Bundesamt
für Sicherheit in der
Informationstechnik

Security Aspects and Prospective Applications of RFID Systems

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

The present study was prepared for, and in cooperation with, the Federal Office for Information Security (BSI) in an interdisciplinary collaborative arrangement between IZT — Institute for Futures Studies and Technology Assessment and the Swiss Federal Laboratories for Materials Testing and Research (EMPA).

Over recent years the realization has caught hold that evaluating technical developments should be done prospectively and in a problem-oriented fashion, in order to gain indications about future technology design. This can be accomplished through interdisciplinary assessment of the opportunities and risks of using RFID, focussing on the areas of IT security and data protection. Only in this way can real or perceived security problems be recognised early as central barriers to the economic use of RFID technology, and thus can perhaps be avoided as early as possible.

The objective of the present study "Security Aspects and Prospective Applications of RFID Systems" is to give the interested (specialized) public an overview of the technical basics, application potentials and risks of RFID systems. The study's main focus lies in the prospective analysis of possible threats which result from using RFID systems, including an assessment of the effectiveness of existing security measures. In addition to that, visual aids and a great number of practical examples demonstrate which RFID systems are being used today and which are being tested for the future.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: RFID@bsi.bund.de
Internet: http://www.bsi.bund.de

Contents

Figures and Tables

Authors

The following were involved in producing this study:

IZT – Institute for Futures Studies and Technology Assessment

Britta Oertel
Michaela Wölk

assisted by:

Barbara Debus,

Volker Handke,

Mandy Scheermesser

Empa – Swiss Federal Laboratories for Materials Testing and Research

Prof. Dr. Lorenz Hilty
Andreas Köhler

assisted by:

Claudia Som,

Thomas Ruddy

BSI – Federal Office for Information Security

Harald Kelter
Markus Ullmann
Stefan Wittmann

Experts

Klaus Finkenzeller,
Fa. Giesecke & Devrient. Forschung & Entwicklung Chipkarten, Abteilung Neue Technologien

Christian Flörkemeier,
Institut für Pervasive Computing, ETH Zürich

Dirk Henrici,
Fachbereich Informatik, Universität Kaiserslautern

Peter Jacob,
Eidgenössische Materialprüfungs- und Forschungsanstalt, Dübendorf

Marc Langheinrich,
Institut für Pervasive Computing, ETH Zürich

Gregor Ponert,
Leiter der Abteilung Research & Development, Skidata AG

Thomas Schoch,
Intellion AG, St.Gallen

Moritz Strasser,
nstitut für Informatik und Gesellschaft, Universität Freiburg

Jens Strücken,
Institut für Informatik und Gesellschaft, Universität Freiburg

Dr. Frédéric Thiesse,
Institut für Technologiemanagement, Universität St. Gallen

Dr. Martin Wölker, COGNID Consulting GmbH

In addition to the experts mentioned above, we would like to thank the experts who participated in the empirical online survey.

We would like to extend a special thanks to Klaus Finkenzeller, who allowed us to use most of the figures on RFID technology for the present study.

We gladly refer here to the RFID handbook that he has written, which holds a wealth of detailed technical knowledge for interested persons (http://www.rfid-handbook.de).

1. Preface

When one regards the technical potential of modern RFID technology and the risks associated with them, one realizes that using this technology is sure to have effects in the most diverse areas of IT security and society.

Today RFID tags are being used in access-control facilities combined with a company ID card, the European Central Bank is planning to use them in mini-versions in bank notes to prevent counterfeiting and public transportation authorities would like to affix transponders to the tickets of their passengers, so as to have a central system of who used which connection when.

Preventing counterfeiting or having an easy way to manage the use of public transportation are sensible uses of RFID chips. In the interest of the citizen, RFID technology can increase security and customer friendliness. However there is also skepticism concerning the unobtrusive transmitters, although they are so hard to see – or perhaps for that very reason: the current discussion surrounding the Metro Future Store, in which RFID tags were to be used, shows that a company that fails to enlighten its customers early on can quickly find itself under attack by privacy and citizen rights organizations.

The reason for the bad feelings is the possibility that the chip could be read without authorization and without even being noticed: the content of one's shopping bag and purse could become totally transparent.

What conclusions should we draw from these facts?

Today the new technologies offer enormously profitable opportunities, as RFID can be used for many purposes including the entire logistics and warehouse management areas. What remains to be done is to analyse the technology with regard to its effects in the most diverse applications, to describe and assess the effects of using the technology and to identify the opportunities and risks that result, in order to provide better recommendations for policy makers, industry and science.

The answers offered in the present study are intended to comprise a contribution toward making the discussion about using RFID technology more objective and to help find ways to apply technology that satisfy the dual goals of utility and data protection.

Bonn, Germany, October 2004

Dr. Udo Helmbrecht

President of the Federal Office for Information Security

2. Foreword

One should be careful with words like revolution. However with the development of the futuristic visions of technology such as pervasive and ubiquitous computing, we think it is appropriate to speak of a revolutionary perspective on technology. This view is based on two reasons: the technology currently unfolding as pervasive or ubiquitous computing unites very basic technologies such as the use of microprocessors, wireless radio technologies and data transmission through universal networks such as the Internet. Such inventions are showing up all over today, especially in the areas of manufacturing and goods distribution, product authentication and animal identification, as well as in areas such as authentication of documents, maintenance and repair, access and route control, theft prevention and environmental monitoring; the new potential use areas abound.

The likelihood that these technologies will permeate all areas of our lives results from one important property of the basic technologies: they raise efficiency with regard to work, time and space, permitting us to react faster to changes in object parameters. The innovation and automation potentials associated with this are strong incentives to have the technologies implemented immediately in a competitive international economy.

