1. European regulation

Council Regulation 2252/2004/EC (that entered into force on 18/01/2005) has laid down standards for security features and biometrics in passports and travel documents issued by the Member States.

The definition of minimum security standards for passports was introduced by a Resolution of the representatives of the Governments of the Member States, meeting within the Council, on 17 October 2000. The Council Regulation upgraded this Resolution by a Community Measure in order to achieve enhanced harmonised security standards for passports and travel documents to protect against falsification. At the same time biometric identifiers will be integrated in the passport or travel document in order to establish a reliable link between the genuine holder and the document.

The Council Regulation is limited to the harmonisation of the security features including biometric identifiers for the passports and travel documents of the Member States. The designation of the authorities and bodies authorised to have access to the data contained in the storage medium of documents is still a matter of national legislation, subject to any relevant provisions of Community law, European Union law or international agreements.

Regulation 2252/2004 only lays down such specifications that are not secret. These specifications need to be supplemented by specifications which may remain secret in order to prevent the risk of counterfeiting and falsifications. Such additional technical specifications will be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission.

In order to ensure that the information referred to is not made available to more persons than necessary, each Member State has to designate no more than one body having responsibility for producing passports and travel documents, with Member States remaining free to change the body, if need be. Member States communicate the name of the competent body to the Commission and the other Member States.

Passports and travel documents must include a storage medium which shall contain a facial image. Member States shall also include fingerprints in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.

This Regulation applies to passports and travel documents issued by Member States. It does not apply to identity cards issued by Member States to their nationals or to temporary passports and travel documents having a validity of 12 months or less. Additional technical specifications for passports and travel documents are established in accordance with the procedure referred to in Article 5(2) of the Council Regulation:

- additional security features and requirements including enhanced anti forgery, counterfeiting and falsification standards;
- technical specifications for the storage medium of the biometric features and their security, including prevention of unauthorised access;
- requirements for quality and common standards for the facial image and the fingerprints.

13.3.2. European biometric passports

The European version of the e-passport is planned to have digital imaging and fingerprint scan biometrics placed on the contactless chip. This combination of the biometrics aims to create an unrivalled level of security and protection against counterfeit and fraudulent identification papers.

In most European countries initiatives have started to develop so as to implement an e-passport. In annexes 4-6 we will give an overview of initiatives in a number of European countries concerning e-passports and ID-cards. Here we describe in more detail developments in some European countries.

United Kingdom

Over the last two years, the Identity and Passport Service (IPS) has implemented a range of new procedures and systems to prevent identity and passport fraud. In March 2006, it launched the Biometric Passport, and in July 2006 IPS issued the millionth biometric passport to a member of the UK public.

Currently, the British biometric passport only uses a digital image and not fingerprinting, however this is being considered by the United Kingdom Passport Service.

The UK Identity and Passport Service introduced biometric passports to normal British applicants "over a period of six to nine months in 2006" for the same price as normal British passports.

Netherlands

The encryption scheme initially used to protect the flow of information between the Dutch biometric passport and a passport reader was cracked on 28 July 2005. Though it has not been attempted in practice yet, in theory and under ideal conditions some of the data exchanged wirelessly between the passport's built-in contactless chip and a reader (more precisely, the one-way flow of data from the reader to the passport) may be picked up from up to 10 meters away. Once captured and stored, the data can then be cracked in 2 hours on a PC. This is due to the Dutch passport numbering scheme which does not provide sufficient randomness to generate a strong enough key to secure the exchange of information between the passport and the reader.

Other passports such as the U.S. passport do not contain this flaw as they use a stronger key to encrypt the data exchange. Also, some readers provide shielding for the passports while it is being read, thus preventing signal leakage that might be intercepted by another device. Moreover, the fairly secure and monitored environment of the passport control area would make it difficult for someone to illicitly set up the sensitive equipment necessary to eavesdrop on the communication between passports and readers from any significant distance.

At another occasion the E-passport was also hacked. Specialists of the Dutch security firm Riscure have demonstrated to the public live on TV in the course of the Dutch science program Nieuwslicht that it is possible to tap into the radio connection between an official document equipped with an RFID chip and its reader and decrypt the data gathered within a matter of hours.

The approach by the specialists of Riscure, which they had earlier presented at the hacker conference "What the Hack", is based on the fact that the passports issued by the Dutch authorities are numbered serially. Moreover, as the number of passports issued each month is fairly constant, a simple linear relationship can be obtained between the date of issue of each document and the passport number. This has the effect of bringing down the effective encryption strength of the transmissions tapped into to a mere 35 bit. Taking these relationships into account, even an average PC in the course of a so-called brute-force attack will only take a few hours to try out all 2^{35} possible keys.

To protect against unauthorized reading of the data stored, the Dutch passports are equipped with so-called Basic Access Control (BAC). In case of BAC the secret key for accessing the chip and the encrypted data transmission are numerically based on the passport number, date of birth of its owner and the document's date of expiry, which have to be read beforehand by optically scanning the document. In theory these numbers taken together should provide encryption strength of about 56 bit, provided they cannot be estimated fairly precisely or even obtained from other sources.

France

Axalto, a world's leader in microprocessor cards, announced it has supplied the electronic part for the new e-Passports being issued in France. Axalto, in coordination with a group of French industrial players, has worked alongside Imprimerie Nationale to meet the deployment schedule set by the French Ministry of the Interior for the electronic passports designed for French citizens. Axalto will provide Imprimerie Nationale with about two Million units in 2006.

The first electronic passports will enable passengers to travel to the United States without the need for a visa. These were first available in the Hauts de Seine region and deployment was extended to the rest of mainland France by the end of May 2006. These new travel documents feature Axalto's e-passport technology: a highly secure operating system with encryption algorithms that work on a contactless chip incorporated into the passport's cover. In addition to the identity information already contained on the first page, this chip also features the passport holder's digitized photo.

13.4. Financial institutions cards

13.4.1. Use of smartcards for contactless payments

The launch of contactless payments across North America has begun in earnest. American Express, MasterCard, and Visa have all launched contactless payment initiatives, with leading banks issuing millions of contactless credit and debit cards to consumers. Major retailers across the U.S. are installing contactless readers that can accept contactless payment and are integrated with point-of-sale (POS) systems. Research shows that consumers, issuers and merchants benefit from the use of contactless payments. Consumers enjoy added convenience, speed and ease of use, while issuers and merchants enjoy faster transaction times, increased spending per transaction, lower operational costs and penetration into the cash payment market.

The resources below were compiled by the Smart Card Alliance Contactless Payments Council to provide information on the status of the contactless payments in the U.S.A.

The Smart Card Alliance commissioned an independent survey of consumer attitudes toward contactless payment devices in August, 2006. The survey, conducted by Javelin Strategy & Research, concluded that there is a large, untapped market for the use of these devices. A significant majority of U.S. consumers are ready to adopt contactless devices for financial payments. Those who have already adopted contactless payment find the contactless experience to be uniformly positive and express a high degree of confidence in the technology.

According to the Smart Card Alliance adopting contactless payments can be a win-win situation for consumers and merchants alike. The major factor driving adoption and use–convenience represents a benefit for both parties to the transaction. Consumers are also willing to use contactless devices for both low- and high-value transactions and are open to trying contactless devices that are embedded in a wide variety of form factors.

The survey indicates that the major challenge to widespread use of contactless devices is reassuring consumers that contactless payment is safe. However, contactless payment appears to be an easy sell once information about it reaches the consumer. Both education and actual use alleviate consumer concerns about security.

Smart cards are also used for electronic purse payment applications. In this application, the smart card carries a stored monetary value. Cardholders generally use these cards to replace cash in making frequent, low-value transactions. Electronic purses are used for both retail payment and transit fare payment.

13.4.2. Advantages and disadvantages of contactless credit cards

Contactless credit card advantages

Credit card companies are claiming the following advantages for contactless credit cards:

- The card is faster to use. To make a purchase, the card owner just waves his card over the RFID reader, waits for the acceptance indicator - and goes on his way. American Express, Visa and Mastercard have all agreed to waive the signature requirement for contactless credit card transactions under $25.
- This technology is satisfying people in their need for speed (see average transaction speeds):
  - Contactless credit card transaction: 15 seconds,
  - Magnetic strip card transaction: 25 seconds,
  - Cash transaction: 34 seconds.

The contactless cards use highly secure data transmission standards.

Contactless cards make use of the most secure encryption standards practical with current technology, which make it nearly impossible for thieves to steal data of the consumer.

The contactless card never transmits the card number. Instead, the RFID chip within the card creates a unique number for the transaction; if a criminal intercepted the number, it would be useless even if successfully decrypted.

One additional fact that is known about contactless cards is definitely an advantage for merchants – consumers may feel otherwise. In a 2004 study, the average number of transactions at a retail location rose by about one percent, and the average “spend” rose fifteen percent for all contactless credit card users. So, it appears that there is a correlation between ease of use and total spending.

Contactless credit card disadvantages

The following disadvantages have been noted with contactless credit cards:

- Contactless cards are more exposed than regular credit cards.
  If a person wants to keep his credit card secure, he could keep it safely in an enclosed wallet or purse; thieves would have absolutely no way to even know if the person has a credit card. However, a thief armed with a suitable reader, within a near distance, would be able to interrogate all of the cards in a person's wallet or purse without his knowledge.
  Also, a regular credit card transaction is fairly secure; the magnetic strip is swiped at very close range (less than a millimetre). However, a thief with a suitable reader could monitor the contactless card transaction while standing at the counter, or just behind a person who carries out the transaction.
  These concerns have, of course, been carefully noted by credit card companies. The RFID chip in the contactless credit card responds to the merchant reader with a unique number used for that transaction only; it does not simply transmit the consumer's account number. This number is also encrypted.
- It is easier to spend.
  Studies have demonstrated that consumers will be more likely to spend, and will spend more frequently, with contactless credit cards.

Privacy advocates are particularly concerned about this technology; it is feared that having this much information available "in the open air" will lead inevitably to problems.

13.4.3. Concern regarding the use of RFID in credit cards

There is a lot of concern regarding the use of RFID in credit cards.

Civil rights groups have expressed concerns about application of RFID technology in financial institutions cards. They worry people could, in theory, be tracked by the tags.

Others are afraid that a credit card can be detected if people are not using the cards and therefore want a kind of button that can turn it off or on. They are afraid that otherwise people could wander around with a RFID detector looking for people with RFID-credit cards.

In a demonstration in October 2006 for 'The New York Times' security researchers easily hacked a University of Massachusetts computer science professor's newfangled RFID credit card. In short order (and with his permission), a researcher working with RSA Labs was able to steal the professor's name and credit card number that was being transmitted in plain text — thereby poking massive holes in Visa, MasterCard and American Express' claims that these card include "the highest level of encryption allowed by the U.S. government."

In a reaction to this demonstration Visa said that "This is an interesting technical exercise, but as a real threat to a consumer - that threat really doesn't exist."

Prof. Ted Selker, a leading professor at the Massachusetts Institute of Technology, has suggested using radio tags in credit cards as a kind of virtual signature. He said the way someone moved their finger over the card would alter the radio transmission, producing a signal unique to that person. A person could have some gesture and that would be his signature. It would be like a personal handshake.

13.5. Discussion

13.5.1. Main issues in e-passport developments

e-passports are valuable to many around the world but also raise a lot of questions. To provide enhanced security, the traditional passport is subject to a far-reaching change. A main aspect is that the next generation passports include biometric technology that will further support border security goals.

Without question, biometrics in e-passports will strengthen border security by creating more guarantees that the person carrying a passport is the person to whom a nation issued that passport. The biographic data, which include the bearer's digitized photo, are on an interior page, and the data is replicated in a contactless chip implanted in the back cover. The data in the integrated circuit is checked by an inspector with an RFID reader. If the data page and the chip data are not the same, the individual bearing the passport is subjected to further ID checks.

In the first generation of the USA e-passport the biometric data is limited to the bearer's photo. It is quite likely that second-generation U.S. e-passports will add iris scans.

The specifications for the new U.S. e-passports are governed to some extent by the Enhanced Border Security and Visa Entry Reform Act of 2002, which requires border entry documents to be machine-readable "containing biometric identifiers" and to be in compliance with the International Civil Aviation Organization standards. ICAO determined in 2002 that facial features, fingerprints and iris recognition are all applicable to machine-readable travel documents. In Europe facial recognition is the preferred biometric, the other two are additional options. ICAO also selected contactless integrated circuits as the best means of implementing the biometrics data standard.

In keeping with requirements adopted by ICAO and directives from the Department of Homeland Security, the new US passports are to be issued domestically to all applicants by the end of 2006. All 27 nations in the Visa Waiver Program (including most European countries) must issue e-passports by Oct. 26, 2006, in order for their citizens to be able to continue to enter the U.S. without first obtaining a visa.

Among the general parameters specified by ICAO to determine the standard for biometric passports, were the requirements that the technology had to support 32 kilobytes of storage, and that stored data needed to be easily accessible and transmitted quickly. As a consequence the chips in the new e-passports will have enough memory to accommodate additional biometric information.

Because RFID allows data to be collected inconspicuously and at a distance, privacy and security advocates are wary of its use in e-passports. The risk will only grow with the push towards unsupervised use of biometric authentication. In response to such concerns many governments have decided that the new e-passports have to be equipped with "anti-skimming" technology. One of the solutions for this is sandwiching a metallic mesh within the front cover and spine to prevent RF reads until the e-passport is opened and read at close range by an official. Also Basic Access Control should be used to prevent unauthorized remote reading of e-passports.

Today's e-passport deployments are just the first wave of next-generation identification devices. E-passports may provide valuable experience in how to build more secure and more private identification platforms in the years to come. Although very challenging technological hurdles have already been overcome in the development of the e-passport, there are still a few other issues. Not the least of these is that the technologies incorporated in the new passports do not come cheap.

13.5.2. Issues to be solved in relation to RFID applications

The infrastructure to support RFID technology is not yet in place globally. Issues range from interoperability of systems to the lack of globally recognized standards, testing and reliability. Four challenges, however, stand out in relation to RFID-applications, both in general and specific in relation to the application in e-passports:

First, the real-time nature of RFID data creates concerns for privacy and security experts. Eliminating paperwork and removing the human element may speed goods through the supply chain, but those advances also threaten implementation of traditional laws, regulations and procedures established to maintain the flow of goods and people across borders. The biggest challenges of RFID arise from the proliferation of data, the sharing of the data and databases, and from the possibility of snooping via tapping of radio waves.

With few standards or common patterns of behaviour yet established on a global basis, RFID watchdogs suggest that the following information practices must be accepted in order for the technology to thrive:

- Users must be warned that the technology is in use with the intent of collecting personal data limited to the purposes for which it is collected.

- Collected data is accurate, complete and timely.
- Personal data are protected by reasonable security safeguards against risk of loss, unauthorized access, destruction, use, modification or disclosure.
- Users can view all information collected about them.
- Compliance with these guidelines is mandated and a system is maintained to implement compliance.

Second, there are no laws yet to provide warranty protection on systems, readers and antenna RFID products. There is little recourse for malfunctioning RFID equipment.

Third, and equally important, is the fact that there is no certification or registry recognizing approved system integrators, RFID consultants and trainers. Some companies do train on their own equipment, but a vendor neutral solution to certifying providers is not yet available.

Especially because RFID technology is remotely readable, invisible and capturing data in real time, trust that the data are being captured and transmitted safely and securely is essential for its acceptance.

Finally, there is the challenge of misinformation and confusion about RFID that is more pervasive than the technology's advocates want to believe. Education is essential to defusing misinformation. RFID is a generic technology with many possible applications, each of which has its own benefits and limitations. Currently, however, each industry using RFID has mounted its own informational campaign, and the resulting consumer confusion is echoed in the press, thus confounding any inherent misunderstandings about the technology. Establishment of recognized, certified courses in its fundamentals is still a work in progress.

Acceptance of any disruptive technology — and RFID is one — takes time. We take bar-code technology for granted now, but it took at least 20 years for it to be incorporated as a mainstay of commerce. RFID technology presents a similar challenge to the way we live and work around the world.

Price-setting of the RFID technology applications is of course a main issue in relation to acceptance of this technology. At least in some countries new passports (with RFID) are more expensive than classical passports (without RFID), which causes negative reactions and negative press comments. The acceptance of e-passports, for which the users has to pay, might be hampered by such a high price setting.

This leads to a number of overall recommendations for policy-issues at a European level.

- A number of fundamental questions concerning the use of RFID in identity management are still under discussion. One of the main questions is whether long-range RFID tag technology should be used only for tracking products, or also for people. These doubts are mainly based on the facts that privacy and security issues are not solved yet to an acceptable level. Advocates of RFID technology wave away the objections, while opponents of RFID technology embrace every hacker demonstration in relation to RFID-applications to give voice to their opinion that the present RFID-applications are not safe yet.
- Policy leaders and researchers have to find clear answers in this debate, in order to come to final conclusions regarding the reliability and acceptance of RFID-technology in identity management for people.
- In this debate one should be aware of the fact that the penetration of RFID-applications for the identification of people has made significant progress in our society and a total rejection of this technology is hardly conceivable anymore.
- This means that everything has to be done to improve the conditions for acceptance and adoption for this new technology in our society. One main suggestion here is in educating people on the various aspects of the RFID-applications, because a large number of people are not aware yet of the pros and cons of RFID-applications and how to handle with care these applications while they can at the same time use the benefits of this new technology. On the other hand still a lot can be done to improve the security of these applications. One concrete point here is the

incorporation of anti-skimming material in the European e-passports. Many problems might be solved if the design and development of RFID applications in identity management involved in an open dialogue all stakeholders. In this context the involvement of potential user groups in the development of the systems is very important. In other words: a user-centred design is needed. It is very important that decision-makers create the conditions under which such a user-centred approach can be realized.

13.5.3. Need for a user-centred design

The U.S. government has spent over a billion dollars on the US-VISIT RFID program so far, and industry experts have dismissed the effort as a very flawed RFID implementation. The success of RFID applications like this that rely on human interaction, according to Vollmer (Volmer 2006) requires a user-centric design, something that has been missing so far in the government's work with RFID. As far as one can tell the e-passport program in the USA has not included any user testing or privacy impact assessments, and this is a problem.

The Real ID Act of 2005 mandates that by 2008 all state-issued ID cards must contain machine-readable technology with defined data elements, and it is very likely that RFID will be the technology used. Users matter a lot in these kinds of systems and programs, and implementers and developers need to keep the users firmly in mind.

14. RFID in public transport

Radio Frequency Identification is a technology that is used in a wide variety of societal settings. Being a technology to identify objects (or persons related to objects) it can also be used to locate these objects and to pass on specific identifying information about these objects. One domain of application that finds widespread use all over the world is the use of RFID in public transport settings. Smart labels and smart cards with an RFID chip (in the future complemented by chipless tags) are used to give people access to buses, trams, metro's, trains and taxis.

RFID is a promising technology for use in the public transport system. It enables the realisation of a more efficient and effective public transport system. It does so by reducing the time needed to board a bus or a train (including the time it takes to buy a ticket), by offering additional information to travellers (time of arrival, time of departure, delays in time schedules, etc.), by offering management information about the traffic patterns in public transport, by fighting fraudulent uses of public transport (not paying for the trip), and by extending the range of services that can be offered by public transport operators, if needed in combination with other service providers.

RFID thus may contribute to modernising the public transport system. Many public transport operators are aware of the potentialities of RFID. The number of pilots of RFID in public transport is high and is still growing. On the basis of a collection of cases around RFID cases in public transport it is possible to get a view on the distribution of RFID-pilots worldwide.

Table 9-1 presents an overview of distribution of cases within the IDTechEx database. It shows that passenger and public transport ranks number three.[162]

The 278 case studies in passenger transport cover introduction of RFID in public transport, in airline systems, in vehicle parking systems, in vehicle highways, in car manufacturing, in toll roads, etc. Public transport pilots are a part of this total number. From the figures presented it is difficult to determine the precise distribution over the various categories. On the basis of the overview, added with internet search, pilots in public transport in Europe have been identified in the following cities: Clermont-Ferrand, France; Edinburgh, UK; Paris, France; Hertfordshire, UK; Nottingham, UK; Hanau, Germany; Rotterdam, the Netherlands; Swansea, Sweden; Torino, Italy. The investments in introducing RFID in public transport are considerable. Within the Netherlands, it is expected that the full roll-out of RFID in public transport (foreseen for 2008) will cost over 1.5 Billion Euro.[163]

RFID technology used in public transport stems from a variety of ICT vendors. The chips are mainly from either Philips (the Mifare chip; ISO 14443 A compatible) or Sony (the FeliCa chip, also ISO 14443 A compatible). Table 14-1 presents an overview of the use of the Sony FeliCa card in a number of Asian public transport systems.

[162] See rfid.idtechex./knowledgebase/en/breakdown.asp; visited 12 April 2006; IDTechEx warns to be cautious in interpreting the figures on face value. Not all cases are similar in scope and coverage. The market value of the cases differs considerably, ranging from a few thousand Euro to over a billion Euro. But overall, the table gives an idea of the relative attention that is given to RFID in the various application domains.

[163] Kamerstuk 23645, nr. 119. Tweede Kamer, vergaderjaar 2005-2006.

Table 14-1: Distribution of Sony FeliCa card in public transport in Asia[164]

Place	# of cards	Start	Application domains
Hong Kong	12 Million	1997	Public transport, e-Purse, e-Identification
Singapore	8 Million	April 2002	Public transport ("EZ-link" card); fast food; vending machines
Shenzhen (China)	n.a.	2004	Public transport ("Trans card"); student ID; discount tickets
New Delhi (India)	n.a.	Dec. 2002	Metro ("Travel card");
Bangkok (Thailand)	n.a.	July 2004	Metro ("Metro card")
Tokyo (Japan)	14 Million		Train; East Japan Railway Company "Suica"

Given the high number of travellers and subsequently the high number of cards to be issued in today's public transport system, the introduction of RFID in public transport is a mass market with high investments in cards, equipment, devices, and information systems needed to run the entire ticketing system smoothly. Pay-back times are in the order of several years, but introduction of RFID in public transport systems in Asia has shown the benefits to be considerable.[165]

From the perspective of this study, the introduction of RFID in public transport is an interesting case to look at. Public transport is embedded in regulation (role of public authorities) and competition (role of private actors). Public transport organisations of various kinds may cover a city, a region or a country, and may encompass one transport modality or several at once. Embedding RFID in public transport tickets is only the first step in setting up a complex system that may have links with additional services, such as car parking, taxis and retail services in and nearby public transport stations.