Against this background no one can wonder why automatic identification systems (auto-ID systems) are prospering in such areas as those in which progress in productivity can be achieved through automation. This applies especially to Radio Frequency Identification (RFID) systems, which expand upon the functions and uses of the older automatic identification solutions such as barcode and Optical Character Recognition (OCR). RFID can be understood as a central step towards further integrative technology development in the direction of pervasive and ubiquitous computing.

As always in case of revolutionary technology waves, the opportunities and risks are close to one another. Socially the risks include the effect of the rationalization potential and new models of work organization on our life and work styles, which were already mobile and volatile. Ecologically, they mean the ever-present use of technological microsystems, which cause us to expect enormous rebound effects and an increase in the dispersion of materials we consider valuable and others we consider ecologically less desirable. Against this background it becomes one of the most important tasks for scientists to discover as early as possible the opportunities, problems and risks. Designing technology in a socially compatible manner includes promoting interaction among various social interest groups and economic and political actors, and then seeking compromises among them all.

When the movement and use of everyday things leave data tracks, which escape any control by the user, this can have serious effects on our understanding of security and privacy. Starting with technology assessment and a constant interaction between science and society, a public dialogue must take place with policy-makers, business leaders, civil society groups and citizens on these problems. Only in such a public discussion process with scientific support can we find out what desirable goals are to be aimed at and which technology developments are suited to maximize the opportunities and minimize the risks.

Thus the present study offers a survey of the central technological developments and economic applications of RFID system. In addition, it analyses the basically new threats and looks at conventional security measures.

We would like to thank all authors and experts who took part in this study for their conscientious and trend-setting work and important findings. We are sure that the required social dialogue will take valuable impulses from this study for these important questions affecting the future of us all.

Berlin and St. Gallen in October 2004

Prof. Dr. Rolf Kreibich

Dr. Xaver Edelmann

3. Summary

Situation at the outset

The new paradigm known as “pervasive computing” or “ubiquitous computing” refers to a new development in the field of information and communication technology. During this development more and more everyday objects will be equipped with microelectronics. Such “intelligent” or “smart” objects will influence almost all areas of our daily lives. Computers will do their work invisibly in the background.

One essential part of the development track in the paradigm of pervasive computing is comprised by digital automatic identification systems (auto-ID systems), which are expected to replace barcode and Optical Character Recognition. Auto-ID technology is designed to provide information about objects (persons, animals, merchandise). RFID systems (referring to Radio Frequency IDentification) expand the functionality and possible uses of traditional auto-ID systems and offer high potential increases in efficiency, for instance, in manufacturing and goods distribution and the areas of product authentication and customer relationship management.

The vision of total networking of our everyday lives offers not only new ways of doing things and great opportunities, but also holds risks. The question as to the security of RFID systems is increasingly becoming a key issue for the development and design of society’s exchanges of data, information and knowledge. Nowadays the economic success of companies depends primarily on the degree to which their internal data stocks and external communication can be protected against data loss and data abuse. A second key issue is the question as to whether and in what form additional consumer and data protection regulations are becoming necessary as RFID systems spread, sparking off a social debate under such terms as “the naked customer” and “naked citizen”.

Over recent years the realization has caught hold that evaluating technical developments should be done prospectively and in a problem-oriented fashion, in order to gain indications about future technology design. This can be accomplished through interdisciplinary assessment of the opportunities and risks of using RFID, focussing on the areas of IT security and data protection. Only in this way can real or perceived security problems be recognised early as central barriers to the economic use of RFID technology, and thus can perhaps be avoided as early as possible.

Objectives of the study

The objective of the present study “Security Aspects and Prospective Applications of RFID Systems” is to give the interested (specialized) public an overview of the technical basics, application potentials and risks of RFID systems. The study’s main focus lies in the prospective analysis of possible threats which result from using RFID systems, including an assessment of the effectiveness of existing security measures. In addition to that, visual aids and a great number of practical examples demonstrate which RFID systems are being used today and which are being tested for the future.

In order to assess better the opportunities and risks of RFID systems, an assessment of the essential technological, economic, legal and social developments is done in the context of RFID systems, spanning a time horizon until 2010. Fictive case studies serve to make the risks more palpable, but are explicitly not to be understood as forecasts.

The present study is intended to contribute to making people more aware of the topic of information security in the innovative area of RFID, to make decision-makers aware of the concrete potential and dangers, and to motivate them to analyse information technology systems in companies and organizations appropriately and proactively, and to protect the systems in a sustainable manner.

Definition of RFID systems

RFID refers to procedures to automatically identify objects using radio waves. The use of an RFID system is appropriate basically everywhere that something has to be automatically labelled, identified, registered, stored, monitored or transported. RFID systems are available in a wide variety. Despite the wide range of RFID solutions, each RFID system is defined by the following three features:

1. Electronic identification:
   The system makes possible an unambiguous labelling of objects by means of electronically stored data.
2. Contactless data transmission:
   Data identifying the object can be read wirelessly through a radio frequency channel.
3. Transmit when requested (on call)
   A labelled object only transmits data when a matching reader initiates this process.

In technical terms, an RFID system consists of two components: a transponder and a reader:

The transponder – also known as a tag – acts as the actual data carrier. It is applied to an object (for instance, on a good or package) or integrated into an object (for instance, in a smart card) and can be read without making contact, and rewritten depending on the technology used. Basically the transponder consists of an integrated circuit and a radio-frequency module. An identification number is stored along with other data on the transponder and the object with which it is connected.

The reading unit – typically only called the reader, as in the following – consists of a reading, in some cases a write/read, unit and an antenna. The reader reads data from the transponder and in some cases instructs the transponder to store further data. The reader also monitors the quality of data transmission. Readers are typically equipped with an additional interface to pass the data received on to an another system (PC, electronic control, etc.) and to process them there.

RFID systems use frequency ranges from long wave to microwave. Another characteristic of RFID systems is the type of storage technology that they use. Basically these can be either of the read-only or read/write type. Also the type of energy supply to the transponder matters, whether it is an active one with its own energy supply, or a passive transponder, which has to get energy from the reader.

The categories obtained in this way can be broken down according to the performance of their respective components into low-end systems, medium-performance systems and high-end systems. Another classification scheme for RFID solutions is based on the respective range, meaning the maximum distance between transponder and reader. It usually distinguishes among close-coupling, remote coupling and long-range systems.

The shapes of transponders vary from glass cylinder transponders to the electrical earmark to credit-card formats, various disc shapes and impact-resistant and heat-resistant up to 200° Celsius for the paint shops of the automobile industry. Their great design freedom for identification points, shapes, sizes and the field characteristics of their antennas make RFID systems a very versatile automatic identification technology on the whole.

The categories described above make it possible to classify RFID systems based on the applications possible with them and to make an assessment of the issues associated with that involving information security and data protection.

The threat situation and an inventory of common security measures

The integrity of RFID systems depends on the following three relationships:

1. The relationship between the data stored on a transponder (RFID tag) and the transponder itself. This must be a unique relation, because the transponder is identified solely by the data. The most important part of the data is a unique ID number (serial number). It is imperative to prevent the existence of two tags bearing the same identity.
2. The relationship between the transponder and the tagged item which it is meant to identify (mechanical connection).
   This relation, too, must be unique in the sense that a transponder must never be assigned to different items while it is in use.
3. The relationship between transponder and reader (air interface).
   This relationship must be established in such a way that authorized readers can detect the presence

of the transponder and can correctly access the data, while access by unauthorized readers is barred.

Considering these prerequisites, we can now turn to the following possible types of attack on RFID systems, each of which takes advantage of one of the prerequisites:

- Eavesdropping the communication between the RFID tag and the reader:
  Eavesdropping via the air interface is possible. The risk grows with the maximum distance of the normal read sequence. The risk is relatively low in the case of transponders with very short ranges.
- Unauthorized read access to the data:
  This is possible without great outlays for the attacker if the reader distance is normal. He has to get a reader and perhaps install it inconspicuously. Software products are on the market that work on mobile readers and, for instance, can read and write tags in supermarkets. The possibilities of such attacks are limited by the short range; in a monitored environment therefore they can be counteracted.
- Unauthorized write access to the data:
  In the case of rewritable tags the possibilities of unauthorized changing of the data are the same as in the case of unauthorized reading. If read-only tags are used, unauthorized changing of data is excluded intrinsically. However read-only tags have the disadvantage that encryption and secure authentication cannot be done with them.
- Cloning und Emulation:
  In the case of cloning, the data content of a tag is read out or discovered in some other way in order to write a new tag with the data. This tag is then used to simulate the identity of the original tag. In addition, it is conceivable to employ devices having a high degree of functionality which are used to emulate any kind of tag with a given data content.
- Deaching the tag from the tagged item:
  This attack appears trivial, but that is precisely why it should also be borne in mind. Each RFID system depends on the tags being present on the intended items. "Switching" tags (as is also done nowadays with price labels) with fraudulent intent or merely with the intention of creating confusion is an obvious manipulation.
- Mechanical or chemical destruction:
  RFID tags can be mechanically or chemically damaged. The antennae in particular are vulnerable.
- Destruction by exposure to an electromagnetic field:
  Destruction by exposure to an electromagnetic field is standard practice in the case of anti-theft EAS tags (1-bit transponders) which are deactivated at the point of sale. In principle, all kinds of transponders can be destroyed by a strong electromagnetic field. However because of the high field strength that is required, this attack can only be carried out at very close range. There are indications that radio inductors or high-voltage switching events taking place close by could induce enough voltage peaks to damage the chips.
- Destruction by misuse of a kill command:
  If, for data privacy reasons, tags are equipped with a kill function that partially or totally erases the data content, this function can be misused.
- Discharging the battery (only in the case of active tags):
  In the case of active tags which have a back-up battery, the latter can be discharged by causing the tag to transmit frequently in response to a rapid sequence of queries.
- Blocking:
  In contrast to the use of jamming transmitters, the use of blocker tags is not forbidden by law, because their passive design does not constitute a transmitting system. Basically there is no absolute protection against blocking with a given protocol. However since various protocols are in use, the user of the blocker tag must either carry several such tags with him in order to cover all the possible protocols, or he must use a single blocker device that copes with all the protocols used.

- Jamming transmitters:
  Effective interference of operation at a distance calls for powerful transmitters. Operating such jamming transmitters is illegal and it is difficult for technically inexperienced persons to obtain them. Radio amateurs do have access to this technology.
- Frequency detuning:
  This attack is carried out by bringing relevant amounts of, for example, water, metal or ferrite into close proximity of the field or the tag antenna. It might even be enough simply to cover the tag with the hand. However, frequency detuning is less reliable in its effect than shielding and no less obvious.
- Shielding:
  Tags can be shielded by wrapping them in metal foil (e.g. aluminium foil) or by placing them in aluminium-coated freezer bags, or in handbags equipped with metal strips.

Against most of these threats there are countermeasures, some of which are more expensive and some of which are less expensive than the attack.