The introduction of RFID in public transport is thus a complex issue, in which public and private interests have to be weighted, and in which decision processes cover more than technological elements alone. It may also be surrounded by public controversies, for instance in relation to the use of the data and the privacy issues that go with it, or related to the public discussion on fighting fraud and aggression in public transport.

From a technological perspective, public transport is interesting because Europe seems to have a reasonable stake in the future development of RFID in public transport, especially when looking to RFID technology from a broader perspective (encapsulating developments such as Near Field Communication).

In the next sections we will present an elaboration of the introduction of RFID in public transport in the following settings: public transport in Europe (generic overview of a number of projects), The Netherlands (starting with pilot in Rotterdam), the introduction of the Oyster system in London and Venice (Italy). These case-descriptions are meant to provide us with empirical details on the issues we want to discuss in the final section of this case-study.

14.1. RFID in public transport

The use of contactless smart cards in Europe is growing. In a number of cities and regions (and in the Netherlands in the entire country) pilots and projects are running to introduce contactless smart cards and tickets for public transport. Numbers are high: many projects deal with millions of cards. The projects are complex, multi-actor undertakings, lasting for several years. It is not only the technological migration towards another system[166] that complicates matters but to get sufficient economies of scale projects sometimes include dozens of different public transport organisations and usually politics play a role as well.

[164] IDTechEx (2006). The RFID Knowledge Base – Sample Case Studies.

[165] IDTechEx (2006). The RFID Knowledge Base – Sample Case Studies.

[166] This migration includes moving from ordinary paper tickets fit to visual inspection or magnetic stripe technology towards a technological infrastructure based on contactless technology that includes access to stations and the use of Internet to upload the credit of the travel pass.

In Annex 7 we present an illustrative but not exhaustive overview of cases in public transport throughout Europe to illustrate the broad variety and complexity of the various projects. As a starter, we present a number of features of these projects.

Technology

Most smart cards make use of the Philips Mifare S70 chip, a passive RFID chip operating at the 13.56 MHz range, with a read range of roughly 10 cm and a memory capacity of 4 kB. The memory capacity is subdivided in a number of different sectors that may be used for different purposes. The chip has different security mechanisms and may use data encryption. It has a three pass authentication mechanism to ensure the proper communication between the reader and the tag (ISO/IEC DIS9798-2 compliant). The tags are ISO 14443 compliant. They can function as an electronic purse: a credit is stored on the card which is debited when one enters a bus or train. The chip stores information about the location where one enters and leaves the public transport system (including changes during the trip), thus enabling the assignment of revenues to the appropriate public transport companies. Communication between the reader and the tag is fast (in the order of milliseconds) enabling a high throughput of passengers. The advantage of having a contactless chip more than a contact-based smart card are obvious: the throughput of passengers is much higher (as stated in the Paris project in the metro: 4 times as high!); the sometimes cumbersome procedure of having to put a card in a slot (in moving buses) is avoided; and the cards will not degrade due to repeated uses. A disadvantage is the relatively high costs of the smart card, including the casing. Within various pilots, figures of €6 to €7.50 are mentioned. Probably, this is slightly more than the pure costs to construct the smart card and personalize them.

Next to the smart card version, the French company ASK has developed a paper-based ticket, based on its C.ticket system. The C.ticket has an RFID-chip (for instance the Philips Mifare chip) encased in a paper label. The antenna is printed on the paper by means of a conducive silver-ink. Printing the antenna is much cheaper than the traditional etching of antenna's from a piece of copper (with relatively high levels of waist). The functionality of the C.ticket is comparable to the functionality of a public transport smart card. It can have secure communication with the reader, just as in case of the smart card.

Though the paper cards are often used for single journeys (or a block of journeys) they can be rechargeable and they may have identifiable information on the chip. During a pilot in Porto (Portugal) it has been demonstrated that the life time of the paper based card, for which a fee of €0.50 was requested, was much higher than originally expected.[167]

The readers are hidden in access gates or stand alone devices. One has to read out the card when accessing and when leaving the station. Given the proximity reading which is necessary in combination with the appropriate authentication procedure the danger of eavesdropping appears to be small.

14.1.1. Actors

RFID chips provider Philips has a considerable share in providing chips. ASK, a French technology provider and consultancy company, has a relatively high contribution to the delivery of chips (including the ASK C.ticket); other European contributors to RFID technology are SMicroelectronics, Infineon, Nokia (NFC consortium together with Philips and Sony) and Applied Card Technologies. System integrators are mainly European consortia (though sometimes based abroad such as Accenture); the consortia combine technological expertise (tags, readers), knowledge about information processing and database management (the backend systems) and consultancy expertise. In a number of projects the consortia responsible for the technological migration towards RFID-based ticketing systems explicitly opt for an open and interoperable approach, enabling vendors to step in whenever they feel to (and are able to live up to the conditions of access). In case of the Netherlands, the responsible consortium Trans Link Systems has involved over 40 providers who have passed the quality test TLS has provided.[168] In the Swedish Skane County an open architecture

[167] Personal communication with Jose Duarte Vieira, director of Metro do Porto, 16 May 2006.

[168] See next section and www.translinksystems.nl (visited 13 July 2006).

is used, enabling the other five counties in the South of Sweden to profit from the lessons learned at the Skane pilot. The consortium of Nokia and Philips is active in Germany with a test of Near Field Communication (NFC)-phones (Nokia 3220 phones) within the city of Hanau. This is the only NFC-pilot we have noticed.

The situation in which RFID-ticketing is introduced is usually a rather complicated one. In Florence, Manchester, Paris, London and the Netherlands several public transport companies are involved. In Paris, next to the Metro-company RATF and the train-company SNCF, 93(!) different private travel operators are engaged in the transition from the traditional Carte d'Orange towards an RFID-based ticketing system. In Manchester 40 bus companies in 10 districts are involved. The London Oyster card is introduced in London metro, buses and trains. Within the Netherlands the five big public transport operators have joined forces, while agreement with the remaining parties (mostly integrated at the level of the twelve Dutch provinces) is sought.

Of the New Member States, one pilot is reported to take place in Warsaw (Poland).

Government is mentioned in a number of cases as a 'limiting' actor, or at least an actor that has a very specific role to play (being responsible for public transport in several – but not all – countries).

14.1.2. The benefits

Due to the complexity of the introduction of RFID in public transport, the stake is high, with a 1.3 billion Euro (over a period of 17 years including 240 million Euro capital investment) of the London Oyster card and a 1.5 billion Euro investment in the Netherlands as top investments. Especially in big cities and densely populated regions the number of passengers per day is high, leading to high numbers of transactions daily (millions per day). Though it is hard to decide on Return of Investment issues, IDTechEx database mentions figures of one to two years for RoI. RoI must be in savings, due to combating fraud (65 million USD in London yearly), increase in passenger flows, more efficient management of resources (trains, buses, etc.) and savings in personnel (check in check out, selling points, services, etc.). The cases do not indicate the savings on these points. Additional information indicates the opposite: extra personnel is needed (at least in the initial stage) to help travellers understand what to do.

The benefits indicated in the case-studies have a rather broad range:

- combating fraud (mentioned quite often)
- improving user convenience (fewer and shorter queues, ease of use (!), additional services)
- operational benefits
- reduction of surveys to monitor travelling behaviour
- improve boarding speed (four times faster in Paris metro)
- better and accurate travel management information
- opportunities to offer additional services

The direct benefits (benefits directly related to the public transport system) are expected to be sufficiently high to support the high investments. Part of these costs will be passed on to the passengers, for instance in additional costs to the fares the have to pay.

14.2. Case 1: the Netherlands

The Netherlands want to introduce RFID in the entire public transport system, covering all transport modalities (trains, buses, trams, metro). To do so, it has started a pilot in the metro of Rotterdam in which the technique will be developed and tested; after a successful testing, the RFID-system will be gradually rolled out over other transport modalities and regions of the Netherlands. Since the test itself has experienced some delays, due to difficulties in transferring the complicated Dutch ticketing system into the software, it is now hoped that roll-out will be ready at 2008. The process started at the end of 2003.

14.2.1. Objective

According to the responsible agency - the Trans Link Consortium (a consortium built around the five main Dutch Public Transport Operators) - an RFID-based public transport has three advantages:

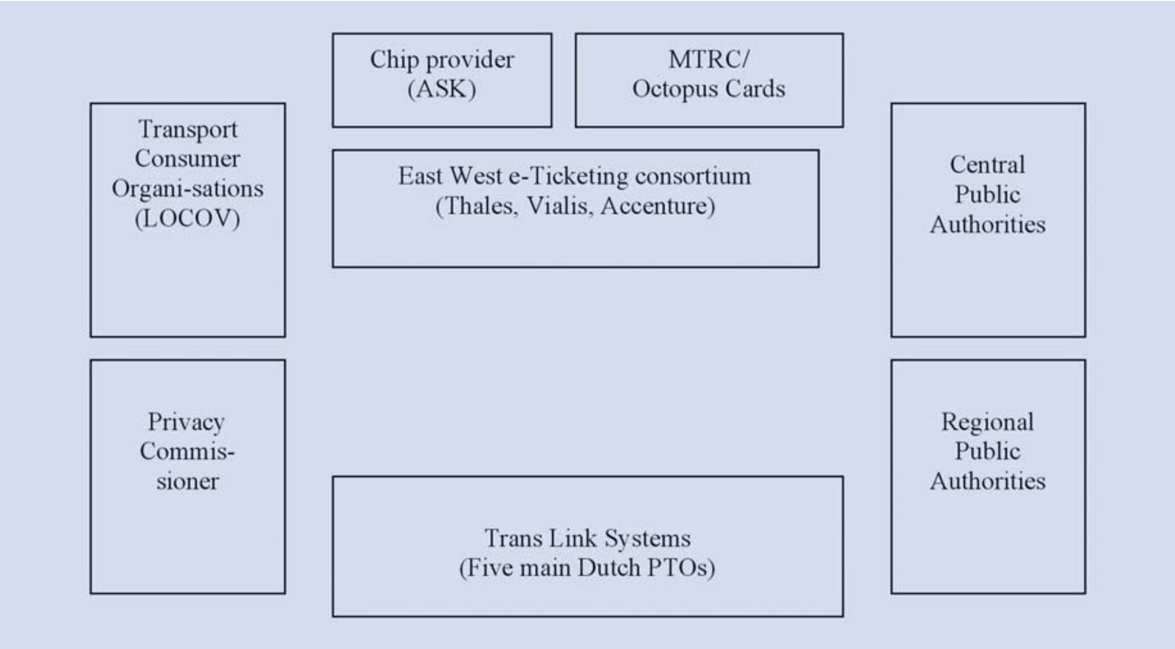
- it is faster (less time needed to buy a ticket and to board a vehicle);
- it is socially more safe (it combats fraudulent use of public transport – using it without paying – and it enhances safety at the stations – need of an entrée ticket to get into the station);
- it makes using public transport easier (only one ticket for all modalities).[169]

To these objectives, a fourth may be added: it should make public transport more cost efficient.

14.2.2. The actors

To understand the dynamics surrounding this specific case, in Figure 14-1 a picture of the various actors that are involved in the Dutch case is sketched.

Figure 14-1: Actors involved in RFID in Dutch public transport


Chip provider (ASK)
MTRC/ Octopus Cards
Transport Consumer Organi-sations (LOCOV)
East West e-Ticketing consortium (Thales, Vialis, Accenture)
Central Public Authorities
Privacy Commis-sioner
Regional Public Authorities
Trans Link Systems (Five main Dutch PTOs)

On the bottom part of *Figure 14-1* one finds the main initiator of RFID in the Dutch public transport system, Trans Link Systems. TLS consists of the five biggest PTOs in the Netherlands, which together are responsible for over 80% of public transport passengers.[170] Next to the Dutch Railways (NS group) it comprises the three public transport companies of the three major Dutch cities (GVB for Amsterdam, RET for Rotterdam and HTM for The Hague) and the regional buss company Connexion. The public transport companies of the big cities cover public transport by bus, tram and metro (metro only for Amsterdam and Rotterdam). TLS is the main initiator of the Dutch pilot. TLS has selected the consortium that was given the task to build the entire system by means of a tender procedure.

On the top part one finds the technology providers. Central to these is the East-West e-ticketing consortium, which consists of Thales, Vialis and Accenture. Thales is responsible for the smart cards and the integrated fare collection system, Vialis for the infrastructure, the readers, the ticketing and fare machines, and Accenture for the integration of the smart cards with the infrastructure, and the operation of the systems for the back office. To support their activities, Hong Kong's MTR Corporation and Octopus Cards act as subcontractors to Thales, providing the central back office, together with their operations expertise, which stems from their participation to the Hong Kong Octopus Card (an RFID-based smart card for the public transport system in Hong Kong). The East-west consortium won the bid that was published by TLS. The bid is

[169] See News feed on public transport issues: 'Consortium wins Netherlands transport ticketing deal'. 3 November 2003.

[170] www.translinksystems.nl; visited 31 March 2006.

valued at approximately 120 Million Euro for the pilot phase; the bid is expected to lead to additional contracts to follow the next five years. The French smart card supplier ASK has been selected by TLS to provide the transit ticketing system. It will deliver e-tickets in a smart card version, based on the Philips Mifare 4k chip, and in a contactless paper version (its CTSS12A contactless paper ticket) to be used for occasional public transport users.[171]

At the right hand side one finds the public authorities that have a say and a stake in public transport issues. Dutch government subsidizes the overall 1.5 billion Euro migration path towards RFID with 100 million Euro (of which 10 million Euro will be reserved for pilots). It has a responsibility as 'director' of the entire introduction. Within Dutch Parliament, discussion is focused on the role of Dutch government: is it able to exert influence when it contributes minimally to the total costs of the migration while it bears responsibility for the overall public transport systems? The regional authorities are responsible for regional public transport affairs, especially related to quality of services and fare prices. The issue of tariff structures for the public transport is a challenging political issue, since it is part of the responsibility of public authorities to decide on the tariffs, and functions as part of social policy. Dutch politics has decided that prices between regions will not be differentiated during the take off, since that would complicate the introduction considerably.

Finally, at the left hand side one finds the consumer organisations, gathered in the Dutch LOCOV organisation (national organisation of consumers of public transport), and the Dutch Privacy Commissioner. LOCOV's priority is to get the best out of the system, which in its view means that the PT-card should be used in a broad array of applications (shopping, facilities around the stations, etc). The Privacy Commissioner has issued a report in which he emphasizes two issues: data retention and the use of the collected data for purposes not directly related to the task of TLS. With respect to this latter aspect, it is interesting to note that TLS has defined as an explicit objective to use collected personal data to extend its services into commercial areas not directly related to public transport.

14.2.3. Technology

As stated above, the East-West consortium has won the bid on providing the technological assets for the RFID-based migration of the public transport system, comprising infrastructure, devices, cards and the accompanying software. It is however under the obligation to develop its equipment and software such that it is open for other market parties to enter; these should be able to offer their own products on the basis of the architecture provided by the East-West consortium. TLS has provided a qualification document in which it addresses the open architecture which is basic to the electronic ticketing system. The architecture consists of the following five levels[172]:

0. Identifiers
1. Front-end Devices
2. On-Site systems
3. PTO systems
4. TLS Central systems

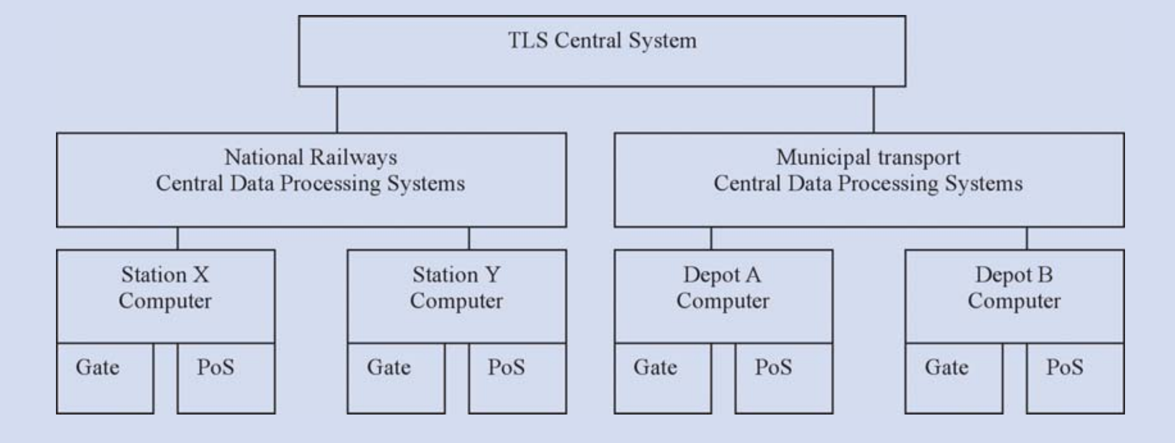
Except for level 4, on which it is agreed that the East-West consortium is the only provider, the other levels are formulated such that any other provider can enter the market.

Figure 14-2 shows the relations between the various levels.

[171] News feed on public transport issues, 'ASK smart cards chosen for Netherlands AFC system', 12 August 2004

[172] See www.translink.nl/media/bijlagen/Qualification_KC3.1.pdf

Figure 14-2: Various service levels as distinguished by TLS (PoS: Point of Sale)[173]



For each of the levels specific requirements have been formulated. We will not cover them all but pay some attention to level 0, the cards (Identifiers). TLS distinguishes:

- Low cost single journey tickets (tickets or re-usable tokens/tickets); the ASK contactless paper-based tickets.
- Smart cards, being :
  - Disposable multi-journey/limited free travel cards
  - Anonymous stored value cards
  - Personalised discount travel/auto-reload cards
  - Personalised free-travel cards and staff cards

In a similar way the other levels are subdivided.

The variety in cards to be provided is considerable, and this has led to specific problems during the Rotterdam test. One requirement formulated by the Dutch government is the one-to-one translation of the existing ticketing system to the RFID-based e-ticketing system. This includes specific reductions for specific groups of travellers (55+, youngsters under the age of 12 years old, but also reduction in case one travels with a group of more than five passengers) and specific subscription types of tickets (a subscription that gives access to all transport modalities for a whole year, a similar subscription but for a period of a month, a subscription for a specific trajectory during a specific period – a month, a year), etc. Introducing all these variations into the system led to considerable delay in the delivery of the entire system in Rotterdam. The Dutch minister for Transport argued successfully in the Parliament that the complexity of this typical system is unique, and it would be wrong to assume that a simple transfer of the Hong Kong system would be possible.

The cards are provided by ASK, a French company that delivers both smart cards and contactless tickets. The latter category is used as disposable category, to be supplied to tourists and for specific events, for instance when a passenger has forgotten his personalised card and needs to buy a ticket on the bus (or tram).[174] The smart cards can be personalised or anonymous. Since TLS wants to gather travelling information in order to optimise the transport system, it wanted to put a premium on using a personalised card (offering them at a cheaper rate than the anonymous card). This however proved to be unacceptable for the Dutch parliament which insisted that both cards would come available at the same price. Passengers have to buy a card at a price of 7.50 Euro. In case of loss or damage no refunds will be made. Passengers have to buy a new card.

[173] Source: Translink KC3 Qualification document. See footnote 172

[174] These are so-called paper-based contactless tickets. The RFID-chip is embedded in a paper folding on which the antenna is printed (metal ink prints). During a pilot in Porto (Portugal) one expected the paper-based tickets to be thrown away, though they could be re-loaded. It however showed that the lifetime of the paper-based tickets was over 3 months and they were regularly uploaded (personal communication José Duarte Vieira, Metro do Porto SA Portugal)

14.2.4. Issues surrounding the introduction of the card

Price

One of the most important assets of the introduction from the perspective of the passengers is whether the new system will increase the price of travelling with public transport. This is a highly political discourse, especially in the Netherlands, which face considerable traffic congestions on the highways and in inner cities. Public transport does only marginally contribute to alleviating the congestion; when the price of public transport would increase due to the introduction of the new ticketing system, public resistance against the public transport might increase and this might lead to further detrimental effects on congestion.

It is however almost impossible to compare both fare systems. In the new system, an access fare has to be paid before travelling starts. This means that short trips (which represents a high volume part of the total number of trips made) will cost relatively more than they do today. The trips will be paid by kilometre instead of per zone, which might decrease the costs for a trip. Overall, it is expected however that roughly 70% of the passengers will pay at most 10% more for their trip, while 30% of the passengers will pay more than 10% more. This is acceptable for the Dutch minister.[175] The 18 regional public transport agencies do have the opportunity to determine their own fares. In order to improve the acceptability of the system, it has however been decided that they all will use the same tariff structure during take off. Dutch central government has already signed mutual agreements with 12 out of the 18 regional agencies (usually provinces; situation May 2006).

Another interesting issue is the status of TLS as a financial institute. The flow of money in the system is such that it needs to be researched whether TLS acts as a formal financial institute, which would mean that specific forms of supervision and of accountability need to be used. This might complicate the introduction of the e-ticketing system considerably. Dutch government expects however, that due to the fact that 'TLS-money', i.e. the monetary value the smart cards represent, only can be used within a closed system of acknowledged institutes (including for instance shopping malls within stations that do accept the electronic money of the smart card) implies that TLS will not be considered to be a financial institute according to European legislation.[176]

Performance

Performance of the system is critical for public perception. By buying a system 'off the shelf' it was hoped that this would improve the quality of services. Due to the complexity of the system, which is allegedly higher than in the Hong Kong situation, quality of services has become a critical asset. The system has to be full-proof and has to have an availability of close to 100%. To safeguard the performance of the system, the introduction phase is subdivided in various phases of increasing complexity. Introduction starts with the Rotterdam metro-system. Initially, only a selected sample of passengers will be able to pay with the smart card (to start with employees of RTM, the Rotterdam partner of TLS). Then, the system is extended to include railways and regional buses, while at the same time GVB (Amsterdam) will start preparation for introduction in the Amsterdam metro system. Finally, when the system is rolled out over the entire country it is expected that some 2 million passengers daily will use RFID-based ticketing.