In the first instance these threats are relevant for the active party, i.e. for the operator of the RFID system, who manages the tags and the data associated with them. For the passive party, who wants to or must use the tags, but has no control over the data, the threat potential is not the same. The latter case is a possible violation of privacy, especially when data traces of object movements are stored in central databases by RFID applications. Access to the database in the back-end of the RFID system may pose a greater risk for the passive party than one to the frontend (eavesdropping the air interface). RFID data traces have a specifically high spatial and time density, which often makes it possible to create personalized movement and contact profiles, even when the data were originally in pseudonymized or anonymized form. Such intrusions on data privacy or location privacy may happen when the active party violates the data protection law or fair information practices or when it is forced by a third party to open its data stocks. The degree to which RFID systems add a relevant threat potential to the data tracks that are already produced by other systems (credit cards, loyalty cards, mobile phones) is controversial among experts. In addition to the violation of privacy, the pushing off of risks from the active to the passive party is to be seen as a possible threat.

Applications

RFID systems have been displaying a continual market development in selected market segments for decades now (for instance, in the area of animal identification or in the form of car locks). Depending on various application conditions, some of which are sector-specific, RFID systems are being used over the whole range of possible technological complexity. In other segments RFID’s means of automatic and contactless identification is being tested in numerous pilot studies.

RFID technology is a typical cross-section technology whose potential application can be found in practically all areas of daily life and business. Theoretically the application areas of RFID systems are unlimited. From a cross-industry viewpoint, the following areas of applications can be distinguished:

- identification of objects
- document authentication
- maintenance and repair, recall campaigns
- theft-protection and stop-loss strategies
- access authorization and routing control
- environmental monitoring and sensor technology
- supply chain management: automation, process control and optimization

Much of the available market data on the use of RFID systems are limited to individual economic sectors and fail to give a comprehensive market overview. The basic data used by various consulting firms, the survey methods and market classifications are very different from one another, not always understandable and cannot be compared with one another. As a result, the status of diffusion, sales and market shares of RFID systems remain unclear. The answer to the question as to whether RFID systems will be used in the future as mass technology depends on such factors as the success of the pilot projects running now.

It is possible to show in individual areas of application the advantages stemming from the use of RFID systems, for example, for retailers, manufacturers or for logistic service providers. Opportunities are seen especially in such application areas and sectors in which productivity advances can be had through more automation. A study done by Booz Allen Hamilton jointly with the University of St. Gallen on the logistic and automobile industries, however, showed that investments in RFID are still risky for many companies and a positive return on investment exists mainly for niche applications. Against this background it is not surprising that company-internal RFID systems dominate in practice. The potential of RFID systems, however, exists especially in inter-company use, for example, in tracking merchandise through the whole value chain.

The use of transponders is nowadays going beyond the pure identification of objects to control merchandise in complex systems. This is why transponders are increasingly used in logistics. In order to manage logistic processes efficiently, more and more data are needed, which are automatically gathered and processed along the entire supply chain. In this application segment RFID technology opens up extensive solutions. Also in the area of environmental monitoring RFID systems with miniaturized sensors can contribute to observing the many phenomena in the natural environment and monitoring environmental stress with a degree of accuracy that had not been possible before.

One of the main growth factors for the spread of RFID systems is the drop in prices and the rise in legal requirements. RFID systems are showing up in the requirements of the European Union on economic actors in logistics and agriculture including all upstream and downstream stages of value creation (such as tracing foods, protecting against epidemics). Likewise, essential elements are to be found that influence the future development of RFID systems in relation to compatibility, interoperability and establishing uniform standards. Positive impulses are also coming from the increasing public knowledge about RFID solutions and the availability of customer-oriented solutions.

Expected developments and challenges

The economic success of RFID technologies will depend not only on technical possibilities. In addition to technology and standardization, the market and price developments, the requirements on information security and data protection have to be considered along with social discourse in the context of RFID.

For the coming ten years one can expect a further exponential increase in the performance of information and communication technology. In addition to the improvement in price/benefit ratios, the technological components used will become dramatically smaller. Even if the miniaturization of transponder antennas encounters physical limits, other possibilities such as weaving the antennas right into textiles could help make RFID tags practically invisible. The miniaturization of microchips will probably continue for another ten years without a technology shift. It is one of the essential drivers behind the vision of pervasive computing.

According to the opinions of experts in companies and research establishments working in the RFID sector, essential technological factors currently inhibiting the spread and use of RFID systems will be overcome by the Year 2007 or 2010. These inhibiting factors include the low ranges of readers, problems in multi-access identification and recognition across different frequency bands. No one expects the current incompatibilities among the RFID solutions of the various manufacturers to be overcome anytime soon. The findings of analyses show for the coming years up to 2010 a positive or at least stable market development in Germany. Likewise on the whole falling prices are expected. Estimates as to which application areas RFID systems will continue to expand in are varied. On the long range, a positive market development is expected in the application areas “Surveillance of access, rooms and routes”, “Supply chain: automation, process control and optimization”, “Labelling merchandise, objects, animals or persons”, “Take-back and multiple-use systems, disposal and recycling”, and “Maintenance and repair, recalls”.

A radical informatization of our everyday and professional lives with objects that sense part of their environment and communicate with one another also has basic effects on information security and privacy in addition to economic potentials. Using RFID systems, it becomes much easier to collect data. As RFID technology continues its advance, the question arises as to who can determine, or is allowed to determine, whether and which information is associated with electronically empowered things. Finally one should also remember that in an informatized world the correct functioning of information technological infrastructure can become a matter of life and death for society and the individual. The advancing miniaturization of technological systems gives one reason to fear that existing legal prohibitions will no longer be monitorable or enforceable as RFID systems advance. Therefore one must counteract the growing difficulties in managing large technical systems by ensuring more transparency, in order to improve user trust in RFID technology.