Societal concerns

Privacy protection is an issue that is usually high on political agendas but that is difficult to address above the level of the generic clauses that are laid down in national Data Protection Agencies. In case of the RFID-based ticketing system the situation is not different. TLS has explicitly stated that it wants to use personal data to improve the level of services offered to the passengers. For one, this means that TLS wants to use travel information to improve the service level of the public transport system (sufficient supply of wagons, fine-tuning travel schemes, may be personalized information on maintenance and delays). On the other hand, it wants to use the information for providing extra services, in and around the stations (some transport related, such as bike hire or taxis, others

[175] Tweede Kamer, vergaderjaar 2005-2006, 23645, no. 135, p. 5

[176] Tweede Kamer, vergaderjaar 2005-2006, 23645, no. 135, p. 6-7

more alien to transport such as shopping). According to the Dutch privacy chamber, TLS is in danger of trespassing the boundaries of the Dutch Data Protection Act, especially in using data for other purposes than these have been collected (purpose binding principle) and that it does not offer clear insight in data retention approaches (quality and accountability principle).

When passengers are offered a choice, it is usually on the basis of an 'opt-out' approach: consent is expected to be given except when one explicitly requests that personal data is not collected for specific purposes. By collecting more sophisticated personal information, the commercial value of this information will increase. It goes without saying that the flow of personal data through use of RFID-based systems (in public transport, but also in other societal domains) offers the possibility to enrich knowledge on personal profiles and enables tracking movements of individuals. This may be at a par with Data Protection Acts.

Another societal concern is the cost structure of the public transport system. Especially the (relatively) poor within a country as the Netherlands are more dependent on a proper functioning and cheap public transport system. As indicated, it is expected that prices on the short distance will rise considerably (over 10% compared to present day situation). Though it is difficult to estimate the consequences of this pricing strategy for use of public transport by low income individuals and households yet, pricing may have an adverse effect on the accessibility of public transport for those groups.

14.2.5. Concluding observations

Introducing an RFID-based e-ticketing system in the Dutch public transport system is a challenge. Technologically, it is a demanding task that has no equivalent yet within the world. It is interesting to observe that even using a system 'off the shelf' is not a guarantee for a smooth introduction. The system needs to be adopted.

From an organisational point of view, the system is a very complicated one, comprising a wide variety of relevant actors. Next to technology providers, an important actor is the central government which is able to impose specific technologically grounded demands (such as open specifications, and the one-to-one translation of existing ticket products to the new situation). The development of the entire system seems to be highly dependent on the outcomes of the political discourse. At the same time, the direct supervision of the central government over the introduction of RFID in the public transport system is limited, due to the fact that it only contributes marginally to the investments required for the full roll-out of the system.

From a commercial point of view, the introduction may prove to have commercial value. This is first due to the change in the fare system (though central government emphasizes a budgetary neutral introduction), second to the increased efficiency (economies of scale, reducing the number of fraudulent passengers), third to the added value the system may have to non-transport activities.

14.3. Case 2: London

London is a city with a very solid and massive public transport infrastructure. Within Greater London, each day 30 million journeys are made with public transport. The tube has some 3 million trips daily, the buses have over 3.5 million trips within the city of London complemented with another 3 million in Greater London.[177] The overall revenue of the London public transport system is 1,5 billion Euro yearly. Each year, roughly 52 million Euro is lost due to fraudulent behaviour. In 1998 it was decided to start introducing smart cards on the basis of RFID within the public transport system. The entire contract was scheduled to cost 1.3 billion Euro, covering a 17 years period of creation, implementation and operation. Capital investments were scheduled to be 240 million Euro in the first years.

The introduction of the smart card would be gradually, so that each component of the entire system could be tested and validated thoroughly. Given the complexity and the scope of the system, this was deemed necessary. Roll-out should start with 80.000 employees and would initially cover

[177] See http://www.tfl.gov.uk/tfl/abt_tfl.asp (visited 12 April 2006) and (IDTechEx, 2006a).

annual and monthly season ticket holders. Full roll-out was foreseen in 2002-2003 having a few millions of card holders able to use a great variety of services. Services should extend to other domains, such as shopping malls. The smart card should become a multi-functional card, which would not only function as public transport ticket but also as electronic purse.

In March 2005, 2.2 million Oyster cards were disseminated. Today, this number has increased to 5.3 million, leading to a total of 11 million trips per week in the tube and 16 million trips weekly on the buses made by Oyster card.[178] The responsible agency Transport for London (TfL) has started a tender to extend the services to the South West main line (to be followed by the North London Railway in Autumn 2007).

14.3.1. Objectives

The introduction of a smart ticketing system in London public transport is directed at realising the following objectives[179]:

- fighting fraud (today estimated at over 50 Million Euro yearly),
- speeding the boarding time (cash will be eliminated from London buses in 2006),
- offering customer benefits (no more queuing, ease of use, outlets off systems sales),
- extending services to include retail sector (in 2006 3850 shops that sell travel passes will accept the travel pass to pay for other services as well),
- offering better travel information (on the basis of actual but aggregated travel information).

14.3.2. Actors

In Figure 14-3 the actors that are part of this case are depicted. The initiator of the card is London transport, succeeded by Transport for London, a London based agency created in 2000, as the integrated body responsible for London's transport system. TfL is a functional body of the Greater London Authority, and is a public private partnership. ITSO, the Integrated Transport Smartcard Organisation, was founded in 1998 as a membership organisation, whose objective is "to facilitate the development of an interoperable smart environment by developing, and then operating and managing a specification for an interoperable smart media environment".[180] Members of ITSO are bus operators, train companies, suppliers to the industry and regional and local authorities, totalling some 75 organisations (of which some 30 governmental organisations all over the UK and 45 private companies). London is not a member of ITSO and this raises some concern about the compatibility of the Oyster card with the ITSO standards. According to TfL, Oyster will in the end be fully compatible with ITSO standards.

Transys, a consortium of EDS, Cubic (each for 37,5%), and ICL (Fujitsi) and WS Atkins as supporting companies, was selected by London Transport to deliver the electronic ticketing system to London. Transys developed the PRESTIGE-project to deal with the introduction of the smart card.[181] Transys has chosen the Philips Mifare chip for use in the London's Oyser smart card project.[182] The smart cards will be manufactured by Giesecke & Devrient, Germany and SchlumbergerSema, UK, while Cubic will be responsible for the readers, and EDS will be responsible for the central information system, the distribution and quality control of the cards.

[178] See IDTechEx (2006a); http://www.tfl.gov.uk/tfl/press-centre/press-releases/press-releases-content.asp?prID=742 (visited 12 April 2006).

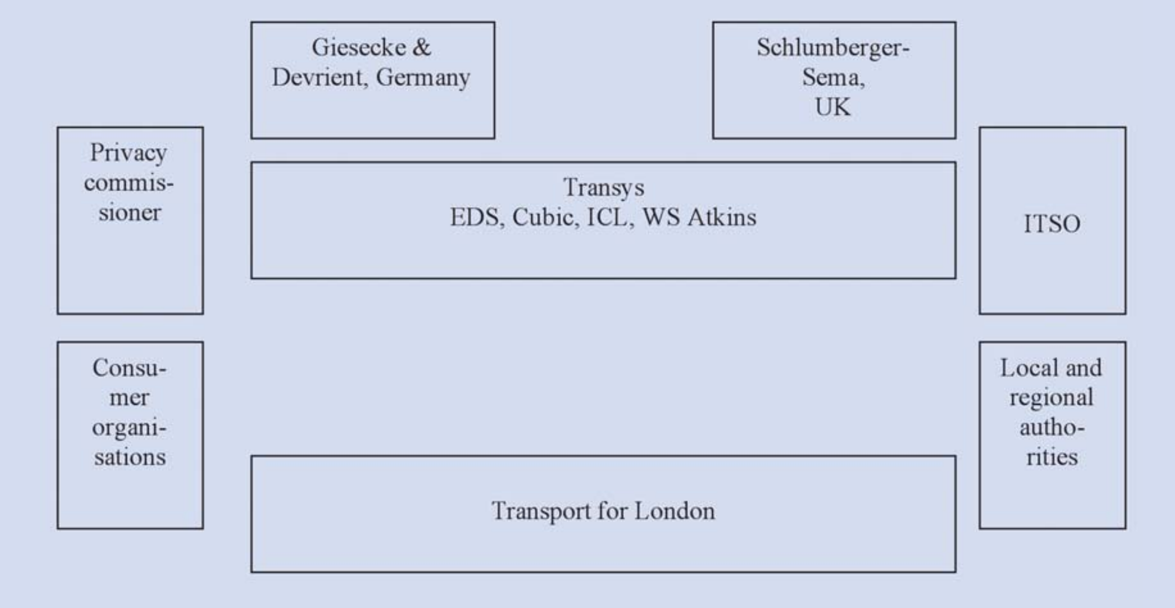
[179] See http://www.tfl.gov.uk/tfl/fares-tickets/2006/downloads/oyster-guides-06/TFL-Oyster_English.pdf (visited 20 April 2006) and IDTechEx (2006a).

[180] See http://www.itso.org.uk/default.asp?contentid=45; visited 12 April 2006

[181] PRESTIGE for: Procurement of Revenue Services for Ticketing Information Gates and Electronics. The project was named the best private finance initiative in operation at the Public Private Finance Awards 2005. See http://www.eds.com/services/casestudies/downloads/transportlondon.pdf (visited 12 April 2006).

[182] See section 2.4 for an overview of the technical characteristics of the Mifare card.

Figure 14-3: Actors in the London Oyster transport ticketing project


Giesecke & Devrient, Germany
Schlumberger-Sema, UK
Privacy commis-sioner
Transys EDS, Cubic, ICL, WS Atkins
ITSO
Consu-mer organi-sations
Local and regional autho-rities
Transport for London

14.3.3. The technology

The Oyster card system will be based on the ISO 14443A standards, to make it fully compatible with the technology standards as proposed by ITSO. The ITSO-standards range from media to data elements, including architecture. Some concerns are raised with respect to the full compatibility of the Oyster system with the alternative scheme as proposed by ITSO. In discussion groups on the internet concerning the introduction of the Oyster card in the various railway lines, concerns are raised with respect to the compatibility of the Oyster card with the 'alternative' standardisation scheme as proposed by ITSO.[183]

The information provided by TfL on the use of Oyster indicates the various forms in which the smart cards and tickets may be used. Cards can be uploaded through Internet. Passing the gates will debit the smart card as authorized. Cards can be personalised and anonymous. A card has to be bought at a prize of 6.50 Euro. Single fares using the Oyster card are cheaper than cash single fares. Each Oyster card can contain up to three travel-cards or Bus Pass season tickets. The card is available at almost 4 000 outlets in the vicinity of buses and the London underground.

14.3.4. Issues surrounding the introduction of the Oyster card

Acceptance of the Oyster card is high. People prefer the card above the cash ticketing system. 85% of people entitled to concessions in London use the Oyster card.[184] No doubt the financial advantage the Oyster system provides above buying a ticket in the traditional way contributes to the acceptance of the Oyster card.

Consumer issues are raised in discussion groups, especially when it comes to double payments due to specific kind of occasional flaws in the system. Though EDS announced that it would train 100 London transport staff to run the project and to answer questions of travellers, this has not taken away concerns.

Privacy

Another issue is that many people are worried about the privacy implications of the card. Each card is uniquely numbered and records each travel details of buses, Tube or train journey made by the holder over the previous eight weeks. The travel information could easily be used for commercial ends by third parties. Regarding this, consumers are worried about the future plans of Transport for London (TfL) to extend the use of the Oyster smart

[183] See Google: Discussion group: subject Oyster.

[184] See IDTechEx (2006a).

card to payments in shops.[185] TfL argues that it only uses this information to better provide customer service and answer customer queries. Though not for commercial ends, BBC News recently published that the Metropolitan Police regularly request journey information about Oyster card users and the use of this information is increasing. In January 2006 it was about 61 times, compared with just seven times in the whole of 2004. In March 2006 the number of requests was 243 times. The information was used as an investigative tool to track criminal movements.[186]

Communication

The minutes of the Strategy and Integration Committee of London TravelWatch, the customer organization for London's transport, mention some other issues. Some of the issues were related with the non-availability of the pay-as-you-go facility on most National Rail routes in Greater London. Many passengers did not understand where they could use the Oyster Pre-pay (former name of Pay as you go) and where they could not and failed to understand why the full benefits of Oystercard could not be made available. Another number of complaints came from passengers who had attempted to use their Oyster Pre-pay for a National Rail journey and found at the end of the journey that the card was not valid. Moreover, these passengers were handed a Penalty Fare Notice for not having the correct ticket. Although TfL produced posters for display at National Rail stations, London TravelWatch found that passengers remained unaware of the terms of conditions of travel and that a number of National Rail stations did not have posters displayed.[187] Since 10 May 2006, TfL announced that in 2008 Oyster would be made available on all national rail services in London. Customers will be able to use their Oyster card in more than three hundred rail stations compared to sixty nowadays. TfL will pay for the Oyster validation equipment in all London rail stations, as well as working with the Department for Transport (DfT) to ensure that equipment will be able to accept other smart cards.[188]

Another communication issue concerned the rejection of Student Oyster card applications, as the authenticating signature on the form differed from the one originally supplied by the university. In some cases the rectification process took more than six weeks and no refunds were offered to the students who had overpaid their travel during these weeks. Students felt being penalised for the incompetence of TfL and the universities in administering the scheme.

Furthermore, a significant number of customers complained about the Oyster Helpline: the Helpline was not accessible or the customers were redirected to London TravelWatch when they had contact with Oyster Helpline; promised call-backs were not made.

Usability

The most significant usability issue of the Oyster card system is that pay-as-you-go customers do not "touch out" at the end of their journeys for several reasons: card readers are not obvious to users and users do not realize that they have to "touch out" when making through journeys to points outside London. The consequence is that customers are not being charged correctly. They often have to pay the maximum price of the journey the customer theoretically could have made.

Besides, users who have run up a pay-as-you-go debt of as little as one pound are prohibited from using any kind of periodical travel-cards on the card until the one-pound debt is repaid.

Customers complained about the lack of outlets where Oyster cards can be "topped up".

Software fault

On 10 March 2005 a software fault meant that the whole Oyster system was inoperable during the morning rush hour. Ticket barriers had to be left open and pay-as-you-go fares could not be collected, which meant a loss of 50 000 pounds. It showed that something had gone awry in passing the black lists with information on travellers

[185] URL: http://www.spyblog.org.uk/spyblog/2004/02/foiling_the_oyster_card.html

[186] URL: http://newsvote.bbc.co.uk

[187] Strategy and Integration Committee of London TravelWatch (2006), Oyster card issues, 14.03.06.

[188] *URL:http://www.londontravelwatch.org.uk/news.php?id=368*;
http://www.gnn.gov.uk/environment/mediadetail.asp

who had been caught the day before. The software fault had been restored at lunch time, according to Transys officials.[189]

So far, the cautious approach adopted by TfL and Transys in introducing the Oyster card in the London Public transport system has lead to considerable delays in comparison to the original planning. Delays are both technical and of political nature. According to high ranking officials, the complexity of this project requires a very cautious planning and moving ahead. One simply can not afford to be confronted with major drawbacks due to failing technology. The extension of the card to include functionalities as an electronic purse has not been fulfilled either. Recently, Times Online published an article where TfL declared that technical and financial partners had not yet provided an acceptable blueprint that would make the system acceptable to retailers without carrying a risk to TfL. This means that the introduction of the functionality of the e-purse will be delayed.[190]

Again, it is argued that one needs a cautious approach in which in first instance travel functionalities are embedded and only when these function properly, extension of services can be considered.

14.4. Case 3: Venice

The city of Venice is characterised by a very peculiar type of public transportation. There are no streets in the city but only narrow roads running by canals so that it is impossible to go along by car. Public transportation within the city and between the city and the islands nearby is by boat (water taxi, water buses and so on). Buses run outside the city centre and to the airport.

ACTV S.p.A. is responsible for public road and water transport in the city of Venice. The company uses 152 craft, including water buses, motor boats, outboard motor boats, ships and ferry boats, to ensure convenient connections between Venice and the islands; plus, more than 600 buses run in excess of 31 million kilometres per year. The main points of access to the city are well connected to the historic centre, with many lines running along the Grand Canal.

Every year about 180 millions passengers are transported producing about 500 000 navigation "movement hours".

Figure 14-4: Venice public transport boat

14.4.1. Pilot

In 1999 a trial of RFID technology for the Venice public transport started. The aim of the trial was realizing an "open telematic square" as a starting point towards Venice as a digital city. The first step in the pilot was the provision of an RFID card, allowing Venice citizens to access multiple services such as: transportation, banking, school, museums, public administration, parking and so on, trying to attract new companies and enterprises to the "square".

The target users of the system in the beginning were city residents, students and people whose main business site was in the city of Venice. At the end of the pilot the system would be extended to tourists.

The system had to support the use of contactless tickets and cards; plus it had to support ticket acceptance, recharging and control.

Initially, some 200 users were involved in the trial; they were selected mainly among the employees of the companies responsible for the elaboration of the trial; this was done to enhance useful feedback on technical aspects concerning the system.

[189] See IDTechEx (2006a)

[190] http://business.timesonline.co.uk/article/0,,9077-2160143,00.html, May 01 2006.

The pilot system was deployed along the Grand Canal. Tag readers were placed on buoys in the middle of canals where boats (equipped with RFID tags) could be monitored. Information on boat transit was going to be used for float management aiming at optimising the passenger waiting time and trying to regulate the high boat traffic in the canals responsible for damaging building and bridges in the city.

The cards provided to users were also designed to support access to services provided by municipality.

14.4.2. Actors

The actors involved in the trial were several public administration companies, companies in charge of giving value added services, banks. Among them:

Telecom Italia, telecommunication operator. Role in the trial: Communications activities

TSP, a company owned by Banks, which develops banking type services.
Role in the trial: management of financial transactions: the cards needed to be initialised according to a specific layout. TSP also provided the cards readers.

INSIEL (52% Finsiel) software and service provider together with **VENIS** (owned by Telecom Italia 51% and Venice municipality 49%)
Role in the trial: system development and deployment

IBM
Role in the trial: twofold. Project leader and provider of systems (i.e. server)

ACTV: Actv is the company which provides transport service, on both land and water, in Venice. The company has fleets of water and land buses for services in the centre, suburbs and out of town.
Role in the trial: providing public transport fleet.

14.4.3.Services

When the trial ended, ACTV decided to develop a real system to be provided to the city of Venice. A call for tender to realize an RFID-based public transport system has been won by the French branch of the ASCOM Company, an international solution provider with competences on Wireless Solutions. ASCOM is in charge to develop and deploy the RFID-based public transport system using contactless smart cards.

By the end of 2006 the system will be accessible to residents only for water transport. The costs of the overall system are evaluated at about € 13 Million; for the water transport the costs are about € 6 Million

Initially the card will be available only to residents. Residents buy the card charged with a number of trips and every time they take the water bus one trip is taken out from the entire amount. When the card is empty, it can be recharged and reused. In order to exploit the full potential of the system it will also be open to tourists in the future. Of course in case the cards would be given to tourists it would be used just for a few trips, sometimes even only one. So other services are going to be designed and provided (such as museum tickets, concerts, theatre and restoration) in order to exploit the cost of the card.

14.5. Discussion

On the basis of the cases presented in the preceding sections we can tackle the issues raised in the beginning of this case-study. We will first present the findings with respect to drivers and barriers of introducing RFID in public transport, and continue with a discussion of the market potential, user aspects, and security and privacy aspects.

14.5.1. Drivers

In the cases presented a number of drivers have been formulated that bear relevance for the introduction of RFID in public transport. These drivers can be combined in one overarching theme: *modernisation* of the public transport system. By means of RFID-based ticketing systems it becomes possible to gather travel information that may be used to optimise various elements of the everyday logistics within public transport. Part of this efficiency operation is the positive effect on reduction of boarding time (including time it takes to buy a ticket).

Overall, critical issues for introduction of RFID-based cards and ticketing systems relate to understanding the business model which is going to be impacted by the new system (actors, services, processes already existing), the identification of the necessary actors and services to be offered, as well as the organisation of actors commitment, considerations concerning users segmentation, integration with the banking systems and integration with already existing systems.

The handling of passenger flows is enhanced, just as checks on the validity of tickets. This latter implies that *fraudulent uses* of public transport (using without paying) will be reduced (though precise figures on the level of reduction are yet absent).

Because RFID-based tickets will also be used to guard off parts of the stations and because aggression related to fraudulent travelling will be reduced in line with the reduction of fraudulent travelling itself, one expects that *safety* on public transport stations will be improved. This 'side-effect' of introducing RFID-based ticketing is nevertheless an important asset and may be used to convince the public of the benefits of the migration towards RFID-based ticketing.

Another driver for the introduction of RFID in public transport ticketing is the *value added* that can be found in using the tickets for other situations. In this case, it is not the direct information related to public transport travelling (i.e. the ticket information: which trajectory may the passenger travel) but information that can be stored extra on the ticket. In the London situation there are quite concrete plans to extend the functionality of the PT-chip card with an electronic purse, enabling travellers to use their purse for shopping in the shopping malls surrounding public transport stations. This is an interesting extension of the functionality of the cards. Closer by, the card can be used for taxi's, for hiring a bike (which may be a service offered in the Netherlands, where hiring a bicycle is part of the services offered at the main railway stations) and for using baggage lockers. It may be extended to include offering tourist services. In the Venice case, one is considering the extended use of the cards for accessing museums, paying restaurants, booking concerts. This might contribute to separate and manage different groups of users (citizens and tourists) and to offer better tuned services to both groups.

14.5.2. Barriers

Barriers with respect to RFID-based ticketing can be found in a number of issues. To start with, all pilots studied were not able to keep to original *time schedules*. The pilots represent complex technological challenges, embedded in complex organisational changes. Buying the basic technology 'off the shelf', which is the case in the Dutch and the UK situation, does not alleviate the technological burden of fine-tuning the entire system to the specifics of the public transport system at hand. The entire system needs to be built up from scratch, on the basis of requirements and specifications as provided by public transport companies. The entire system (including the gates, other check points, the point of sales, the system per participating company and the overall information system) is a very complicated one, and typically one in which specifications and requirements are changed during the construction phase of the system. The experiences with the cases studied thus questions the possibility to migrate a system developed in one situation to another situation with different characteristics (tariff structure, companies involved, infrastructural aspects).

It is also subject to the results of *political reality*. Given the long lead time of these pilots (typically in the order of three to five years for full-fledged implementation and roll-out of RFID) there is an intrinsic uncertainty in the entire introductory phase, because of politically motivated changes that have to be implemented. These changes may refer to tariff structures that change during the project, to security mechanisms, to privacy issues to be taken aboard, etc. The role and position of governments depends very much on the local situation. In The Netherlands the national government wants to have the driver's seat, but realises that this may be impossible given its relatively modest contribution to the total investments needed for the full roll-out. In the UK, the Transport for London is part of the London Greater Authority. This Authority has released a master plan detailing the issues of future London transport. TfL has outsourced the contract to Transys, a consortium made of ICT providers and system integrators. This is comparable to the position of the East-West e-Ticketing consortium in the Netherlands.

The issue of *standardisation* may be a barrier. Though ISO standardisation seems to be the starting point for each pilot under study, problems are raised in the London situation because of the non-compliance between Oyster-standards and the standards as proposed by ITSO. Within the Netherlands, the system is developed on the basis of the Hong Kong Oyster system as well, but we have not found problems with standardisation in this case. Concerns on the ISO 14443 standards are raised. The standard is considered to be incomplete thus hindering open interoperability and competition among vendors.[191]

Another issue is the issue of *costs versus security*. In case of single journey tickets, the costs for security may be low, since the tickets may not be rechargeable. But, as the project in Porto showed, even paper-based tickets can be used as rechargeable cards. In that situation, security measures need to be improved. Michael Barjanski, head of Public Relations of RATP considers this to be a problem: "Regarding security, no progress in that domain has been made. RFID tickets cannot be securely used in rechargeable mode, and raise great risks for titles that have to be stored, and for titles with no or a long term limit date for use. Therefore, RFID tickets will only be qualified for that part of tickets sold for "immediate boarding".

The RFID ticket has been a paradox - It is cheap and secure, but for the uses for which it is secure its costs are not reasonable, and for the uses for which the costs is bearable it offers no security. Some experts even think that using magnetic atripe cards are more secure.[192]

Finally, the roll-out of the entire system requires *huge financial investments*. Pay back times are estimated at a few years, but it is not clear where this is based upon. Investments in the order of 1.5 billion Euro are mentioned for both the Dutch system and the London system. We have not had time to search for the business models that indicate how one expects to turn the investments into profits. One aspect – reducing fraud – offers an interesting asset, but is not substantial given the huge investment costs.

14.5.3. Market potential

The market potential for RFID in e-ticketing systems seems to be high. Within the pilots studied, one expects to disseminate a few million tags, with accompanying infrastructure and information systems. Of course, when a system will be introduced, demand for new cards will be high. Over time this demand will slow down. But new innovations may trigger new uses and new markets (for instance NFC as a follow up of present day chip cards, or multi-functional smart cards which have additional e-purse functionality). Within the pilots studied a distinction is made between smart cards and smart tickets (paper based). The tickets will be provided on a one-time use basis and may serve as a continuous source of income. Passengers will have to pay for a card (in the order of €6,- to €7.50 to pay for the costs of providing and personalising the card). In case of loss they have to buy a new card. After the introduction phase of the cards (substitution market) there will be a continuous request for new cards (replacement market). Adding new functionalities to the card will enhance the usability of the card: new application domains, new modes of usage, new markets.

14.5.4. User acceptance and trust

User acceptance may be expected to be a crucial issue in this domain. In the UK case, travelling with the Oyster card offers financial benefits to the passenger over using the traditional tickets: the same journeys are less expensive with an Oyster card than with a traditional ticket. This has promoted the user acceptance of the Oyster cards. Within internet, discussion groups discuss adverse experiences of users with tickets (those that were not accepted by the gates, or those that were charged twice, etc.). One system failure led to a temporary breakdown of the system. When these kinds of events occur on a regular basis, this could have an adverse effect on trust. As far as reported, this only happened once in the past few years and the failure was allegedly to the benefit of the passengers.[193]

[191] IDTechEx database http://rfid.idtechex.com/knowledgebase/en/casestudy.asp?casestudyid=1043

[192] Michael Barjanski at the Smart Label Conference 2004, quoted in IDTechEx knowledge base: http://rfid.idtechex.com/knowledgebase/en/casestudy.asp?casestudyid=233 (visited 13 July 2006)

[193] IDTechEx (2006). London – transport for London TfL, Oyster Card, UK

14.5.5. Privacy and security issues

In line with the issue of acceptance is the issue of privacy and security. In the cases studied, a choice is offered to passengers to opt for a personalised card or an anonymous card. In the latter case, the public transport organisation is not able to profit from the data collected on individual travels and can not offer additional services to passengers on the basis of specific profiles. Within the Dutch case, one wanted to offer the personalised card at a reduced price compared to the anonymous card, in order to get as many passengers accepting the personalised card. This has however been corrected by the Parliament at a latter instance. Both cards are offered at the same price. This is also the case in the UK. Within the Netherlands, the Privacy Commissioner has reacted to the plans of the Dutch Railways (NS) to use the data for commercial purposes. It objected the absence of clear guidelines with respect to data retention and it objected the too broad use of data gathered for the purpose of public transport issues. TLS Card Issuer (the organisation that is responsible for the management of the data) defines as legitimate purposes for using data on the card the production and release of the card, the reconstruction of the personal card, the management of credits on the cards (the e-purse), the facility to block cards that have been reported as missing or stolen or lost, the guaranty of restitution of the credit that is left on a card, services to the customer and internal management. The discussion between the Privacy commissioner and NS (and as part of their consortium TLS) has not been settled yet (situation July 2006).

Collecting data on individual travel schemes is possible with personalised cards and with cards containing an ID (that need not be co-related to a person). Privacy dangers are profiling and tracking. During a Dutch workshop organised by the Dutch parliamentary technology committee the example was brought to the fore of the London Oyster system being used to search for criminals on the basis of suspect travel schemes. Old discussions about so-called ‘Rasterfahndung’ techniques[194] may pop up, even when the rationale behind the search may be perfectly legitimate.

14.5.6. The European situation

One can experience a trend towards RFID-based ticketing systems within public transport. The benefits of RFID (faster throughput of passengers, increased ease of use, opportunities to improve the efficiency of the transport system, opportunities to offer additional services) seem to outweigh the disadvantages (high initial costs, high human resource investments to ‘get the thing running’, long lead times). Regarding the European actors involved, Philips as chip producer plays an important role, while other European micro-electronic firms (ASK, Infineon, STMicroelectronics) play a substantial role as well.[195] The paper-based C.ticket of ASK is used in many trials and pilots. Contrary to initial intuition, paper-based tickets seem to offer the same potential and functionality – using the same RFID-chip – as contactless smart cards, though their lifetime is – of course – shorter. EU-consultancy firms play an important role in the consortia that are formed to guide the introduction of RFID-tickets in public transport and the accompanying transition for the back offices. The number of pilots and projects will increase in the years to come, requiring more specialised knowledge and firms that are able to guide the accompanying transition processes. Up till now, each new project represents a new situation which requires rethinking the approach. Even in case of using ‘off-the-shelf’ systems, as in London and the Netherlands, the technology providers needed considerable time and resources to adapt the system to the local situation. There is no ‘one size fits all’ approach available yet. Still, one should expect the learning curve to be steep in this initial phase, thus offering the opportunity for economies of scope in successor projects.

Though we do not have in depth information on all pilots/projects, a few projects explicitly urge for transparent and interoperable systems, thereby organising a levelling playing field and increasing the competitive edge on these systems within Europe. Having major players (Netherlands, London) opting for transparency no doubt will have a beneficial effect on the sector as a whole.

[194] Rasterfahndung is a German term used in criminology, which means “pinpointing of suspects by means of computer analysis of data on many people” (Oxford Superlex, Oxford University Press, 1994-96)

[195] Meanwhile, the situation has changed. Philips has outsourced its chip division into to newly founded firm NXP (for Next Experience). NXP consists of 6700 employees, housed in one of its 24 centres all over the world, with an annual turnover of 4.8 billion Euro (2005 figures) and an R&D investment of 950 million Euro (2005).

Part four

Policy analysis and recommendations

Institute for
Prospective
Technological Studies

15. Policy analysis and recommendations

The foregoing chapters have detailed various aspects to the emergence of RFID technologies. In this final chapter we will use the policy relevant insights that have been acquired to construct a policy analysis. The guideposts used for this analysis are the following:

1. Are there differences in the approach of the stakeholders due to variation in Member State markets? Does this have an impact on EU market integration? (section 15.1)
2. What are the perceived (if any) EU-wide benefits? What role may the public sector play in achieving this benefit? (section 15.2)
3. What are areas for public policy intervention? What are appropriate policy actions? (section 15.3)
4. What are policy options to further research needs? (section 15.4)
5. What policy recommendations can be given to the European Commission on the basis of the overall results of this project? (section 15.5)

15.1. European RFID stakeholders and markets

RFID stakeholders can be differentiated in the following categories:

- vendors (including firms producing tags, interrogators, middleware, system integrators, and services providers)
- end users (including automotive, healthcare, government services, manufacturing, retail, consumer goods, etc;)
- research institutes and academia
- governments

A recent study in RFID workforce distribution shows the end-user market by far is the biggest market (almost 90% of RFID workforce), followed by the vendor market (almost 10%) (RFID Tribe, 2006). Academia and government contribute (in terms of workforce) only marginally. The strategies of the various (European) stakeholders differ depending on their position in the value chain. At present, system integrators and service providers are invited by end users to support the RFID implementation process. *End users* will follow the dynamics of their (home) market, while *system integrators* and *service providers* will follow the logic of the end users.

Hardware development (tags, readers) is a worldwide game. Europe is clearly visible on the market with important players as Dutch based Philips, France based ASK and Swiss based EM Micro-Electronics. ASK has developed the innovative paper-based C-ticket, which is in use in a number of public transport trials and projects. Philips has a broad range of RFID chips available, for different frequency ranges and different application areas. The Mifare and HiTag chip are but two of the well-known examples of RFID-chips. The recently outsourced semi-conductor part of Philips (called NXP for Next Experience) produces a high portion of the Philips RFID chips. In relation to hardware equipment like *readers*, Europe houses a number of suppliers. Reader development is dependent on the application domain in which they are used. The case studies we have performed show a fragmented picture on this part of the market: readers are provided by both European and US-based suppliers.

Figures about the European market, at country level, are not known in detail for RFID. To get a hold on the position of Europe we have to make use of 'circumstantial evidence', in this situation the information provided by the IDTechEx database.[196] This database collects publicly known data about RFID initiatives. In Annex 8 an overview of European case studies in a broad range of RFID application domains is presented. This overview shows:[197]

[196] www.idtechex.com. During the time of the project we have had access to the database.

[197] IDTechEx database. Accessed 16 October 2006.

- For Europe a total of 715 cases are documented on RFID; this is roughly equal to the US (with 812 cases documented).
- The new member states are only marginally represented in the database, with a total of 26 cases (of which eight are military).
- The UK (255), Germany (120), France (86), Netherlands (62) and Italy (40) are the most active European countries; they are active in all application domains the database discerns.
- Leisure and sports is the application domains with most cases, followed by logistics, financials (including security and safety) and passenger transport/automotive (all over 90 cases). Retail, healthcare, manufacturing and military follow (30 – 90 cases). Airports, animal tagging and libraries are closing ranks (20-30 cases) while laundry so far has only 3 cases. Laundry relates to item level tagging (surgical garments, wardrobes).

Figure 15-1: Position of EU countries in adopting RFID[198]

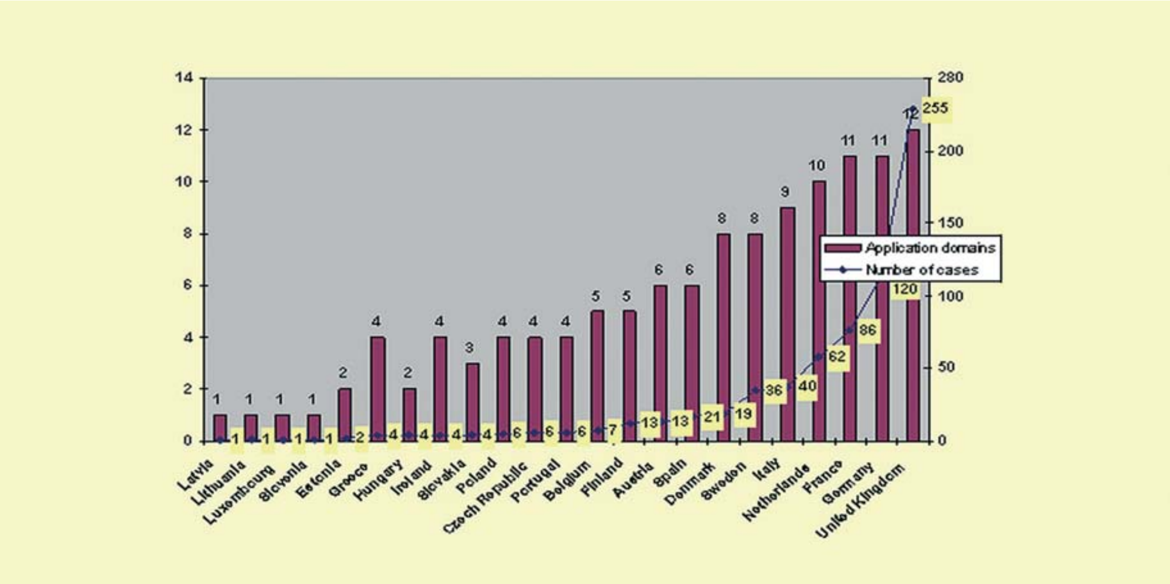


Figure 15-1 shows the relation between the number of application domains and the number of cases per country: the more cases a country has the more application domains are encompassed. The figure shows a gap between the leading countries (UK, Germany, France, the Netherlands and Italy, followed by Denmark, Belgium and Sweden) and the tail of European countries in adopting RFID.

Member State markets clearly vary. We can differentiate between three distinct groups: the countries which have only recently started with a number of RFID projects (Latvia, Lithuania, Luxembourg, Slovenia, Estonia and Hungary), a group which has a moderate track record in RFID projects (Slovakia, Poland, Greece, Czech Republic, Portugal, Finland, Poland Austria and Spain) and a group which already has an established track record with a number of RFID projects (Belgium, Denmark, Sweden, Italy, The Netherlands, Germany, France and the United Kingdom).[199] The market of RFID is diversified as well: from massive implementation of simple tags to high value added uses of smart cards. Supply chain use of RFID is expected to be in the lead of RFID developments for the next few years. Some RFID application domains are driven by regulatory considerations (an-

[198] Left axis: number of application domains; right axis: number of cases (see Annex 9 for additional data)

[199] Measured in terms of cases. All the 'slow starters' are countries with a moderate population. If corrected for the size of the population a distinct perspective would arise. But even then, it shows that the slow starters are only very moderately visible in one or a few application domains.

imal tagging, identity cards). The size of the market (number of animals to be tagged, number of people to equip with an identity card), market driving forces (enforcing use of RFID by dominant market parties) and expectations concerning value added services (use of ID-cards, combination of animal tagging with food tracking) will drive stakeholders' participation. Other RFID application domains are dependent on initiatives taken with a public-private background (healthcare, libraries, public transport).

Stakeholders may be aware of differences in the innovative landscape within a specific country, the awareness for RFID opportunities, the support from public authorities and governments for pilots and trials, and the opportunities for value added services. They will try to step in trials and pilots that may provide them a privileged position (being first to the market, opportunity to trial specific RFID uses). Markets that are identified in the cases we have done are markets with a huge potential. RFID in public transport, for instance, relates to projects worth a total of over a billion Euro (UK introduction of Oyster, Dutch introduction of RFID nationwide). All special appliances markets (animal tagging, healthcare) are potentially big markets. The two most important market players are:

- vendors: the more generic technology providers (tags, readers, software) operate worldwide; system integrators and service providers will tune their activities to promising markets;
- end users: they will act more locally and will be dependent on opportunities offered in public sector domains and opportunities created in the private domain.

End users will rely on vendors (including consultancy firms) for the implementation of RFID in the early stages of its development.

The second issue is whether the differences have an impact on EU market integration.

RFID markets are diversified markets; specialisation in specific application domains is likely to occur. Diversification in hardware (tags, readers) and software (middleware, services) will not primarily be driven by differences between countries but will primarily be driven by the promises of specific applications. Diversification in implementation will be driven on a case by case basis, and will depend on future prospects, future markets, and available expertise and know-how within a specific application domain.

Roll-out of RFID-based systems in various applications has only just begun, so it is difficult to extrapolate the findings so far over what this implies for market integration. On the basis of the characteristics of RFID projects – determined by the specific application domain – we are tempted to say that indeed the differences in attitude towards RFID may have an impact on EU market integration.

The countries that are yet lagging behind may profit from their backward position once RFID has grown mature. They can learn from the mistakes of the early adopters. Not all trials and roll-outs have been and will be successful.[200] The technological playing field of RFID is not mature yet. The future, economic and societal prospects of RFID are not entirely clear. The Return of Investment dispute is far from settled. The societal debate (privacy) is far from settled either. Those countries leading the way will be confronted with the initial problems the introduction of RFID brings with it. But they will also profit in terms of gaining experience with the introduction of RFID in diverse applications, and the creation of a knowledge infrastructure around RFID implementations, and commercialise this knowledge.

Given the stage of RFID developments at the moment (the early adoption stage) and the position of RFID in the 'hype-cycle' (Gartner, 2005) we expect the impact of RFID on market integration to be modest, though differences between countries will certainly be aggravated in the short term.

15.2. EU-wide benefit of RFID

Figure 15-2 presents an overview of European strengths and weaknesses, opportunities and threats in the field of RFID.

[200] It is however difficult to track failed pilots; those responsible for the pilot will not happily admit that the pilot failed. Usually other reasons (lack of funding, withdrawal of commitment) will be brought to the fore. Still, it goes without saying that especially the failed pilots and projects entail rich experiences which can deliver fruitful insights for other parties.

Figure 15-2: SWOT analysis of EU-wide implementation of RFID

Strengths
- Europe houses part of the big RFID suppliers;
- High market potential;
- Leading EU countries with RFID focused attention (UK, France, Germany, The Netherlands, Italy);
- Focus of attention comparable to USA;

Weaknesses
- Many European countries with only marginal attention for RFID;
- No level-playing field for RFID across countries;
- No harmonised frequency policy in the EU;
- Vulnerable image of RFID - Trust issue;

Opportunities
- Increasing efficiency of production, trade and services;
- Creation of new services, new workplaces;
- Spur for economic development
- Increased convenience in citizens' everyday life;
- Increased security, reliability and trust;
- Stimulation of research and development of related technologies (enabling, enhancing and concurrent)

Threats
- High initial and high transition costs;
- Rapid technological evolution may help displace a technology before it is widely adopted;
- High hidden costs (societal and organisational such as for training and education);
- Possible job losses due to wide deployment;
- If not implemented properly, RFID may bring a number of threats to privacy and security (Function creep, surveillance capacity);

The SWOT analysis shows strengths and opportunities to be balanced against weaknesses and threats. The identified strengths are part of weaknesses and threats as well: only a few European countries are active in RFID; the public climate towards RFID is vulnerable. Other factors add to the challenges with which widespread diffusion of RFID has to cope with: hidden costs of RFID (training and education) may be high, the role of legislation is yet unclear, and negative experiences may have an effect far beyond the domain where they originate from.

The perceived *EU-wide benefits* of RFID are of an economic, social and/or political nature. They can be found especially in areas where European integration, cooperation and coordination have progressed most. The fight against terrorism is one such area. The fight against animal diseases is another. The coordination of European research is a third. In these domains RFID may contribute to realising European benefits. The effort in achieving this however is not trivial. Experiences with RFID until now indicate a number of problem areas: The possibility to gather personal data with RFID raises privacy issues, law enforcement to enforce the use of RFID in the tagging of animals knows many exceptions, and the creation of a European research agenda on RFID requires cooperation between different parties in the value chain (to unravel security issues for instance).

The RFID technology market is a global market, with globally operating vendors; the RFID end-user market is a 'local' market with aspects going beyond the state frontier (identity cards, healthcare, animal diseases). Economic benefits thus are either globally or country specific.

Next to the EU-wide benefits, application of RFID in specific domains may be beneficial to the European population at large. Public transport, health and retail are three of these domains. Use of RFID is expected to increase the cost-effectiveness of public transport, to fight fraud, to increase social safety and to introduce additional services; within healthcare RFID is expected to combat counterfeiting, to increase the quality of care, to improve the availability of health information, to prevent surgical mistakes, and to reduce theft of medical equipment. In the retail sector RFID is expected to lead to less out-of-stock items, to more efficient logistics, to better consumer profiles, to better quality information. These are clear benefits which show up in the short return on investment periods, indicating the high economic value of the RFID implementations. But there is a price to pay as well: organisations have to restructure their business processes in order to benefit from RFID adoption; they have to invest in the novel RFID infrastructure before profits will be made. For individuals privacy may be at danger: individuals will become more transparent due to the collection of information related to specific behaviours.