In order to use the opportunities of RFID and at the same time to keep the threats as small as possible, it will be a matter of implementing the principles of modern data protection (privacy) laws early in the design process and in market introduction. This will also entail the principle of data economy and the most rapid possible anonymization or pseudoonymization of person-specific data. This urgency is all the greater since it is increasingly difficult to redesign any single country’s political and legal environment in the face of globalization.

The question as to whether and how fast social groups may open themselves to RFID technology is difficult to answer. In the debate about the opportunities and risks of RFID technology two opposing positions are crystallizing: whereas one side focuses on the opportunities which result from use of RFID, the other side emphasizes the risks, threats and limitations. The present study has focused more on the risks than on the opportunities, as its initiator requested. In the way of precaution, risks should be identified as early as possible so that one can reflect on a development and steer it in a positive direction.

Since in a modern, differentiated society a variety of different sized interest groups exists, some of which are in competition with one another, it will be important for future developments to reflect the pluralism of these opinions in an appropriate ratio in the field of RFID. One should create more transparency in the discussion of RFID. That would be a central step toward making the discussion more objective, and social opinion formation could be improved by more objectivity.

4. Introduction

4.1 RFID as a key technology of pervasive computing

Many factors have been determining the development of information technology systems for many years now: some of them are the continuing miniaturization of components, the continually rising performance of processors, the availability of memory even in small places, higher communication bandwidth in telecommunication and progress in materials sciences. The rapid exchange of digitally stored information in large networks by means of a rising number of actors and transmission paths is a central feature of information and knowledge societies. Human/machine communication is gradually being supplemented by the communication and networking of machines – without any people being directly involved.

Against this background the term “ubiquitous computing” and pervasive computing are being pushed to the forefront of public discussion: the term “ubiquitous computing” describes a vision of unobtrusive technology in which the computer as we know it today recedes into the background and smart objects communicate directly with one another.

In the area of business, the term “pervasive computing” is used for this paradigm. It also describes the ever-present, pervasive processing and networking of information. However pervasive computing” emphasises those solutions that are feasible in the near future more so than does ubiquitous computing. [Source: LaMa 03] Pervasive computing is regarded as a new application form of information and communication technologies (ICT) and is characterized by the following features:

- miniaturization: ICT components are becoming smaller and thus more portable than the devices common today
- embeddedness: ICT components are being embedded into other devices and objects of daily life (smart objects)
- networking: ICT components are being networked with one another usually wire lessly
- ubiquity: ICT is becoming ever-present and does its work less and less conspicuously or even invisibly
- context-sensitivity: ICT components are can get information by wireless data exchange and by means of sensors. [Source: HBBB 03]

RFID systems (referring to Radio Frequency IDentification) comprise one important development track in the framework of ubiquitous or pervasive computing. RFID is a method of automatic identification and has been getting more and more public attention recently. If RFID had to be put in plain terms, it would mean “contactless identification”.

Automatic identification has the purpose of providing information on persons, animals, assets or merchandise in such a clearly defined and highly structured way that the data can be read and processed further by machines. In the future RFID will replace or supplement barcode, Optical Character Recognition (OCR) and contact-bearing smart cards. RFID systems can be used as powerful systems of identification with which a large quantity of data can be gathered and in some cases updated. However RFID does not unleash its full power until it is used for open- and closed-loop control of processes in a variety of application areas. From access control to following merchandise flows from the manufacturer to the consumer, the range of application areas – established or in pilot-testing – is growing continually.

RFID is not a new technology. The US military has been using RFID or its predecessor technologies since 1940, in order to trace the whereabouts of supplies such as fuel or explosives or to support the friend/foe recognition in allied airplanes. Since 1977 RFID systems have been released for civilian applications. One of the first applications was transponders for animal identification toward the end of the Eighties. [Source: Krem 04]

RFID is a term for technologies used to identify objects over certain distances without making contact. Typically the distance to be overcome (their range) is a matter of centimeters or meters.

Seen technologically, an RFID system consists of two components: a transponder and a reader:

- The transponder – also called a tag – acts as the data carrier. It is mounted on an object (for example on a product or package) or integrated into an object and can be read by radio technology without mak- ing contact and even updated depending on the technology. Basically the transponder consists of an integrated circuit and an RF module. An identification number and further data about the transponder itself and the object with which the transponder is connected are stored on the transponder.
- The reading device – typically called simply a reader, as it will be in the following remarks – consists of a read or read/write unit and an antenna depending on the technology used. The reader reads data from the transponder and in some case instructs the transponder to store more data. The reader also checks the quality of the data transmission. Readers are typically equipped with an additional interface (RS 232, RS 485, etc.), in order to pass on the data received to some other system (a PC, a machine control) and to process them there.

The great interest that business has shown in RFID systems is based on the assumption that the costs of RFID systems will drop in the future. Against this background advantage can be taken of the advantages of RFID systems that other Auto-ID methods do not have, in order to better implement process changes in distribution logistics, product life cycle management or customer relationship management. Governments as well as businesses are talking more and more about RFID applications, for example, as authentication certificates for passports and as carriers of biometric features.

Today the application areas are often such that the significance of the costs per RFID tag are low compared with the number and duration of use cycles or with the high value of the products tagged. For the coming years both the vendors of RFID systems and market researchers predict a sharply rising growth in RFID use.