Given these advantages for Europe as a whole and the implications for European countries, European public policy should focus on:

- Reaping the benefits of RFID as supportive/enabling technology for European-wide policy issues (terrorism, security, animal diseases, sustainability)
- Supporting European roll-out of RFID-enabled activities with clear societal and economic benefits.
- Keep an eye on the balanced introduction of RFID (within application domains, within countries and within specific user constellations).

In the next chapter we will elaborate the European opportunities for policy intervention.

15.3. Issues for public policy intervention

The public sector may play a role in achieving these EU-wide benefits. The activities of the EU and of the separate Member States can be subdivided in a number of categories, which are related to specific components of the RFID system.

Figure 15-3: RFID systems approach

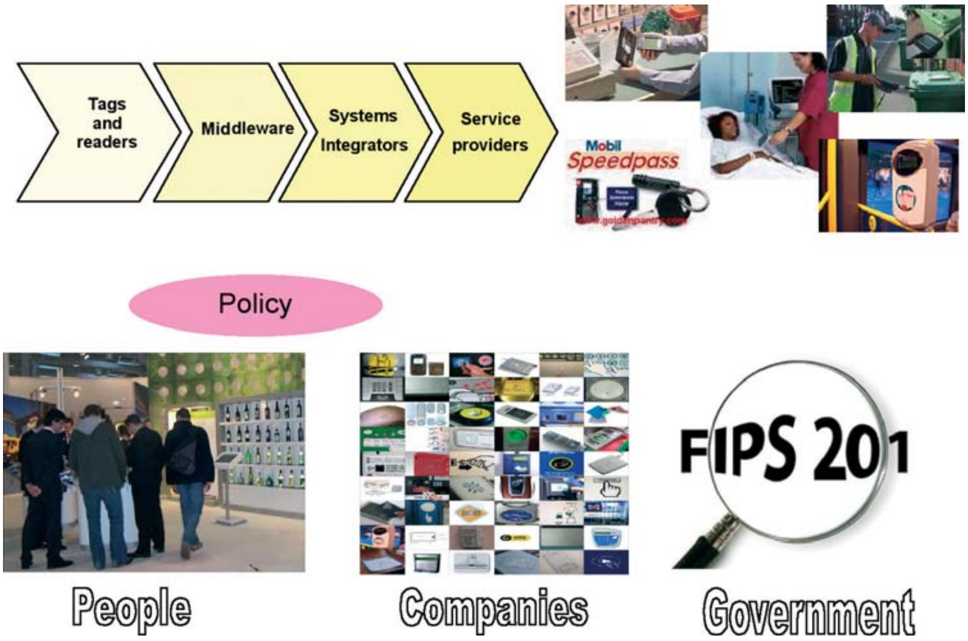


Figure 15-3 shows the RFID system on top and the various application domains in which RFID may be used, while the bottom part of *Figure 15-3* presents the three main actors. Policy issues such as the ones discussed above link actors, application on areas and the components of the RFID system.

EU public policy activities can be of various kinds: creating beneficial conditions for the widespread adoption of RFID, raising awareness, enforcing specific standards and implementations, stimulating research in technical and non-technical aspects of RFID, developing and implementing innovation policy instruments and for governments adopting a role as launching customer.

Table 15-1 presents an overview of public policy initiatives related to the RFID system and the application areas.

Table 15-1: Overview of issues for public policy intervention

	Policy approach	Activities
RFID tag-reader	Creating beneficial conditions	Setting up frequency policy Contributing to standardisation of data formats
	Raising awareness	Indicating presence of RFID readers Raising awareness on health issues of RFID readers Raising awareness on electronic waste related to RFID
	Stimulating research	Funding or stimulating research on - Advanced RFID tags - Security issues - 'Privacy by design' - Patent research - Health issues - Electronic waste
	Innovation policy instruments	Updating existing legal framework (privacy directives, WEEE directive)
Application domain	Creating beneficial conditions	- Stimulating use and/or development of standardisation of data formats - Stimulating use and/or development of interoperability and integration of back-end systems - Stimulating and advancing Training and education
	Stimulating research	Funding or stimulating research on - Interoperability - 'Best practices'
	Raising awareness Innovation policy instruments	- Inventorying 'Best' practices - Research funding - Subsidizing pilots and trials - Promoting specific innovation instruments for lagged countries and regions, and slow-uptake application domains

15.3.1. RFID tag-reader:

The tag-reader combination differentiates the RFID system from other technological systems that make use of identification technologies. Public policy intervention dedicated to the tag-reader combination will encompass RFID-specific elements which will not be found in other identification systems.

Reader-tag systems function at specific *frequencies*. The frequency used is dependent on the specifics of the application (required read range, data transfer rate, read-write capacity, data processing capacity). Frequency issues are covered by a number of international organisations (ISO, ETSI, CEN). Though frequency issues seem to have been settled with the recent adjustment of the UHF-band for Europe (leading to a tenfold increase of available frequencies in the UHF region compared to the original situation), two issues remain problematic. First, within Europe not all countries have adopted the frequency regulation proposal. This is a barrier in the EU-wide dissemination of RFID. Second, the US still has a comparative advantage in this frequency domain due to a greater availability of frequencies that may be used in this band (and that may be important for item level tagging). This might jeopardize the position of Europe in two ways: the need for readers that can function on different frequencies (the EU and the US spectrum) will continue to exist, and there is a possibility that the available frequency band in Europe will result in having insufficient capacity before this happens in the USA. Thirdly, larger users of RFID have reported that specific configurations of RFID readers will fail when they operate in close proximity.[201] The frequency dispute thus is not settled yet.

[201] Richard Foggie, RFID Validation workshop 3rd October 2006. The specific configuration relates to use of narrow waveband and use of Listen before Talk protocol in EN 302 208. This situation can not handle more than 70 readers at once.

An important aspect for the widespread diffusion of RFID is uniformity in the *data formats* (the identification data). Identification data will be domain specific. Within animal tracking for instance, use is made of ISO standards to identify countries. Specific identifiers – such as identifying a specific farm – are part of negotiations relating to the remaining data fields. Up till now, the Electronic Product Code is the most elaborate version of a data format standard including the middleware (Savant) and the Object Name Services. Not all EPC standards are however compatible with ISO standards for air interfaces, though the situation seems to improve for the recent EPCglobal Class 1 version 2 protocol.

European policy could embark on stimulating a specific European input and response to ISO- and EPC-committees.

A very important design aspect of the RFID reader-tag combination is the so-called '*privacy by design'* approach. RFID is often looked at as a technology in which privacy and security go hand in hand. Security measures may positively impact on the ability to protect one's privacy. 'Privacy by design' implies that privacy is considered to be one of the design criteria of tags, readers and backend systems. There is a straight line to the discourse on Privacy Enhancing Technologies in which anonymity, pseudonimity, unobservability and unlinkability are the basic characteristics to be realised in an information system. Privacy by design may be a decisive instrument in raising public trust in RFID-systems and a number of researchers in the field of privacy and security state that "privacy by design" should be promoted.[202] Within the European consultation workshops on RFID (held in the spring of 2006) privacy by design was mentioned frequently as the process with which to guard privacy and secure the communication between RFID tags, readers and backend systems. The Privacy by design approach is a layered approach:

- Technological: one could opt for 'consumer in control' solutions supported by appropriate encryption approaches. R&D funding governments as launching customers are options to research the technological merits.
- Organizational: anonymization, system design, new business models. This may require rethinking the privacy principles in use today and give room to more radical principles.
- Societal (rule-based protection): self-regulation and law are the most obvious activities here. Policy options are: compliance verification and harm- or abuse laws.[203]
- Europe could stimulate the on-going exploration of the privacy by design approach.

Privacy by design goes hand in hand with *security measures*. The security concerns for RFID are manifold, and range from preventing direct attacks to the reader, the tag and the reader-tag communication (unauthorized modification of data on tag and/or reader, de-activation, detachment or destruction of the tag, eavesdropping, blocking, jamming and relay attacks) to attacks to the backend systems. The latter ones are not typical for RFID but encompass a broader class of threats. Starting point for a security policy is to have minimum data on the tag and to transpose all sensitive data to the backend system. Use of encryption should be made compulsory in high sensitive systems (identity cards, health sector).

Europe could stimulate research on security of passive RFID tags, including security architectures of RFID systems.

Awareness raising with respect to RFID readers and tags means offering people the opportunity, whether they are users or not, to be notified of the presence of RFID systems (tags, readers) and to be notified about what data the reader collects and to what organisation the collected data will be disseminated. Plans as to in what technical way to enable notification of the presence and data content exchanged of ambient RFID systems are under development. The Free University of Amsterdam for instance, is preparing a so-called RFID-guardian, an instrument that enables people to locate tags in goods they have bought or intend to buy, to signal scans and to prevent unauthorized

[202] See (Floerkemeier et al., 2005), (Juels, 2005).

[203] Jeroen Terstegge, RFID Validation workshop, 3 October 2006.

readings of tags.[204] Readers and tags can be made such that they show their presence when requested ('privacy by design'). Europe could further stimulate the development of devices that may promote trust in RFID uses. It could also increase awareness for RFID-based applications by the public to ensure a better understanding of the changes at hand.

Research as to the health effects of readers so far has shown that radiation levels are sufficiently low that no thresholds in terms of *emitted radiation doses* will be trespassed (RIVM, 2004). Nevertheless, some concerns remain regarding long-term exposure to specific levels of electromagnetic radiation. This may especially be the case for workers in the logistic chain who will be called to work on a permanent basis in an environment with relatively high powered readers (~5 Watt) in the ultra high frequency spectrum. Another concern relates to the possible detrimental effects of permanent exposure to radiation in specific frequency areas for people carrying a cardiac pacemaker.[205] Finally, the consequences of exposure to a cocktail of frequencies and powers are still not sufficiently researched. Europe should stimulate research in health issues wherever knowledge about the consequences proves to be insufficient. Adoption of a Precautionary Principle with respect to health issues should be considered.[206]

RFIDs themselves are composed of *hazardous waste*. Two European directives can be applied: The Directive on Waste Electrical and Electronic Equipment (/2002/95/EC) and the Directive on Reduction of Hazardous Substances (2002/96/EC). According to the European Commission, no extra precautions need to be taken with respect to the interpretation of these two directives. When RFID is only part of packaging – of electronic equipment – WEEE is not considered to be applicable. The RoHS directive determines that specific substances which are considered to be highly hazardous may not be used in the construction of RFID chips (neither in any other chip). Further awareness may be needed against new forms of hazardous substances, relating to RFID manufacturing. In the USA for instance, concerns are voiced regarding the use of printed electronics.[207]

Finally, what is often questioned is the appropriateness of the existing *legal framework* for RFID. RFID is based on identification. Objects identified may be linked to persons. Applicability of the European privacy directives 95/46/EC and 2002/58/EC is discussed on three issues:

- should all RFID data be considered as personal data since all RFID data may be linked to an identifiable person at a specific point in the future?
- how to deal with informed consent when people are not aware of data collected on them?
- is 2002/58/EC applicable in situations where RFID data are collected as part of traffic data in a subscription situation in which a public infrastructure has been used (for Real Time Location Services for instance)?

These three issues are under debate. The result of negotiations on these issues is of high importance for the widespread diffusion of RFID. The stakes are pretty high. For instance should the conclusion drawn specify that IDs associated with objects are personal data (due to a possible linkage sometime in the future) this will raise serious problems to the widespread use of RFID in for instance item-level tagging. These issues also raise the more generic issue of the privacy approach in use today. On the other hand, one should avoid regulations which are technology specific - these regulations are of no use when new technologies emerge. On the other hand, due to the emergence of new information system architectures, indicated as ubiquitous or pervasive computing and ambient intelligence, the pressure on the privacy approach that is in use today will grow. Europe should face the need to rethink the basic assumptions of the existing privacy paradigm.[208]

[204] Bruno Crispo. RFID Validation workshop 3 October 2006; (Zaal, 2006).;.

[205] http://gtresearchnews.gatech.edu/newsrelease/eas-center.htm ('Improving Medical Devices: Georgia Tech Research Center Expands Testing Capabilities to Help Reduce Potential Interference"), posted 25 July 2006, accessed 29 November 2005.

[206] Gaynor Backhouse. RFID Validation workshop, 3 October 2006.

[207] Britta Oertel. RFID Validation workshop, 3 October 2006.

[208] Bart Schermer, RFID Validation workshop, 3 October 2006.

Next to these generic issues, within the respective application domains specific laws may enforce or prohibit the use of RFID. An example of *law enforcement* is provided by the European law on using RFID in animal tracking, the use of RFID in medicine and the use of RFID in European identity cards. With respect to the European approach in using law enforcement to stimulate the use of RFID, a recent analysis shows Europe to be much more reserved in enforcing the use of RFID for opposing drug counterfeiting than the USA (IDTechEx, 2006b). Europe still considers 2D-barcode to offer a sufficient and cheap protection against counterfeiting, notwithstanding the possible longer term benefits of adopting RFID.

15.3.2. Application domain

The *dynamics* of RFID in the various application domains differ considerably; they are dependent on specific requirements for RFID, expected benefits, expected Return on Investments, etc. In the cases we have studied, the overall drive towards the coupling of the physical world with the virtual world is strong and offers novel economic incentives. On the other hand, experiences are still scarce, in the sense that RFID implementation is still in its early phases, awareness is low and barriers with respect to the application domain are still prominent. Given the overview (Annex 8) on RFID-cases throughout Europe, one is tempted to say that except for a few early adopting countries (UK, France, Germany, The Netherlands, Italy) most countries have only limited experience with the implementation of RFID.

To improve this situation, there is a need to *gather experiences* with the implementation of RFID. One not only needs a technical evaluation of the implementation but an in-depth overall evaluation, taking into account the totality of technical, organisational, societal and legal issues which apply. Next to examples of successful introductions one needs examples in which the implementation has not been (entirely) successful, in order to understand better the pitfalls and barriers.

Europe could gather and disseminate information about best practices and lessons learned.

Pilots and trials are needed before one can decide about full roll-out of RFID. The yet asymmetric distribution of pilots and trials over Europe indicates that there may be a need for additional funds to stimulate RFID uses in countries and regions (and application domains) that are lagging.

Training and education is an aspect of RFID introduction that is often overlooked. In the cases we have studied, training and education is not at the forefront of activities undertaken to realise a beneficial introduction of RFID. We found a few cases in which training was considered to be essential for a proper introduction of RFID (within animal tagging for instance). But overall, awareness for training and education is low. Barriers and pitfalls will differ between the cases, and probably not all situations require in-depth training and education facilities. The more complex and isolated uses of RFID no doubt will require sufficiently skilled personnel to operate the equipment and to deal with unforeseen events.

We did not find many companies in Europe that are *active in the field of training and education*. Exemplary may be the fact that on a recent well-known RFID congress in the UK a US-based company has been invited to present its views on training and offer training courses on the spot. Though we did not research this issue in-depth, the evidence found point in the direction that Europe faces a backlog in providing sufficient and qualified RFID training and education courses.

While training and education courses will be directed at the end-users, concerns are raised on the size of *the RFID-skilled labour force*. These concerns have increased over the past few years. The shortage is both quantitative (too few skilled people) and qualitative (sufficiently skilled people but with the wrong competencies). There is a need for technicians with radio technology skills and software/business process/data architecture skills. Within Europe this shortage requires specific attention, given the rather low outflow of technical experts in ICT.

Table 15-2 presents an overview of actors and related policy issues.

Table 15-2: Overview of actor-related policy issues

Main actors	Policy approach	Activities
People	Creating beneficial conditions	- Ensuring appropriate legal framework (privacy, health, work, ...) - Stimulating Privacy by design - Stimulating/enforcing 'Watchdog' readers - Stimulating/enforcing 'RFID Guards' - Solving health issues (workers) - Stimulating creation and rising awareness on benefits to society
	Stimulating research	Social science research on RFID acceptance, trust
	Raising awareness	Communication campaign on RFID uses
	Innovation policy instruments	Supporting Pilots and trials
Firms	Creating beneficial conditions	Creation of limited liability pilots
	Stimulating research	- Research in economic feasibility of small scale RFID applications
	Raising awareness	- Communication campaign on RFID
	Innovation policy instruments	- Targeted innovation instruments: - Competition and Innovation Programme; promoting SME involvement
Governments	Launching customer	Introducing RFID in public domains

15.3.3. People

Part of what has been stated above concerns individuals as well (training and education, skills shortage). The lack of attention over RFID is reflected in the surveys that have monitored *awareness of people*. Public awareness is known to be low; yet, those who are aware usually consider RFID to be more beneficial than those who are unaware. People are very much aware of the privacy threats that are related to RFID. The European Consultation process on RFID (having over 2200 responses) showed privacy to be the top level concern. People consider RFID to be more threatening to the privacy of people than previous ICT innovations which intruded the personal sphere (such as mobile phones, and surveillance cameras). Awareness over RFID developments can be raised by means of targeted communication campaigns in which a balanced view on RFID is presented.

Trust and user acceptance are important yardsticks for the social implementation of RFID. Trust is formed by factors such as the basic attitude towards trust (the ability to trust), previous experiences, expectations regarding the performance of the innovation, the information provided, the values shared, the quality of the communication about the innovation (both effective and sufficient), and the design of the interface. Trust may be increased by offering people more control over their own position within the RFID system and the collected and disseminated data that are related to them. Trust may be enhanced by offering specific tools, such as the RFID-Guardian and the Watchdog reader.[209] Trust may also be enhanced by a quality mark that indicates RFID equipment to be designed according to specific privacy requirements. Logo's identifying RFID readers and overt statements on the kind of data collected (and uses made of the data) will be appreciated by users and will contribute to enhancing trust.

In addition, the way users *perceive the risks* associated with the RFID innovation is also critical. As has been demonstrated with nuclear energy and biotechnology, risk perception is a strong determinant for the attitude of people vis-à-vis novel products. Risk perception depends on factors such as the basic risk perception attitude (which may be of various kinds, such as fatalistic, hierarchical, individualistic or system-oriented), the level of uncertainty, the provision of personal details (the more personal details to be provided the higher the risk percep-

[209] Both tools provide people with technical means to identify the presence of tags and readers and to exert influence on the exchange of data.

tion), the availability of alternatives, lock-in and dependability, and autonomy. Reduction of risk thus is not a straight forward exercise, but an interplay between people, technologies and institutions.

Health is an issue of specific concern for people who will have to work with RFID readers on a permanent basis (logistics, retail). Up till now evidence points to no explicit concerns, but research programmes to study the consequences of long term exposure to specific forms of electromagnetic radiation are being implemented. Specific groups, such as people carrying a cardiac pacemaker, deserve special attention. The consequences of being exposed to mixes of frequencies require further research.

15.3.4. Companies

SMEs may find the *business case* of RFID hardly convincing to start using RFID. More research is needed to come to an understanding of business cases that are profitable to firms. The knowledge, gathered in pilots and trials by the early adopters, should be gathered and translated into clear business cases that show the costs and benefits of RFID introduction in specific situations.

European *innovation policy instruments*, such as the Competitiveness and Innovation Programme, can be used to organise pilots and trials in regions and countries where awareness on RFID in the business community is relatively low.

New Member states and other European states fulfilling specific conditions regarding implementation of RFID could be supported by additional funds in cases where public interest is shown to be high (for instance in the health sector).

15.3.5. Governments

National states and public organisations can act as *launching customers* in order to promote the use of RFID. Whether this is a desirable role is very much dependent on – again – the business case that can be presented in the respective domains. The cases we have studied identify in all situations a number of benefits from having objects, animals and persons tagged. Usually there is a price to pay in terms of privacy and security concerns, control over data flows, and reorganisation of information processes within organisations. Commercial parties are interested in the added value (information economy) that can be realised by using the aggregated data as a result of the additional services. Starting from the benefits, public agencies are in a favourable position to research the precise conditions of introducing RFID when trials and pilots run under their supervision (public transport, hospitals, identity cards).

Governments have a more extensive role as presented in *Table 15-2*. Perhaps, the role of public authorities is essential for the beneficial uptake of RFID. However, one could argue that market forces will have to be leading in realising the potential of RFID. This is a sound premise, which indicates that government initiatives should be reserved in promoting RFID as such, stimulating the use of RFID in domains which are still under their control (such as e-health) and when cost-benefit analysis shows the balance to be positive. In addition, their participation is justified because the parties involved in deployment of RFID systems will not be expected to bear the negative externalities of RFID (such as probable loss of jobs, privacy and security concerns, and health issues). Governments will be expected to take care of such issues. Finally, the broader issue of awareness raising is partly government's responsibility as well; market parties surely will invest in raising awareness as to the beneficial aspects of RFID implementation but the public interest is best served with a balanced view guided by public authorities. Again, the European consultation process shows citizens to be interested in receiving information on emerging RFID applications. On the other hand, one needs to be cautious since the message of the European Commission or any of its member states could easily be misinterpreted.[210]

15.4. Policy options to further research needs

In the preceding paragraphs, in addition to the proposed policy initiatives, a number of research needs have also been identified. *Table 15-3* presents the needs related to the various components and actors of the RFID system.

[210] As formulated by Gaynor Backhouse during the RFID Validation workshop: "Show, not tell".

Table 15-3: Overview of research issues

RFID-system	Research issues	Research orientation
reader-tag	privacy by design; security aspects; health issues; new and advanced RFID technologies	Technology; health research
application domain	'best practices'; interoperability and standards	Technology; social science
people	trust and acceptance; raising awareness; health issues	Social science; health research
firms	business cases	Organisational science; economy

Such research issues cover a broad scope: from technology to management and social science. Research opportunities within Europe are provided on a European scale and within national research programmes. The most obvious implementation of RFID research on a European scale will be the IST-programme and the CIP-programme. A prime example of such a research effort is the recently launched BRIDGE-project, a €7.5 Million, three year project in the Sixth Framework programme for Research and Technological Development.[211] BRIDGE ('Building RFID solutions for the Global Environment') combines research institutes, a number of GS1 offices (five from Europe and one from China), twelve solution providers and seven business end users. The focus of BRIDGE is on providing solutions for the supply chain in a number of application areas (anti-counterfeiting, healthcare, retail, textile, …). It will study business based research, provision of information services and hardware (sensor, tags) and software development.