However the technical, economic and social changes that accompany information and communication technologies raise not only questions about the opportunities but also ones about the dangers of these technologies. The question of the safety of information and communication connections is turning more and more into a key issue for the development and design of new levels of data and knowledge transfer. The economic success of companies depends on the degree to which they succeed in protecting their databases and external communications against data loss and data abuse. From the standpoint of consumer and data protection it becomes a matter of implementing principles in the world of networked and pervasive data processing that whenever data can be associated with persons – even after the fact – data are collected and processed in a manner avoiding personal references, only when necessary and only for the respective purpose intended. [Source: RPG 01]

Thus the recognition is growing that the evaluation of technological developments should take place prospectively and problem-oriented manner, in order to gain indications for a sustainable technology design in advance. Interdisciplinary assessment of the opportunities and risks of using RFID systems form part of this process with attention focussed on the areas information safety and data protection. Only in this way can real or perceived safety problems be recognized early on as central barriers to the cost-effective use of RFID technology, and thus be avoided whenever possible.

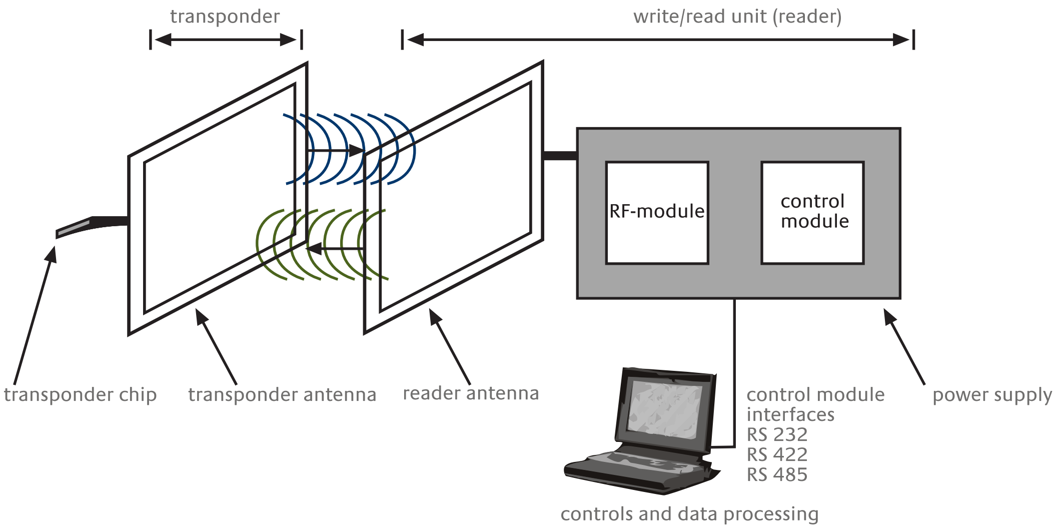


Figure 4- 1: Layout and basic functions of RFID systems [Source: Vinc 03]

4.2 The goals, methodological approach and structure of the study

Against this background the goal of this study “Security Aspects and Prospective Applications of RFID Systems” is to:

- document the current technological development in one part of pervasive computing, namely the use of RFID systems, and to highlight selected application areas;
- to assess effects in the area of IT security, and
- to present opportunities and risks of the use of RFID systems.

The study is intended to contribute to making people more aware of the topic of information security in the innovative area of RFID, to make decision-makers aware of the concrete potential and dangers and to motivate them to analyse information technology systems in companies and organizations appropriately and proactively, and to protect the systems in a sustainable manner.

The methodical approach of the present study is based on an intentional mix of quantitative and qualitative techniques. First, the status quo was established in the framework of a thorough analysis of literature and documents. Then a survey was done of companies offering RFID solutions and the variety of their RFID systems available on the market in Germany. It is on the basis of these findings that we present the basics of RFID technology, determine the variety of current solutions and classify the RFID systems available (Chapters 5 and 6).

Building on this, the types of attacks and countermeasures in the area of the information security of RFID were classified. Expert interviews were done as qualitative input on the phone or in person using a written guide. Judgements by recognized experts from companies and research institutions supplemented and deepened the findings of the literature and document analysis and the analysis of manufacturer information about the RFID systems available on the market (Chapter 7).

One further area on which the study concentrated was the determination of existing and future areas of application for RFID technology. Methods and approaches used today and being tested in pilot studies were presented in detail (Chapter 8).

Both the factors promoting and discouraging increased use of RFID systems were identified in a quantitative approach as were the strengths and weaknesses of selected Auto ID technologies compared with one another, the projected market development and the used of authentication techniques and other security measures from the standpoint of companies. We collected views from 70 companies which had had practical experience in the RFID field in an online survey done in August 2004. A total of 160 representatives of companies and research institutions were contacted by e-mail.

The organizations addressed included all the entities organized in the Association for Automatic Data Acquisition, Identification and Mobility (AIM-D e.V.). 43.75 per cent of the companies and research institutions responded to the online survey within three weeks.

Figure 4-2 shows how the responding companies are broken down by the various business sectors; it was possible to join more than one. Seven of the 160 companies replied that they were not working in the RFID sector und two questionnaires were filled out by companies that had not been addressed directly by us.