A recent overview of *RFID research in Europe* shows a total of 40 collaborative research projects being supported over a 5 year period by European industry and research organisations. The European Commission contributed €150 million to a total investment of €306 million. The 40 projects cover a broad array of issues. 41% of the project funding is related to interoperability and standards-setting, 16% to research of the radio spectrum, 20% to governance aspects and 23% to protection of personal data and privacy. We have not made an in-depth analysis of these projects (what consortia, what prime focus?) so it is difficult to judge whether this portfolio of research covers the research needs in Europe.

We looked in more detail to the coverage of RFID security aspects in the 40 selected projects. The result is that security was not a prime area of interest. Except for two projects – OPTAG and SWAMI – security was not mentioned as an issue to be studied in depth. In the academic world security of RFID is a widely studied topic. The combination of *privacy and security* is an issue that is seriously taken on board.[212] We did not find examples of IST-funded research projects in which the idea of privacy by design was adopted as a starting point. Europe could take a vantage point by embedding this notion in the future FP7 programme and develop a research program around this notion. This might lead to a bridging of the academic interests in the issue of RFID security and the use of this knowledge in application oriented research projects. Solving the issue of security is of crucial importance for the widespread adoption of RFID-based applications and for preventing the occurrence of negative societal experiences.

Another research issue that is underexposed in present day research efforts is the notion of *trust and user acceptance*. Again, academic interest in this issue is clearly visible. A number of European research institutes have adopted RFID as a topic to be studied from a social science perspective. But since the success of RFID applications is critically dependent on the willingness of end-users (either firms or individuals) to use the technology offered, we would argue for embedding social science research on RFID in the European research agenda. The field of social science research issues of importance for RFID is much broader than privacy and data protection. It deals with issues such as the diffusion of innovations, the characteristics of user constituencies, drivers and barriers for adoption of RFID-based applications and the like.

[211] See http://www.bridge-project.eu

[212] See for instance the webpage http://lasecwww.epfl.ch/~gavoine/rfid/ which presents an up to date overview of recent academic papers on privacy and security.

The *health* consequences of long term endurance to relatively high powered UHF radiation (such as in case of people working in RFID based warehouses) are not well understood. A number of issues are still open (interference of cardiac pacemakers with RFID equipment, the consequences of long-term exposure to low radiation doses and to a 'cocktail' of frequencies).

Research interest in *future oriented RFID technologies* seems to be well covered by the present generation of RFID projects. Industrial parties and academic institutes co-operate in these projects and know how to join forces.

Regarding the *policy tools* to be used, apart from the European Framework programme (especially the Information Society Technologies part of the Seventh Framework Programme), the recently launched Competitiveness and Innovation Programme is a candidate for RFID-based activities. One of the pillars of the CIP is the ICT-policy support programme with a budget of €728 Million for the duration of the programme (2007-2013) and as one of its policy goals the following is mentioned: "provide a bridge between research investment and wide adoption, by providing a testing ground for pan-European electronic services in both the public and private sectors".[213]

Since many of the RFID implementation projects are Member State based, it seems appropriate to *stimulate nation-based research activities*. These activities can be dedicated to researching specific business cases, such as the use of RFID in health, animal tagging and libraries, and the role of SMEs in the RFID value chain. Having such a nation-based research programme in various countries creates an incentive for a comparative analysis in which country specific factors are analysed in relation to successful and failed RFID implementation trajectories.

15.5. Policy recommendations

RFID technologies are emerging in a variety of application domains. Notwithstanding the contribution RFID might offer to these application domains, RFID is still far away from widespread diffusion. Many RFID implementations concern pilots and trials meant to improve understanding of what can be done with RFID, what pitfalls to avoid and what gains to realise. The potential of RFID is enormous, and is expected to materialise within the next ten to fifteen years. This makes RFID an interesting and challenging policy domain. Though the baseline scenario should be that the market will shape the future of RFID technologies, and governments thus may take a backward position, a deeper investigation of issues that are at stake shows many issues to have policy relevancy. In the preceding paragraphs we have indicated – along the lines of the RFID-system (reader-tag and backend systems), its application domains and the most important actors – the kind of policy challenges that are at stake. This turns out to be a rather lengthy list of activities, which we have grouped into five main domains:

- stimulating research,
- creating beneficial conditions,
- raising awareness,
- developing innovation policy instruments,
- a role as launching customer (for governments only).

The range of policy actions shows to be very broad and entails issues such as frequency policy, communication campaigns, supporting privacy by design approaches, ensuring security of RFID systems, stimulating training and education programmes, etc. They all contribute to countering the famous 'Collingride dilemma': When a technology is still in its infancy, it is very difficult to shape the technology and to tune it to potential social and economic problems that may arise when the technology is full-fledged introduced. On the other hand, when a technology is widely disseminated, it becomes highly problematic to alter the course of events and to re-shape the specific technology. RFID is a technology in its early stages, and the technology and innovation assessment we have made show a distinct number of pitfalls that should be avoided to reap the full benefits of RFID. The policy challenge is to create a policy framework that will stimulate beneficial uses of RFID, that will regulate a level playing field for RFID, that will coordinate the learning experience offered by

[213] See http://ec.europa.eu/enterprise/enterprise_policy/cip/index_en.htm

RFID and that will prevent the detrimental consequences of unreflective introduction of RFID to become a reality.

In this final paragraph we will try to refocus these policy issues on a slightly more abstract level. Together these span up the proposed policy arena and the innovation system for RFID.

15.5.1. Technology and research policy

The main instrument for stimulating research and technology developments in the area of RFID for the European Commission is its *Framework Programme* (7th FP from 2007 till 2013). Within the 7FP, a total of 13 Billion Euro has been reserved for the IST-programme. This programme – the biggest of the nine thematic programmes, in the coordination part of the framework – has formulated a working programme that centres around seven challenges and two cross-cutting issues. The seven challenges mention RFID in a number of situations (healthcare delivery, intelligent vehicle and mobility systems, micro and nano systems, organics displays and future networks). What is lacking is attention for privacy by design and security issues. These could get more specific attention in one of the foreseen calls, related to the IST-programme.

Considering the focus of FP7 on the European Technology Platforms, RFID could become a core in a European Technology Platform on sensor networks, ambient intelligence and/or personalized context aware services, in case these networks should be created. Within the ETP eMobility RFID is one of the technologies that is mentioned in the context of a number of research challenges (healthcare, robotics, deployment issues). Though not central stage, these hooks may offer interesting (additional) opportunities to have technical research on RFID issues and prospects, and are in line with the general approach that RFID research should be application oriented.

15.5.2. Innovation policy

The *Competitiveness and Innovation framework Programme* has a total budget of 4 Billion Euro of which some 700 Million Euro is reserved for the ICT Policy support programme, which is one of the three pillars of this programme. The rationale behind CIP stresses that several indicators show the EU is lagging in terms of entrepreneurship, sustainable innovation, use of ICT and (sustainable) energy innovation. Several EU-programmes have been established to solve this problem. Within the context of ICT the Commission refers to the e-Ten, the MODINIS and the eContent programme. These programmes fail however to address the innovation problem in a synergetic and holistic manner. CIP will complement major initiatives such as the cohesion activities, the framework programme for research and the EU programme for lifelong learning. As of today, it is hard to see in what manner RFID issues will be taken on board. According to the CIP website, no specific action programme is in place today. Given the focus of the ICT policy support programme, it is clearly possible to have RFID-related activities financed within this programme, the focus of the CIP being to:

- "underpin regulatory and research actions of the Commission to stimulate emerging digital economy based on the convergence between network services, media content and new electronic devices
- provide a bridge between research investment and wide adoption, by providing a testing ground for pan-European electronic services in both the public and private sectors
- reinforce European cultural and linguistic identities by support for the production and distribution of European digital content
- assist the development of an open and inclusive European Information Society through stimulating innovative approaches to inclusion, quality of life and public services." [214]

Actions within the CIP could focus on the role of SMEs, the contribution of countries that are lagging in the adoption and diffusion of RFID, the establishment of a database with best (or: good) practices in the introduction of RFID, and the establishment of 'communities of interests' or 'com-

[214] http://ec.europa.eu/enterprise/enterprise_policy/cip/index_en.htm

munities of practitioners' over various member states and over different RFID application domains.

15.5.3. Regulatory activities

The reflections on the state of affairs regarding the regulatory issues concerning RFID focus on generic issues such as privacy and security on the one hand and more specific issues such as law enforcement in special domains (such as animal tracking) on the other hand. The *privacy and security issues* are the most outspoken instances of regulatory activities that need to be undertaken. Various European legislative bodies and organizations have focused on these issues. The most important European directives (the so-called privacy directive 95/46/EC and the e-Privacy directive 2002/58/EC) do not settle the dispute on personal data to be collected with RFID. A number of issues are under discussion yet. Starting point for the Article 29 Working Party is that *all* RFID-data can become personal data in due time. Another issue to be solved is the issue of informed consent, which is problematic given the automatic collection of personal data by RFID-systems. A third issue is whether 2002/58/EC applies for instance in using NFC, given the interpretation of NFC data as traffic data relating to subscribers of telecommunication services. These issues require more attention, especially since the European consultation has shown that European citizens place a lot of emphasis on the privacy consequences of RFID.

Law enforcement as a means to enforce specific behaviour should be applied with utmost care. In case of animal tracking, law enforcement is beneficial both from the point of view of animal welfare (no need to destruct large quantities of animals in case of an infectious disease outbreak) and people's health. In this situation it seems appropriate to use the instrument of law enforcement. One can imagine that in the case of drugs anti-counterfeiting specific laws may be created that support the anti-counterfeiting strategy in order to increase the well-being of (European) citizens. On the other hand, the continent of Africa is much more prone to drugs counterfeiting than Europe, and law enforcement would probably not change that situation. US analysts point at the backward position of Europe in this respect (IDTechex, 2006b). This might be an issue to take more care of.

Another example of law enforcement is the use of RFID based biometrics in European identity cards. Though the political battle over which data to present to the USA in case of European citizens flying to the USA is not over yet, the implications for the required RFID readiness of electronic identity cards are rather clear.

Other regulatory aspects relating to RFID deal with *environmental degradation* (WEEE directive and RoHS directive), and with *health consequences*. Regarding WEEE (directive 2002/95/EC), in the USA concerns are raised against the use of printed electronics (silver ink antenna's for instance) which may cause extra environmental burdens. Regarding health issues, the baseline approach is that no detrimental consequences are known for exposure to RF radiation. This is studied for instance in the case of use of mobile phones (microwave radiation). Health issues which are yet not clearly known relate to two problem areas: long term exposure in high radiation environment (logistics for instance) and the consequences of being exposed to 'cocktails' of radiation (mixed frequencies).

15.5.4. Stimulating adoption and dissemination of RFID

This heading encapsulates a broad range of activities, from broadly disseminated communication campaigns to the public at large, more focused communication campaigns to specific audiences (such as SMEs), activities to enforce training and education programmes, activities to increase the number of skilled RFID professionals, targeted subsidies for pilots and trials, dissemination of learning experiences, and stimulation programmes for specific countries and regions.

Communication campaigns can contribute to raising awareness by the public at large for the 'silent revolution' that takes place today. The outcome of the European consultation process clearly points in the direction of the need for more and better communication about the various aspects of RFID. Other studies have shown that people who are better informed are more inclined towards the beneficial uses of RFID than those who are not. There is thus a premium on a good communication strategy. The problem is that RFID is an *enabling* technology which can be used in a variety of settings, but the consequences of using RFID will always be situation specific. It is no use to inform the public on the mere presence of RFID as a novel and enabling technology. What is required is an approach in which the application areas of RFID are leading in illustrating the chances to which RFID may give rise. These chances may be for better and for worse; both sides have to be communicated.

Next to these broad campaigns there is a need for more focused *communication campaigns. These might be specifically directed at SMEs*; overall, SMEs face the problem that they are too small to bear the initial costs of deploying RFID technologies, while they may be confronted with requirements of vendors to re-organise their logistics in such a manner that RFID can be used (as is for instance the case in the Wal*Mart situation). SMEs may be interested in supporting RFID technologies when the advantages for them are sufficiently clear. Business cases that demonstrate the viability of RFID (in specific situations) and that show RoI-times to be beneficial might be one way to go forward. This requires a dedicated effort of technology transfer centres within the European countries. Budgets to establish such dedicated awareness campaigns must be made available.

New Member States are another point in respect. The overview shows these European Member States to be lagging in the overall dissemination of RFID. For one, the EU might want to create a knowledge base which shows the presence of RFID cases in all Member States, in order to keep track of the dissemination of RFID over the 25 European Member States. Given the empirical data used in this study, the backward position is surely not only related to the Member States. A focused financial effort might help in getting sufficient RFID-pilots and trials running in these backward countries, in order to prevent them from facing an ever increasing backlog. Successful practices in other Member States may be used as starting point to research the potentiality of starting similar practices in other Member States. Lessons learned can be disseminated in order to create a level playing field.

An issue that is largely ignored in RFID trials and pilots is the required *training and education of (end-) users*. In those situations where it is taken on board (animal tracking, for instance) it shows to be a highly determining factor for successful or failed introduction of RFID practices. Awareness on the need for training and education and the establishment of a European basis for a training and education programme including promoting common terms of reference and development of baseline skills, could be an issue to support at European level.

Awareness with respect to the employment consequences of RFID is another issue which deserves more attention. Overall, information about the employment consequences of RFID is scarce. The main suppliers of RFID technologies do not have an interest in putting this issue high on the agenda. This issue could be addressed preferably at European level by starting a research activity that is dedicated to getting a better view on the employment consequences of wide spread dissemination of RFID, based on realistic prognoses regarding the diffusion of RFID in distinct application domains. The results of such a study may be compared with scenario-studies directed at a broader array of societal trends such as ageing, migration, up-skilling, etc, in order to help develop a set of policy recommendations concerning the employment consequences of RFID.

The other side of the emergence of RFID is the noted *shortage of RFID-skilled professionals*. A study as to whether the stated imbalance (raised within the USA) is valid for the European situation as well could be also undertaken. This is part of the broader societal discourse on foreseeable shortages of the technically skilled workforce in Europe and should thus be treated as part of this discourse.

15.5.5. Acting as launching customer

Finally, governments could adopt a role as *launching customer*. Though much attention goes to the prospects of item level tagging and the business cases associated with the full roll-out of RFID on the supply chain, we have demonstrated in this study that a number of highly challenging application areas are related to public domain applications, such as public transport, animal tracking, identity cards and healthcare. A number of the cases we have studied are clearly in the realm of public-private partnerships (such as public transport) or regulated private spaces (such as in case of animal tracking). Regulatory issues are within the jurisdiction of (European, national or regional) authorities.

Governmental judgement to support the introduction of RFID in specific public domains will be based on the profits that can be made with introducing RFID. These profits need not only be economic profits (efficiency gains for instance) but may also be encapsulated in enhanced public value (better healthcare, improved public transport, a more secure society, etc.). Since governments operate in a political arena (in which business incentives may be very important but need not be dominant) the political assessment of the feasibility of specific RFID applications will be based on a variety of incentives. The case studies indicate that economic parameters (efficiency gains) are important but are positioned in the perspective of improved service delivery and added value services. Given the potential of RFID to improve public services, the role of governments as launching customer should get more attention.

Annex 1: References

AIM Global. 2006. *Why RFID chips can't infect cats - or computers*. March 20. 2006. *http://www.usingrfid.com/news/read.asp?lc=c62028cx673zn&version=printable*

Allbrecht, K. 2005. *RFID: The Doomsday Scenario.* In: Garfinkel, S. & Rosenberg, S. 2005. *RFID, Applications, Security and Privacy*. Addison Wesley.

American Civil Liberties Union (ACLU). 2004. *Naked data: how the U.S. ignored international concerns and pushed for radio chips in passports without security*. An ACLU White paper. November 24 2004.

Article 29 Working Party on Data Protection. 2005a. *'Working document on data protection issues related to RFID technology'*. 10107/05/EN. 19 January 2005.

Article 29 Working Party on Data Protection. 2005b. '*Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology'*. 1670/05/EN. 28 September 2005.

Ashbourn, J. 2006. *The societal implications of the wide scale introduction of biometrics and identity management.* Background paper for the Euroscience Open forum ESOF 2006 in Munich. July 2006.

Auto-ID center. technical report. *860MHz–930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification*. Candidate Recommendation. Version 1.0.1. *http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf*

Bagué, S. 2005. *Overviews Current Biometric Implementations in European Union Member States.* For: The European Biometrics Portal. September 29, 2005.

Becker. G. 2006. *Animal identification and meat traceability*. CRS Report for Congress.

Bickmore, T., & Cassell, J. 2001. *Relational agents: a model and implementation of building user trust.* Proceedings of SIGCHI '01. March 31 – April 4. Seattle, WA. USA. 396-403.

BIGresearch & Artafact LLC. 2004. *RFID Consumer Buzz*. October 2004. www. bigresearch.com

The Boston Consulting Group. 2003. *Customer Acceptance of FSI Applications* Metro AG press Release. October 2003.

CAP (Consulting Technology Outsourcing) & National Retail Federation. 2004. *RFID and Consumers: Understanding their mindset.* http://www.nrf.com/download/NewRFID_NRF.pdf

Capgemini. 2005. *RFID and Consumers – What European consumers think about radio frequency identifications and the implications for businesses.*

Carr, N.G. 2003. *IT doesn't matter*. The Harvard Business Review. May 2003.

EPCglobal. 2004. The EPCglobal Network. September 24, 2004. http://www.epcglobalinc.org/news/EPCglobal_Network_Overview_10072004.pdf

Cassell, J. & Bickmore, T. 2000. *External Manifestations of Trustworthiness in the Interface*. Communications of the ACM. 43(12). 50-56.

Centre for Democracy and Technology. 2006. *Privacy Best Practices for Deployment of RFID Technology – Interim draft.* May 2006.

Chappell, G., Durdan D., Gilbert G., Ginsberg L., Smith J. & Tobolski, J. 2003. *Auto-ID in the Box: the Value of Auto-ID technology in retail stores.* Accenture and Auto-ID Centre MIT. February 1, 2003

Cheskin Consulting and Strategic Market Research & Studio Archetype/Sapient. 1999. *eCommerce Trust Study*. January 1999.

Clap, S. 2006. *House votes to freeze FY2007 spending for animal ID*. Food Traceability Report. June 2006. 6 (6).

CompTIA. 2006. *CompTIA adds Depth to shallow pool of RFID talent.*

Convert, James. 2004. *Business Solutions: Down, but far from out: RFID technology is off to a disappointing start; but retailers are convinced its future is as bright as ever*. Wall Street Journal. January 12. 2004. p. R5.

Corsten, D. & Gruen, T.. 2004. *Stock-Outs mean Walkouts.* Harvard Business Review. May 2004. 82 (5)

Davis, F. D. 1989. *Perceived usefulness, perceived ease of use, and user acceptance*. MIS Quarterly. 13 (3). 319-340.

DEFRA/ADAS. 2005. English Pilot Trial of EID/EDT in sheep. DEFRA. 31 October 2005.

DHS Emerging Applications and Technology Subcommittee. 2006. *The use of RFID in human identification.* Draft report to the Full Data Privacy and Integrity Advisory Committee. version 1.0. 2006.

Dillon, A., & Morris, M. G. 1996. *User acceptance of information technology: Theories and models*. Annual Review of Information Science and Technology. 31. 3-32.

ECP 2005. *Privacyrechtelijke aspecten van RFID ('Juridical aspects on RFID and privacy')*. Den Haag: ECP.nl.

EPC global. 2005. *Guidelines on EPC for Consumer Products*. Revised September 2005.

E-skills forum. 2004. *E-skills for Europe: Towards 2010 and beyond. Synthesis ReportThe European Consumer's Organisation.* Consumer concerns on potential applications around RFID. Issue: *http://www.rfidconsultation.eu/docs/ficheiros/ISSUE_PAPER_RFID_Workshop__BEUC.pdf*

European Biometrics Portal. *Biometrics in Europe*. Trend report Unisys. Brussels. June 2006.

European Commission. 2006a. *Radio-Frequency Identification tags (RFID) Portfolio of European research (Factsheet).*

European Commission. 2006b. *Appendix III: EU-funded Research and developments projects*. February 2006.

European Commission .2006c. *The RFID Revolution: Your voice on the Challenges, Opportunities and Threats. Online Public Consultation*. 16 October 2006.

European Commission 2006d. *Next steps in the EU RFID policy initiative*. Directorate General Information Society and Media Belgium. Final Conference on RFID. 16 October 2006.

European Commission. 2004. *Smart Wireless Tags research needs: consultation report: Part of the wide consultation for the definition of the content of the work programme 2005-2006.* Information Society Technologies Programme, Directorate D: Communication Networks, Security and Software-applications. Unit D5: ICT for business.

Eurosmart. 2004. *Recommendations for European Electronic visa and passport* Recommendations to European Union. October 2004.

Finkenzeller, K. 2003. *RFID handbook, fundamentals and applications in contactless smart card and identification.* Willey. 2nd Edition.

Floerkemeier, C., Schneider, R.& Langheinrich, M. 2005. *‚Scanning with a purpose – Supporting the Fair Information Principles in RFID Protocols.*

FOIS. 2004. *Security Aspects and Prospective Applications of RFID Systems*. BSI. October 2004. Federal Office for Information Security.

Forrester. 2005. *RFID: The Complete Guide*. Forrester Research.

Forrester. 2005. *The information workplace will redefine the world of work – at last!*

Friedewald, M., Lindner, R. & Wright, D. 2006. *Safeguards in a World of Ambient Intelligence (SWAMI); Threats, Vulnerabilities and Safeguards in Ambient Intelligence*. Deliverable D3.

Garfunkel, S.& Rosenberg, B. 2005. *RFID, applications, security, and privacy.* Edison-Wesley.

Garfunkel, S., Juels, A. & Pappu, R.. 2005. *'RFID Privacy: An Overview of Problems and Proposed Solutions'*. IEEE Security & Privacy. May/June 2005.

Gartner. 2005a. *Hype Cycle for Radio Frequency Identification.*

Gartner. 2005b. *Understanding Gartner's Hype Cycles*. 2005. ID Number G00128180.

Gartner. 2005c. *Market Share and Forecast: Radio Frequency Identification, Worldwide, 2004-2010 (Executive Summary).* November 2005.

Group Radish/CSCI E-170. 2005. National Identification Cards: Balancing Technology & Privacy www.simson.net/ref/2005/csci_e-170/p2/radish.pdf

The Guardian. 2004. *I've got you under my skin.*
URL: *http://technology.guardian.co.uk/online/story/0,3605,1234827,00.html*

Heydt-Benjamin, T. S., Bailey, D. V., Fu, K, Juels, A. & O'Hare, T. 2006. *Vulnerabilities in First-Generation RFID-enables credit cards*, In Press. see www.rfid-cusp.org

Hoepman, J-H., Hubbers, E., Jacobs, B., Oostdijk, M. & Wichers Schreur, R. *Crossing borders: Security and Privacy Issues of the European e- passport*. www.cs.ru.nl/~jhh/publications/passport.pdf

Holvast, J. 2001. *'Privacy en beveiliging in het perspectief van de Wet bescherming persoonsgegevens'*. Contribution to the Dutch Yearbook Security.

Home Office. 2003. *Identity Cards. the next steps.* Document Cm 6020. November 2003.

IBM. 2005. *RFID: A driving force for innovation.*

IDC. 2004. *Worldwide and U.S. RFID Services competitive Analysis and Leadership Study. 2004: Disruptive Technology in Waiting and why the Services Value Chain Matters.*

IDTechEx. 2005a. *RFID Forecasts, Players and Opportunities2006 to 2016.*

IDTechEx. 2005b. *Active RFID 2006 – 2016, fast growth and Zigbee, WiFI and Bluetooth leverage*.

IDTechEx. 2005c. *RFID in Healthcare 2006-2016.*

IDTechEx. 2006. *The RFID Knowledge Base – Sample Case Studies.*

IDTechEx. 2006a. *London – Transport for London TfL*. Oyster Card UK. 26 January 2006.

IDTechEx. 2006b. *Drug counterfeits in Europe – Another Wake-up Call*. Smart Labels Analyst Issue 67. August 2006. 22-23.

IEEE. 2006. *Security and Privacy in RFID and Applications in Telemedicine*. IEEE Comm.Mag. April 2006.

ISO/IEC standard 9798-2. 1999. *Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms.*

ITU. 2005. Internet of Things – ITU Internet report.

Juels, A. 2006. *RFID Security and Privacy: a Research Survey*. 28 September 2005. To appear in IEEE Journal on Selected Areas in Communication. 2006.

Juels, A., Rivest, R. & Szydlo, M. 2003. *The blocker tag: selective blocking of RFID tags for consumer privacy*. CCS'03. October 2003. Washington.

Kfir, Z. & Wool, A.. 2005. *Picking virtual pockets using relay attacks on contactless smartcard systems.* Cryptology ePrint Archive. Report 2005.

Kim, Y.K.. 2002. *Consumer Value: An Application to Mall and Internet Shopping.* International Journal of Retail and Distribution Management. 30 (12). 2002. 595-602.

Lee, J., Kim, J., & Moon, J.Y. 2000. *What makes Internet users visit cyber stores again? Key design factors for customer loyalty*. Proceedings of CHI '2000, The Hague, Amsterdam. 305-312.

Lewandowsky, S., Mundy, M. & Tan, G.P.A. 2000. *The dynamics of trust: comparing humans to automation*. Journal of Experimental Psychology: Applied. vol. 6. 104-123.

Liard, Michael. 2004, *White Paper: Radio Frequency Identification (RFID) Middelware Solutions: Global market Opportunity.* Venture Development Corporation.

Löer, Th., 2005. *Implementing the German ePassport.* Keesing Journal of Documents & Identity. issue 14. 2005

Loretto, Jonathan. 2005. *Understanding the impact of RFID technologies and enhancing business performance.* KAZ White Paper. KZA Group Ltd.

MIC (Ministry of Internal Affairs and Communications), METI (Ministry of Economy, Trade and Industry) Government of Japan. 2004. *Guidelines for Privacy Protection with regard to RFID tags.* July 8. 2004.

Molnar, D.A. 2005. *Security and Privacy in two RFID deployments, with new methods for private authentication and RFID pseudonyms.* M.Sc. thesis. University of California.

Moon, J., & Kim, Y. 2001. *Extending the TAM for a World-Wide-Web context.* Information & Management. 38 (4). 217-230.

MSNBC. 2006. *Identity tags implanted under workers skin.* February 13, 2006.

URL: *http://www.msnbc.msn.com/id/11331144/*

NVVIR. 2005. *Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen.*

OECD. 2004. *Information Technology Outlook. Chapter 6: ICT skills and employment.*

OECD. 2005. *New perspectives on ICT skills and employment.*

OECD. 2006. *RFID: Drivers, challenges and public policy considerations.*

OECD. 2006a. *Radio-frequency identification (RFID): Drivers, challenges and public policy considerations.* Report DSTI/ICCP(2005)19/FINAL, published on 27 February 2006.

OECD. 2006b. *Foresight Forum "Radio Frequency Identification (RFID) applications nd public policy considerations – Proceedings.* DSTI/CCP(2006)7

Pape, W. and Smith, G. 2006. *The NAIS database is on firm middleware ground.* Food Traceability Report. June 2006. Vol. 6, No. 6.

Patrick, A. 2002. *Privacy, trust, agents & users: a review of human-factors issues associated with building trustworthy software agents.* Human Factors of Trustworthy Agents. National Research Council. Canada. 1-12.

Ping Zhang, Na Li. 2005. *The importance of affective quality.* Communications of the ACM. 48 (9). 105-108.

Politecnico di Milano. 2005. *RFID tra presente e futuro.* Collana Quaderni AIP. April 2005.

Politecnico di Milano. 2006. *RFID alla prova dei fatti.* June 2006.

Privacy Rights Clearinghouse. 2003 *RFID Position Statement of Consumer privacy and Civil Liberties Organisations.* http://www.privacyrights.org/ar/RFIDposition.htm

RAND. 2005. *9 to 5: Do you know if your boss knows where you are? Case studies of RFID usage in the workplace.*

Rander, R., & Rothchild, M.1975.*On the allocation of effort.* Journal of Economic Theory. 10. 358-376.

Reed, J., Erickson, J., Ford, J., & Hall, N.P.. 1996. *The After Effects of a Residential Marketing Program: Implications for understanding market transformation.* In: Building Skills and Strategies for Individuals and Organizations: Proceedings from the 1996 AESP Annual Meeting. Boca Raton: Association of Energy Service Professionals. 250-259.

Reed, J. & Hall, N. 1998. *Market Transformation and the adoption and diffusion of innovations*. In: Reed, J., Hall, N. Energy Centre. Market Effects Study. TecMRKT Works. Arlington/Oregon. May 1998.

Redding, V. 2006. *The RFID Revolution: challenges and options for action.* Member of European Commission – Commissioner for Information Society and Media. International CeBIT Summit.

Registratiekamer, TNO. 1995. *Privacy enhancing technologies: the path to anonymity*. The Hague.

RFID Tribe 2006. *The RFID Workforce: The Fast and the Furious*. April 2006.

Rieback, M. 2006. *Tag-borne attacks against RFID middleware*. Presentation in SAFE-NL workshop. 8 June 2006. Delft. The Netherlands.

Rieback, M., Simpson, Crispo, B. & Tanenbaum, A. 2006. *RFID Viruses and Worms. http://www.rfidvirus.org/*. Department of Computer Science. Vrije Universiteit Amsterdam.

Riegelsberger, R. & Sasse, M.A. 2001. *Trustbuilders and trustbusters: the roll of trust cues in interfaces to e-commerce applications* 1st IFIP Conference on e-commerce, e-business, e-government (i3e). October 3-5 2001. Zurich. Switzerland. 17-30.

RIVM. 2004. *Gezondheidseffecten van blootstelling aan radiofrequente electromagnetische velden.* ('Health consequences of exposure to radiofrequency electromagnetic fields'). RIVM-rapport 861020007/2004.

Roache, A., McCullagh, D., 2006. *New RFID travel cards could pose privacy threat,* CNET News.com, 19/4/2006

http://www.zdnetasia.com/news/software/0,39044164,39352807,00.htm

Rogers, E.M. 1962. *Diffusion of Innovations*. New York: The Free Press of Glencoe.

Rogers, E. 1995. *Diffusion of Innovations.* 4th ed. New York: The Free Press of Glencoe.

Rotter, J.B. 1980. *Interpersonal trust, trustworthiness, and gullibility*. American Psychologist. 35 (1). 1-7.

Roussos, Georges. 2004. *Building Consumer Trust in Pervasive Retail.* International workshop series: information sharing and privacy. Tokyo. Japan.

Schneier, B. 2005. *Fatal flaw weakens RFID passports*. Wired news. November 3, 2005.

Sharma, Aditya & Citurs, Alex. 2005. *Drivers and rationales in RFID adoption and post adoption integration: an integrative perspective on IOS adoption*. DIGIT 2005. 1-22.

Smith, T. 2005. *A Focus on Animal Electronic Identification.* http://fsrio.nal.usda.gov/document_fhseet.php?product_id=61 (visited 13 June 2006).

Sopensky, E. 2005. *The technology behind e-passports promises to dramatically streamline the global movement of goods and people*. Foreign Service Journal. December 2005. 29-35.

Spiekermann, S. & Ziekow. H. 2006. *'A systematic analysis of privacy threats and a 7-point plan to address them'.* Journal of Information System Security. 1 (3).

Steven, Toby, Enterprise Privacy Group. 2005 *Privacy Code of Conduct for RFID Technologies.* Enterprise Privacy Group. Hants.

Squires, P. & Neary, D.P. 2006. *Optimizing RFID readiness: When business as usual intersects with disruptive technology.*

Technische Universität Darmstadt. 2005. Department of Computer Science. RFID Seminar. Winter Term 2005/2006.

Telematica Instituut. 2006. *RFID: Kans of bedreiging? Een blik op RFID toepassingen en verkenning van de beleidsimplicaties.* Enschede.

UK RFID Council. 2006. *A UK code of practice for the use of radio frequency identification (RFID) in retail outlets.* Release 1.0, 12 April 2006.

University of Florida. 2000 *2000 Retail Survey Report.*

USA Strategies Inc.. 2005. *RFID Adoption in the retail industry.* Willowbrook. Illinois.

Venkatesh, V., Morris, M. G., Davis, G.B., & Davis, F. D. 2003. *User acceptance of information technology: Toward a unified view*. MIS Quarterly. 27 (3). 425-478.

Volmer, B. Chr. 2006. *Biometrics, RFID technology, and the ePassport: are Americans risking personal security in the face of terrorism?* M.A. thesis. Georgetown University. 2006.

Von Locquenghien, K. 2006. *On the potential social impact of RFID-Containing everyday objects*. Science, Technology & Innovation studies. vol. 2.

Westin, A. 1967. *Privacy and Freedom*. London: The Bodley Head.

Wireless Healthcare. 2004. *RFID as an eHealth Platform in eHealth-insider.* URL: *http://www.e-health-insider.com/news/item.cfm?ID=959*

Witteman, M. 2005. *Attacks on Digital Passports*. Riscure. July 28.

Yankee Group. 2004. *Users and Vendors are beginning to explore the Utility of RFID Technology in the Supply Chain.*

Zaal, R. 2006. *RFID-intimiteiten zijn binnenkort te pareren* ('RFID-intimacies can soon be warded off'). AutomatiseringsGids 28 July 2006.

Related URLs

http://www.rfidjournal.com

http://autoid.mit.edu//

http://www.epcglobalus.org

http://www.dutchrfid.nl

http://europa.eu/information_society

http://cordis.europa.eu/search/

http://ec.europa.eu/research/aeronautics/projects/article_3718_en.html

http://www.rfidconsultation.eu/

Annex 2: Acronyms

AIM	Automatic Identification and Mobility
ANSI	American National Standards Institute
CAPEX	Capital Expenditures
CRM	Customer Relationship Management
DRM	Digital Rights Management
EAN	European Article Numbering Association
EPC	Electronic Product Code
ERP	Effective Radiated Power; Enterprise Resource Planning
FCC	Federal Communications Commission
FDX	Full Duplex
GCI	Global Commerce Initiative
GDS	Global Data Synchronization
GPRS	General Packet Radio Service
HDX	Half Duplex
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technologies
ISO	International Standards Organization
IST	Information Society Technologies
IT	Information Technologies
LF	Low Frequency Band
HF	High Frequency Band
NFC	Near Field Communication
OPEX	Operational Expenditures
PIN	Personal Identification Number
RFID	Radio Frequency IDentification
SAW	Surface Acoustic Wave
UCC	Uniform Code Council
UHF	Ultra High Frequency Band
UMTS	Universal Mobile Telephone System
USDA	United States Department of Agriculture
UWB	Ultra Wide Band

Annex 3: Regulatory status RFID in the UHF spectrum[215]

The table attached provides an overview of the Ultra High Frequency (UHF) regulations worldwide. Each entry includes the following data:

- **Country name**. All GS1 member countries as well as major non-member countries are included, representing a total of 98,46% of the world Gross National Income (GNI) according to EPCglobal. (http://www.epcglobalinc.org).
- **Status**. The following convention indicates the status of UHF regulation in the country:

  OK Regulations are in place or will be in place shortly

  IP **I**n **P**rogress. Appropriate regulations expected first half of 2006

  NA Information **N**ot **A**vailable
- **Frequency**. Indicates the frequency band(s) authorized in the country for RFID applications. The objective is to get a band available in the 860 to 960 MHz spectrum.
- **Power**. Indicates the maximum power available to RFID applications. The power is expressed either as EIRP (Effective Isotropic Radiated Power) or ERP (Effective Radiated Power). Please note that 2 Watts ERP is equivalent to 3.2 Watts EIPR.
- **Technique**. Indicates the reader to tag communication technique. FHSS stands for Frequency Hopping Spread Spectrum and LBT stands for Listen Before Talk.
- **Comments**. Provides additional information on the regulatory status.

The following statistics can be derived from the data that are currently available:

- Regulations are in place or will be in place shortly in 29 countries representing 72% or the global GNI.
- Regulations should be settled by the first half of 2006 in 27 countries representing 12% of the global GNI.
- Issues need to be sorted out in 5 countries representing 11% of the global GNI.
- Information is not yet available for 55 countries representing 4% of the global GNI.

Country	Sta-tus	Frequency	Power	Technique	Comments
Algeria	NA				
Argentina	OK	902-928 MHz	4 W eirp	FHSS	
Armenia	IP	865.6-867.6 MHz			
Australia	OK	920-926 MHz	4 W eirp		4W eirp available through license managed by GS1 Australia. Situation likely to remain until 2007 at which time it is hoped that a permanent change to a limit of 4 W eirp will be made
Austria	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since 2 February 2006
Azerbaijan	NA				
Bahrain	NA				
Bangladesh	NA				
Belarus	NA				
Belgium	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Bolivia	NA				
Bosnia					

[215] Data up to date 6 June 2006; excerpt from: http://www.epcglobalinc.org/standards_technology/RFID%20at%20UHF%20Regulations%2020060606.pdf

Country	Sta-tus	Frequency	Power	Technique	Comments
Herzegovina	NA				
Botswana	NA				
Brazil	OK	902-907.5 MHz	4 W eirp	FHSS	
Brazil	OK	915-928 MHz	4 W eirp	FHSS	
Bulgaria	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Cambodia	NA				
Cameroon	NA				
Canada	OK	902-928 MHz	4 W eirp	FHSS	
Chile	OK	902-928 MHz	4 W eirp	FHSS	
China	IP	917-922 MHz	2 W erp		Provisional allocation. Temporary license required.
Colombia	IP				Dialogue with regulators initiated by GS1 Colombia
Congo, Dem. Rep.	NA				
Congo, Rep.	NA				
Costa Rica	OK	902-928 MHz	4 W eirp	FHSS	
Côte d'Ivoire	NA				
Croatia	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Cyprus	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Czech Republic	OK	865.6-867.6 MHz	2 W erp	LBT	
Denmark	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since January 2005
Dominican Republic	OK	902-928 MHz	4 W eirp	FHSS	
Ecuador	NA				
Egypt, Arab Rep.	IP				Work in progress
El Salvador	NA				
Estonia	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006. License possible.
Finland	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since 3 February 2005
France	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be implemented in July 2006
Georgia	NA				
Germany	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since 22 December 2004
Greece	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Guatemala	NA				
Honduras	NA				
Hong Kong, China	OK	865-868 MHz	2 W erp		
Hong Kong, China	OK	920-925 MHz	4 W eirp		
Hungary	IP	865.6-867.6 MHz	2 W erp	LBT	Implementation is in progress
Iceland	OK	865.6-867.6 MHz	2 W erp	LBT	
India	OK	865-867 MHz	4 W erp		Approved in May 2005
Indonesia	IP				Band 923 to 925 MHz being considered
Iran, Islamic Rep.	NA				
Ireland	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006

Country	Sta-tus	Frequency	Power	Technique	Comments
Israel	IP				Work in progress
Italy	IP	865.6-867.6 MHz	2 W erp	LBT	Conflict with band allocated to tactical relays military application. Temporary licenses available.
Jamaica	NA				
Japan	OK	952-954MHz	4 W eirp		License required for using 952-954 MHz at 4 W eirp
Japan	OK	952-955MHz	4 W eirp		952-955 MHz available for unlicensed use at 20m W eirp
Jordan	NA				
Kazakhstan	NA				
Kenya	NA				
Korea, Rep.	OK	908.5-910 MHz	4 W eirp	LBT	Approved July 2004
Korea, Rep.	OK	910-914 MHz	4 W eirp	FHSS	Approved July 2004
Kuwait	NA				
Kyrgyz Republic	NA				
Latvia	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Lebanon	NA				
Lithuania	IP	865.6-867.6 MHz	2 W erp	LBT	Individual license required. New regulations should be in place in 2006
Luxembourg	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
Macao, China	NA				
Macedonia, FYR	NA				
Malaysia	OK	866-869 MHz			Allocation under consideration. 868 MHz available at 50 mWatt power.
Malaysia	OK	919-923 MHz	2 W erp		Unlicensed use allowed up to 2 W erp. Use up to 4 W erp allowed under license
Malta	IP	865.6-867.6 MHz	2 W erp	LBT	Individual license required. New regulations should be in place in 2006
Mauritius	NA				
Mexico	OK	902-928 MHz	4 W eirp	FHSS	
Moldova	OK	865.6-867.6 MHz	2 W erp	LBT	
Mongolia	NA				
Morocco	NA				
Netherlands	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations will be in place since 27 February 2006
New Zealand	OK	864-868 MHz	4 W eirp		
Nicaragua	NA				
Nigeria	NA				
Norway	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations will be in place in 2006
Oman	NA				
Pakistan	NA				
Panama	NA				
Paraguay	NA				
Peru	NA				
Philippines	IP	918-920 MHz	0.5 W erp		In progress
Poland	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since October 24th 2005
Portugal	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006

Country	Sta-tus	Frequency	Power	Technique	Comments
Puerto Rico	OK	902-928 MHz	4 W erp	FHSS	
Romania	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place since April 7, 2006
Russian Federation	IP	865.6-867.6 MHz	2 W erp	LBT	Licensed use only. Will decide whether to adopt following completion of internal compatibility study due mid 2005
Saudi Arabia	NA				
Senegal	NA				
Serbia and Montenegro	NA				
Singapore	OK	866-869 MHz	0.5 W erp		
Singapore	OK	923-925 MHz	2 W erp		License required for power above 0.5 W erp
Slovak Republic	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place
Slovenia	IP	865.6-867.6 MHz	2 W erp	LBT	New regulations should be in place in 2006
South Africa	OK	865.6-867.6 MHz	2 W erp	LBT	Should be in place by March 2006
South Africa	OK	917-921 MHz	4 W eirp	FHSS	
Spain	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations will be in place by January 2007. Temporary licenses available.
Sri Lanka	NA				
Sudan	NA				
Sweden	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations approved 13 Dec 2005. In the law since 1 Jan 2006
Switzerland	OK	865.6-867.6 MHz	2 W erp	LBT	
Syrian Arab Rep.	NA				
Taiwan	OK	922-928 MHz	1 W erp	FHSS	Indoor
Taiwan	OK	922-928 MHz	0.5 W erp	FHSS	Outdoor
Tanzania	NA				
Thailand	OK	920-925 MHz	4 W eirp	FHSS	New regulations effective since 20 January 2006. License required for power above 0.5W.
Trinidad and Tobago	NA				
Tunisia	IP	865.6-867.6 MHz	2 W erp	LBT	Plans adopting European regulations
Turkey	IP	865.6-867.6 MHz	2 W erp	LBT	Conflict with band allocated to tactical relays military applications
Turkmenistan	NA				
Uganda	NA				
Ukraine	NA				
United Kingdom	OK	865.6-867.6 MHz	2 W erp	LBT	New regulations in place as of 31 January 2006
United States	OK	902-928 MHz	4 W eirp	FHSS	
Uruguay	OK	902-928 MHz	4 W eirp	FHSS	
Uzbekistan	NA				
Venezuela, RB	OK				Band 922-928 MHz will be allocated shortly
Vietnam	NA				
Yemen, Rep.	NA				
Zimbabwe	NA				

Annex 4: Self regulation: guidelines and code of practices

This annex contains a description of 4 different guidelines and code of practices regarding the implementation and use of RFID technologies.

a) Electronic Product Code™ (EPC) guidelines[216]

Electronic Product Code™ (EPC) is an emerging system that uses RFID for the automatic identification of consumer products. EPC has the potential to be used on many everyday consumer products as they move through the supply chain. To allow EPC to realize its potential for consumers, retailers and suppliers, it is important to address privacy concerns prompted by the current state of the technology, while establishing principles for dealing with its evolution and implementation. Accordingly the sponsors of EPC have adopted a number of guidelines for use by all companies engaged in the large-scale deployment of EPC. These guidelines are intended to complement compliance with the substantive and comprehensive body of national and international legislation and regulation that deals with consumer protection, consumer privacy and related issues

The guidelines have been followed since January 1, 2005. The EPCglobal Guidelines on EPC for Consumer Products are dealing with 4 main issues (revised version September 2005):

1. Consumer notice

Consumers will be given clear notice of the presence of EPC on products or their packaging and will be informed of the use of EPC technology. This notice will be given through the use of an EPC logo or identifier on the products or packaging.