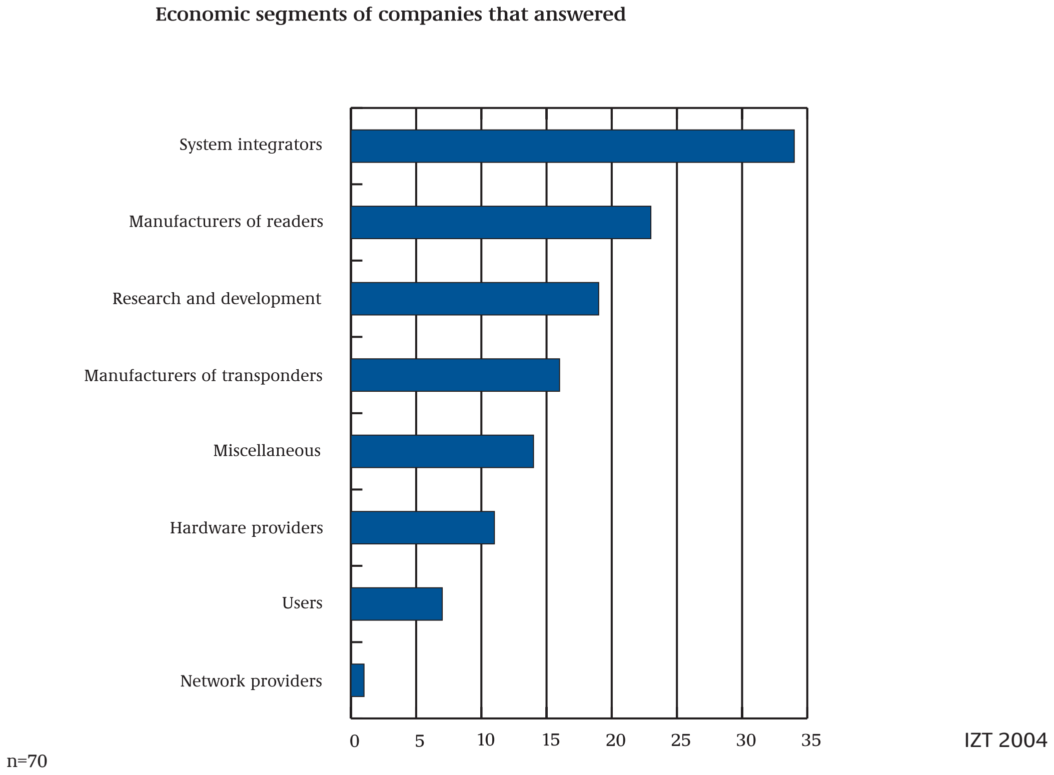


Figure 4-Fehler! Es wurde keine Folge festgelegt.**: Economic segments of companies that answered**

For one thing, the findings of the online survey in addition to the results from the literature and document analysis and the interviews conducted with experts form the basis for identifying factors promoting and discouraging the use of RFID systems. For another thing, they served as well in the analysis of central strengths and weaknesses of selected automatic identification methods (Chapter 9).

Furthermore, the findings helped us to estimate the development perspectives of RFID systems for the period up until the Year 2010. That involved first developing fictive case studies in the application contexts “Labelling Products” and “Access and Route Control”, which revealed theoretically possible risks of the use of RFID systems. Focussing on possible risks is based on the assumption that one decisive factor for the successful future development of RFID technology and the services and applications based on it lies in taking into account the requirements of information security and data protection in all phases of design and implementation. Thus, the case studies were intended to help reconcile the parties in a current discussion that is often controversial.

The study concludes with projections in the context of RFID systems. These include technological development tracks, a rise in the quality demanded from the areas of information security and data protection and the social acceptance of RFID systems (Chapter 10).

5. Basics of RFID technology

5.1 Features and versions of RFID systems

RFID systems are offered in a great variety. Despite the large variety of RFID solutions each RFID system is defined by the following three characteristics:

1. Electronic identification:
   The system makes possible an unambiguous labelling of objects by means of electronically stored data.
2. Contactless data transmission:
   Data can be read wirelessly by radio frequency channel identifying the object.
3. Transmit when requested (on call):
   A labelled object only transmits data when a matching reader initiatives this process.

RFID systems are a type of radiowave system. They differ from other digital radio technologies such as mobile phones, W-LAN or Bluetooth in two ways: electronic identification and transponders' feature of transmitting data only when requested to do so.

RFID systems must offer at least the following features:

1. identify the transponder within a specified range,
2. read the data of the transponder,
3. select the transponders relevant for the particular system,
4. guarantee that more than one transponder can be managed within the range of the reader,
5. have some way to recognise errors in order to guarantee operation security.

RFID systems may also have other features, for example the storage of additional data and security functions or the coupling with sensors. Then one is looking at special subclasses of RFID systems. Features to guarantee information security (for example cryptographic techniques for encrypting the transmitted data) are dealt with in Chapter 7.

One criterion that is important especially for inter-company applications is the so called ISO/IEC compatibility, which is becoming even more important. In the area of RFID systems the International Organization for Standardization (ISO) exercises the task of international standardization. ISO7IEC standards, for example, lay down frequencies, transmission speeds, protocols and codes. Currently there are standards for only a few RFID systems. Some of them are close-coupling systems, vicinity and proximity cards, which have the same dimensions as typical smart cards such as credit cards. Functions of vicinity cards are defined in ISO/IEC 15693. ISO/IEC 14443 defines the functions to be displayed by proximity cards. One of most important standards is the future ISO/IEC 18000, which will define the air interface for RFID systems of different frequency ranges. This standardization process will be published soon and then considered completed.

Both transponders and readers are currently being offered in various forms aimed at specific areas of application. The range of readers available can be roughly broken down into stationary and mobile versions, some of which are suitable for use in demanding environments. The range of transponder versions is also wide. These include:

- Smart labels: transponders used for labelling goods with numbers or prices, or placed on packages, boxes and palettes in the logistics area or fastened to airline luggage. These are called identification labels, which are applied to paper, cardboard or plastic as overlays;
- Glass cylinder transponders for applications requiring small dimension (such as locks or animal identifiers);
- Transponders in a plastic sheath for challenging applications, for example, in manufacturing or applications with exposure to moisture such as laminated disc tags;

- Industrial transponders in metal shapes for application to the area of industrial manufacturing for resistance to heat and chemicals;
- Large-scale transponders with long ranges for applications in the logistics systems for containers and railcars;
- Card transponders: embedded in plastic, transponders in credit card format (for instance, for access control and ticketing or as loyalty, bonus or service cards.