2. Consumer choice

Consumers will be informed of the choices that are available to discard or remove or in the future disable EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable. EPCglobal, among other supporters of the technology, is committed to finding additional efficient, cost effective and reliable alternatives to further enable customer choice.

3. Consumer education

Consumers will have the opportunity easily to obtain accurate information about EPC and its applications, as well as information about advances in the technology. Companies using EPC tags at the consumer level will cooperate in appropriate ways to familiarize consumers with the EPC logo and to help consumers understand the technology and its benefits. EPCglobal would also act as a forum for both companies and consumers to learn of and address any uses of EPC technology in a manner inconsistent with these Guidelines.

4. Record use, retention and security

The Electronic Product Code does not contain, collect or store any personally identifiable information. As with conventional barcode technology, data which is associated with EPC will be collected, used, maintained, stored and protected by the EPCglobal member companies in compliance with applicable laws. Companies will publish, in compliance with all applicable laws, information on their policies regarding the retention, use and protection of any personally identifiable information associated with EPC use.

b) UK code of practice[217]

On 12 April 2006 the UK RFID Council published a proposal for a UK code of practice for the use of RFID in retail outlets. It is hoped by the UK RFID Council that this Code of Practice will be

[216] EPC global. 'Guidelines on EPC for Consumer Products', Revised September 2005

[217] UK RFID Council. /A UK code of practice for the use of radio frequency identification (RFID) in retail outlets', Release 1.0, 12 April 2006

adopted by a company under the statement: ‘XYZ Company endorses this code of practice and agrees to abide by its objectives’

The UK Code of Practice follows in general the Electronic Product Code™ (EPC) guidelines, in addition to the 4 items another one is added on:

5. Health and safety

Companies will take the greatest care of their suppliers, employees and customer to ensure that all applicable health and safety, and recycling and other regulations are met. RFID tags for use in retail outlets do not contain a batter, cannot emit any power and are harmless in all general applications. They are passive devices and only send information when questioned by a scanning device in the retail outlet, for example at check-out or during stock-taking, The tags are thus reliant upon the scanners for the small amount of power required for them to operate. The scanners must comply with regulatory constraints on the power, delivered and adhere to guidelines, standards and constraints on human exposure levels to the electromagnetic fields produced by scanning devices.

c) Government of Japan: Guidelines for Privacy Protection with Regard to RFID Tags[218]

The Ministry of Internal Affairs and Communication (MIC) and the Ministry of Economy, Trade and Industry (METI) of Japan jointly developed guidelines within the scope of consensus among stakeholders regarding privacy protection of consumers.

The guidelines were developed on the basis of the vision that to address the privacy problems caused by characteristics through the implementation of RFID tags, it is essential to promote their social acceptance through the implementation of appropriate measures from the viewpoint of protecting the privacy of consumers.

The Guidelines contain the following articles:

Article 1 (Purpose)

The purpose of these Guidelines shall be to clarify basic matters common to relevant industries on privacy protection for consumers pertaining to RFID tags, in order to utilize the advantages of RFID tags, ensure benefits to consumers and enable society to smoothly accept RFID tags.

Article 2 (Scope of these Guidelines)

These Guidelines shall, where RFID tags are embedded in products and stays there even after consumers have been handed said products, stipulate preferable rules that companies dealing with the said RFID tags and products tagged with said RFID tags should abide by.

Article 3 (Indication, etc. of the Fact that Products Are Tagged with RFID Tags)

Where RFID tags are embedded in products and stays there even after consumers have been handed said products, the companies concerned shall, prior to transactions, explain or post the fact that products are tagged with RFID tags, tagged positions of RFID tags, features thereof and information contained in RFID tags (hereinafter referred to “RFID tag information”), or attach indications to said products or packages thereof so as to enable consumers to recognize details of RFID tag information. The companies concerned shall be requested to make efforts at their stores to enable consumers to recognize the said fact through such explanations or indications.

Article 4.(Reservation of the Right of Final Choice of Consumers with Respect to Reading of RFID Tags)

Where RFID tags are embedded in products and stays there even after consumers have been handed said products, the companies concerned shall, when a consumer wants to deactivate said RFID tags while recognizing the features of said RFID tags, explain or post in advance the methods to deactivate said RFID tags, or attach indications to said products or packages thereof so to ensure that the consumer has a choice.

[Examples of methods to deactivate RFID tags]

1. Where it is possible to shield RFID tags by aluminium foils, communications between RFID readers and RFID tags can be blocked.

[218] MIC (Ministry of Internal Affairs and Communications), METI (MInistry of Economy, Trade and Industry) Government of Japan, ‘Guidelines for Privacy Protection with regard to RFID tags’, July 8, 2004

2. Electromagnetically erase all information including unique numbers in RFID tags or part information selected by consumers, or deactivate reading functions relating to said information.

3. Remove RFID tags.

Article 5 (Information Offerings Concerning Social Benefits of RFID Tags)

In cases where the reading functions of RFID tags are deactivated pursuant to Article 4, and where consumer benefits or the social interests is eroded, such as where environmental problems occur by losing information necessary for recycling products, or where driving safety is not ensured by losing information on auto-repair histories, the companies concerned shall make efforts to provide consumers with information to the effect that consumer benefits or the social interests would be eroded through methods including indications.

Article 6 (Handling of RFID Tags in Cases Where Information Is Used by Linking Personal Information Databases, Etc. Stored in Computers with RFID Tag Information)

Even in cases where a specific individual cannot be identified only by information recorded in RFID tags, when information can be easily processed by linking personal information databases, etc. stored in computers with RFID tag information, and when the specific individual can be identified, the information recorded in said RFID tags shall be deemed as personal information to be covered under the "Personal Information Protection Law."

Responsibilities under the "Personal Information Protection Law" pertaining to companies dealing with personal information (examples)

(1) In relation to purposes of the use of personal information

- To specify the purposes of the use of personal information to the greatest extent possible
- To obtain consent from the principal when using personal information for purposes other than the purposes of the use of personal information

(2) In relation to collection of personal information

- To prohibit unlawful collection of personal information
- When having collected personal information, to inform the person concerned of the purposes of the use of personal information without delay, or to announce to that effect

(3) In relation to management of personal data

- To make efforts to keep personal data correct and to reflect the latest status
- To take measures for safety management to prevent leakage, lose, damage, etc. of personal data
- When providing a third party with personal data, to obtain the consent of the person concerned

Article 7 (Limitations on Information Collection and Use in Cases Where Recording Personal Information in RFID Tags)

Companies dealing with personal information by recording such information in said RFID tags shall, notwithstanding the amount of personal information to be dealt with by the said companies, where collecting or using personal information, make efforts to inform persons concerned of the purposes of the use of personal information or announce to that effect. Companies shall make efforts to obtain consent from the principal when using the said personal information for purposes other than the purposes of the use of personal information

Article 8 (Ensuring of Information Accuracy Where Recording Personal Information in RFID Tags)

Companies dealing with personal information by recording personal information in RFID tags shall, notwithstanding the amount of personal information recorded in said RFID tags to be dealt with by the said companies, where collecting or using personal information, make efforts to meet the following items:

1. To keep personal information accurate and to reflect the latest status, in light of the purposes and details of the use of personal information recorded in said RFID tags

2. In response to consumers, to disclose information recorded in RFID tags relating to the said consumers and personal information of the said consumers linked from ID information recorded in RFID tags; and in response to requests from said consumers, to correct errors contained in said information

3. To prevent lose, damage, alteration and leakage of personal data recorded in RFID tags

Article 9 (Establishment of Information Administrator)

Companies concerned shall, in order to ensure adequate management of information pertaining to privacy protection concerning RFID tags and to make appropriate and swift response to complaints, establish an information administrator in charge of such matters and disclose methods to contact the said information administrator.

Article 10 (Explanation and Information Offerings to Consumers)

Stakeholders, including companies, industry organizations and public entities, shall make efforts to encourage consumers to understand RFID tags through information provision, so that consumers can obtain correct knowledge on the purposes of the use of RFID tags, characteristics thereof, merits and demerits thereof.

d) Enterprise Privacy Group[219]

The Enterprise Privacy Group, a consultancy firm that is active in the area of data protection, freedom of information and related privacy issues, has developed a Privacy Code of Conduct for RFID Technologies (published 3 May 2005).

The Code of Conduct has to ensure that every user associated with an RFID system understands his responsibilities for protecting personal information, and acts accordingly.

Organizations that implement consumer-facing RFID Systems without first considering the misuse of the technology have suffered adverse media publicity from watchdog groups, and in consequence have had to modify or abandon their plans.

Any RFID implementation should therefore, according the Enterprise Privacy Group, incorporate privacy safeguards, based on a rigorous risk assessment process coupled with 'best practice' recommendations for controls. One such control device is the Code of Conduct.

[219] Toby Stevens (2005). 'A privacy Code of Conduct for RFID Technologies', Enterprise Privacy Group, Hants, 2005.

Annex 5: European activities in E-passports

MEMBER STATE	E-PASSPORT	PARTNERS
Austria	RFID-chip based Flex cover	OeSD (State's printing institute)
Belgium	RFID-chip based Flex cover	Oberthur
Cyprus	no data available	no data available
Czech Republic	Polycarbonate cover	Cz National Printing Agency STC Trüb (CH) Axalto tech
Germany	RFID-chip based Flex cover	Bundesdruckerei
Denmark	Polycarbonate RFID-chip based	Setec (Gemplus)
Estonia	RFID-chip based	Gemalto
Spain	Flex cover	FNMT
Finland	Polycarbonate RFID-chip based	Sentec (Gemplus)
France	Flex cover	Imprimerie nationale Axalto tech
Greece	Flex cover	Toppan (JP) ASK
Hungary	Flex cover	Multipolaris
Ireland	Polycarbonate	Bearingpoint
Italy	Flex cover	Polygraphico
Lithuania	Polycarbonate RFID-chip based	Setec (Gemplus)
Luxembourg	RFID-chip based	Bundesdruckerei Group, Phillips (NXP)
Latvia	RFID-chip based (expected to rollout by 3rd quarter of 2007) Polycarbonate	Gieseke & Devrient; Gemalto Bundesdruckerei Group
Malta	RFID-chip based, not rolled out yet	no data available
The Netherlands	Polycarbonate RFID-chip based	SDU Datecard Group Collis
Poland	RFID-chip based	Gemalto
Portugal	Flex cover	INCM
Sweden	Polycarbonate RFID-chip based	Crane/Setec (Gemplus)
Slovenia	Flex cover	Mirage/Cetis
Slovakia	RFID-chip based, not rolled out yet	no data available
United Kingdom	Flex cover	SPSL

Annex 6: Overview on ID documents in Europe

Country	Name	Card (C) or Procedure (P)	Purposes covered (explained below)	Technology or technologies used	Status, Comments, References
Europe	European Passport	C	Ident	RFID, Bio (Face, later Finger)	Concept, prototypes and early implementations (e.g. in Germany); implementation until October 2006.
Austria	“Bürgerkarte”	P	Sign	Cert, ElSig, requires PKI	Implemented since 2005, especially for e-government.
	e-card	C	e-health (Option: Sign)	SmCh	Implemented since 2005 with 8.3 Mio users.
Belgium	ID Card	C	Ident (Option: Sign)	SmCh, Cert, ElSig, requires PKI	Implemented since 2005.
Finland	FINEID Card	P	Sign	Cert, ElSig	Implemented since 1999.
France	e-ID Card	C	Ident	RFID, Bio (Face, later Finger)	INES concept (Identité Nationale Électronique Sécurisée); implementation planned to start in 2007.
Germany	ID Card	C	Ident (Option: Sign)	SmCh, Cert, (Option: ElSig)	Concept; implementation planned in 2007.
	E-Health Card	C	e-health (Option: Sign)	SmCh, Cert, (Option: ElSig)	Prototype.
	“JobCard”	P	Requires Sign, used for SocIn	Requires ElSig and PKI	Concept, planned to start in 2007. Aim is to centralise different procedures concerning social insurance in Germany. The access of the insurance holder to this information shall be possible via electronic signature card.
Greece	Traditional ID card	C	Ident	-	No plans for eID found.
Hungary	HUNEID	C	Sign	SmCh, Cert, ElSig	Concept and prototype. Within the Hungarian Electronic Public Administration Interoperability Framework currently standards are being defined and middleware is being specified.
Italy	ID Card (CIE)	C	Ident, Sign	SmCh, Cert, ElSig, Laser	Prototypes. Includes laser-band to store up to 1.8 mega-byte of data.
Malta	eID Card	P	e-Gov, m-Gov	Cert	Launched in 2005.
The Netherlands	ID Card	C	Ident	RFID, Bio (Face, later Finger)	Prototypes, introduction planned August 2006.
Portugal	“Cartão comum do cidadão”	C	Ident, SocIn, e-health, voting, tax	SmCh, Mag Stripe, Bio (finger, other?)	Citizen card project approved by Council of Ministers on April 2005. Seems to be in design phase still.

Country	Name	Card (C) or Proce dure (P)	Purposes covered (explained below)	Technology or technologies used	Status, Comments, References
Spain	eID card (“DNI electrónico”)	C	Ident (Option: Sign)	SmCh, Cert, ElSig (requires PKI), Bio (finger)	1st version presented in 2004. Card scheduled to begin in 2006. Delays probable.
Sweden	eID Card	C	Ident (Option: Sign)	SmCh, RFID, Bio (Face, later Finger), Options: Cert, ElSig; Options require PKI	Issued since 1st of October 2005. Includes contact chip, RFID and biometrics in accordance with the ICAO standards for international passports. Card issued by police, biometric and other identification data is centrally stored at police.

Source: Study on ID Documents, FIDIS (Future of identity in the Information Society.) 20 December 2006. fidis-wp3-del3.6.study_on_id_documents.doc

Purpose of identity document:

Ident	Official identification of a citizen of a state by passports or official identity cards
Sign	Identification of an individual/company and electronic signing for egovernment and / or e-commerce applications; remark: PKI integration needed
e-health	Identification of an individual and transfer of or access to sensitive data in the e-health sector (e-health cards)
SocIn	Identification of an individual and transfer of or access to sensitive data for social insurance purposes

Annex 7: RFID in European Public Transport projects

Public transport cards	Tag	system	application	numbers	project	benefits
Florence, Italy, ATAF	13.56 MHz C. ticket (ASK)	ASK	local and regional bus companies	n.a.	roll-out	optimise resources; meet passenger demands
Manchester, UK, GMPTE	13.56 MHz (ASK); ITSO compliant	ERG (Prepayment Cards Limited) (interrogator and system integrator); Stagecoach Holdings, Firstgroup, National Express Group	local and regional bus companies; 40 companies, 10 districts	10 districts transactions yearly, 650.000 residents	trial from 2004; roll-out 2006	Reduce abuse and fraud Reduce survey data costs Data capture for viable multi-operator Reduce misuse;
Liverpool, UK multi-functional card	13.56 MHz Applied Card Technologies 16 kB EEPROM	Global Smart Media Merseytravel	local public transport extended use as city smart card (if successfull)	n.a.	2005-… costs: 3.8 M USD cost per card: 6.5 USD	improved customer experience and value joint promotional opportunities coalition and affinity marketing oportunities
Paris RATP, France	13.56 MHz; ASK (C-tickets); Schlumberger; D&G		Successor to Carte Orange (since 20 March 2006); endorsed by RATP, SNCF and 93 private travel operators			Reduce maintenance costs; combat fraud; Increase passenger flows (up to 400%)
Rhein-Main Verkehrsverbund buses	13.56 MHz (Nokia, Philips)) NFC application	Nokia, Philips	NFC application in public transport	n.a.		
Skane County, Sweden	Cubic Nord	Cubic Nord	Smart card in trains and buses 56 rail stations, 950 buses; open architecture		started costs: 21.8 M USD	Reduce fraud and misurse Increase user convenience (internet based uploading of cards
Southport, UK	13.56 MHz (Philips Mikron card))	na	10.000 cards issued for buses		roll-out (on-going)	
Stor-Oslo Lokaltrafikk, Norway	13.56 MHz (Thales)	Thales	Clearinghouse system to settle payments of contactless cards		2006-2007	user convenience (contactless cards are better than contact cards in moving buses); fraude detection
Translink, Netherlands	13.56 MHz (Mifare 4K card, Philips) C.ticket (ASK) ASK	Thales, Accenture, Vialis	Dutch public transport system	pilot phase 1.4 M cards; roll-out: 10 M cards processing 1.5 B transactions yearly	2004	travel information fraud reduction speeding up boarding time
Transport for London, Oyster card	13.56 MhHz Schlumberger Sema, G&D, Infineon, Axalto	Cubic (interrogator); TranSys (system integrator)	Oyster travelcard for London	2.2 M Oyster cards	value of the contract: 1.6 B USD (17 years creation and operation) 300 M USD capital investment programme	Fraud reduction (now 65M USD per year); Speeding up boarding time Customer benefits (queues, ease of use); operational costs

Public transport cards	Tag	system	application	numbers	project	benefits
Umico Capri, Italy	13.56 MHz ASK (C.ticket)	ASK	Public transport at Capri	2.5 M C. tickets	300 M capital investment programme	
Verband Deutscher Verkehrsun-ternehmen, Germany	card.etc; ERG, SmardTech SMicroelec-tornics	card.etc; ERG, SmardTech SMicroelec-tornics	Local transport companies to use smart cards for all PTO-services	2.3 M cards initially	Roll-out 2009	Research
Warsaw transit Cards			Payment on subway trains and buses in Warsaw	1.5 Million cards		

Source: IDTechEx Knowledge base www.idtechex.org (visited 25 June 2006)

Annex 8: RFID pilots and trials within the EU and the US

Member states	Total	Airlines and airports	Animals and farming	Books, Libraries, Archives	Financials, Security Safety	Health care	Land and Sea Logistics, Postal
Austria	13		1	1			1
Belgium	7			1	1		3
Czech Republic	6				2		1
Denmark	19			1	2	1	2
Estonia	2				1		
Finland	13	4			2		2
France	86	2	3	4	12	12	14
Germany	120	7	1	6	14	12	16
Greece	4				1		
Hungary	4						
Ireland	5				2		1
Italy	40			1	4	4	4
Latvia	1						
Lithuania	1						
Luxembourg	1						
Netherlands	62	2		2	12		11
Poland	6						1
Portugal	6			2		2	
Slovakia	4						1
Slovenia	2				1		
Spain	21		2				1
Sweden	36	2	1		4	1	6
United Kingdom	255	11	10	7	65	27	32
USA	812	26	24	22	121	90	56
Total Europe	714	28	18	25	123	59	96
Total	2240	54	42	47	244	149	152

Member states	Laundry	Leisure, Sports	Manufacturing	Military	Passenger Transport, Automotive	Retail, Consumer Goods
Austria		8	1			1
Belgium		1		1		
Czech Republic				1	2	
Denmark		7	1	2	3	
Estonia				1		
Finland		2			1	2
France		12	2	4	9	12
Germany		11	14	3	16	20
Greece		1		1	1	
Hungary		3		1		
Ireland		1	1			
Italy		8	2	2	9	6
Latvia				1		
Lithuania				1		
Luxembourg				1		
Netherlands	2	18	3	2	6	4
Poland		1		1	3	
Portugal				1	1	
Slovakia		2		1		
Slovenia				1		
Spain		8		3	1	6
Sweden		7	3		8	4
United Kingdom	1	17	13	7	36	29
USA	5	40	58	33	89	248
Total Europe	3	107	40	35	96	84
Total	8	147	98	68	185	332

Source: IDTechEx Knowledge base www.idtechex.org (visited 16 October 2006)

Annex 9: Full contents

European Commission

EUR 22770 EN – Joint Research Centre – Institute for Prospective Technological Studies

Title: RFID Technologies: Emerging Issues, Challenges and Policy Options

Authors: Marc van Lieshout, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij, Claudio Borean.

Editors: Ioannis Maghiros, Pawel Rotter, Marc van Lieshout…

Luxembourg: Office for Official Publications of the European Communities

2007

EUR – Scientific and Technical Research series – ISSN 1018-5593

ISBN 978-92-79-05695-6

Abstract

Radio Frequency Identification (RFID) technology, an enabling technology for automatic identification based on radio waves, will impact the daily lives of European citizens in many different ways, as it is a bridge between the physical and the virtual world. RFID has enormous socio-economic potential but it also brings challenges, such as serious security threats and the potential danger of impinging on personal lives, which if not addressed properly may limit the foreseen benefits from the wide-spread deployment of this technology. This report gives an overview of established and emerging RFID technologies, RFID standards and spectrum allocation, presents RFID market parameters and forecast, privacy and security issues and social aspects of RFID. Five case studies from different application sectors (animal tracking, healthcare, ICT sector, identity cards and public transport) allow us to draw conclusions about both specific areas of development and the whole RFID market in Europe. In the final part, the likely role of Europe is presented, as are policy options for further initiatives.

RFID Technologies: Emerging Issues, Challenges and Policy Options

EUR 22770 EN

JRC
EUROPEAN COMMISSION

INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES
ipts

EN
LF-NA-22770-EN-C

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

Publications Office
Publications.eu.int

ISBN 978-92-79-05695-6
9 789279 056956