5.2 Features for distinguishing RFID systems

5.2.1 Frequency ranges

RFID systems use frequency ranges made available originally for Industrial, Scientific and Medical applications (so-called ISM frequencies) for one thing. In addition to that, in Europe the frequency range below 135 kHz and in the United States and Japan that below 400 kHz can be used for RFID applications. Worldwide the frequency ranges below 135 kHz , 13.56 MHz, 869 and 915 MHz respectively (the EU and the USA respectively) are available for the commercial use of RFID systems. The 2.45 GHz frequency range has still not reached a high degree of product maturity. The 5.8 GHz frequency range is also under discussion, but thus far there has not been much demand for it. In summary, the frequency ranges below 135 kHz and around 13.56 MHz appear to be proven and harmonized worldwide.

Frequency regulation is one of the main problems holding back the development of internationally usable RFID systems because of the lack of worldwide uniformity. In addition to the deviations in committing frequency ranges, different specifications regarding the transmitting output of readers is a second important limiting factor. In the range between 869/915 MHz , for instance, in the USA a maximum transmission output of four watts is permitted; in Europe however only 0.5 watts are allowed. That gap causes a significant difference in range: in Europe data may be transmitted only from a distance of approximately one meter to 2.5 meters. Even with RFID systems having the same design the range in the USA is only about six to eight meters. [Source: IDTE 04, RF-ID 04]

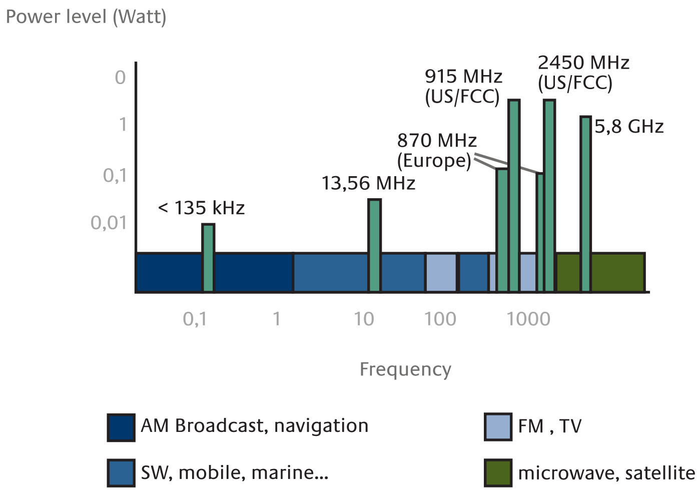


Figure 5-1. Worldwide frequency allocations for radio frequency identification [Source: Schu 00]

The characteristics of the different frequency ranges result in specific features or parameters that have to be taken into consideration in the design of RFID systems. Thus, typical fields of application have developed which have proven themselves most appropriate for the different types of transponder (see Table 5-1).

Parameter	Low frequency	High frequency	Ultrahigh frequency	Microwave
Frequency	125 – 134 kHz	13,56 MHz	868 bzw. 915 MHz	2,45 bzw. 5,8 GHz
Reading range	up to 1,2 m	up to 1,2 m	up to 4 m	up to 15 m (in some cases up to 1 km)
Reading speed	slow	acc. to ISO* standard	fast	very fast (active transpon-ders)
Moisture**	no effect	no effect	negative effect	negative effect
Metall**	negative effect	negative effect	no effect	no effect
Aiming of transponder during reading	not necessary	not necessary	sometimes necessary	necessary
Worldwide accepted frequency	yes	yes	in some places (EU/USA)	in some places (non EU)
Current ISO standards	11784/85 and14223	14443, 15693, and 18000	14443, 15693, and18000	18000
Typical transponder shapes	glass tube transponders, transponders in plastic housings, smart cards, smart labels	smart labels, industrial transponders	smart labels, industrial transponders	large-format transponders
Examples of applications	access and route controls, brakes, laundry cleaners, gas readers	laundry cleaners, asset manage-ment, ticketing, tracking and tracing, multi-access	palette tracking, container tracking	road pricing, container tracking

Table 5-2: Characteristics of RFID technologies [Source: Isch 04, endorsed]]

* under 1 s to 5 s acc. to ISO 14443 (5 s for 32 kBytes), average (0.5 m/s in passing acc. to ISO 15693)

** The influence of metal and liquids varies depending on the product. RFID tags are being offered nowadays that can also be used in the low-frequency range according to the manufacturer (for example, the "((rfid)) on metal" label from Schreiner Logidata).

5.2.2 Storage technology

General

One central distinguishing feature of RFID systems is the storage technology used, some of which are of the read-only type and others of the read/write type of system:

- Read-only transponders that can only be read by the reader once they have been programmed by the manufacturer are cheaper to produce. Variable information that is supposed to be associated with the tag must be stored in a database in the backend of the RFID system. When the tag is read, this information is retrieved from the database using the ID number (serial number) of the tag.
- Read/write transponders are more expensive to manufacture due to their memory feature. They can implement powerful security mechanisms and record information right on the transponder itself.

RFID systems utilize the ROM and RAM technologies described below.

ROM solutions (EPROM, EEPROM and flash EPROM)

ROM refers to a digital Read Only Memory in which data are recorded in an unchangeable form for long periods of time. The data are stored permanently during production in the structure of thee semiconductors and can neither electrically nor optically be erased or changed.

On the other hand, with EPROM, EEPROM and flash EPROM data can be erased and rerecorded. An EPROM (Erasable Programmable ROM) requires for this certain voltage impulses, which are delivered by an EPROM programmer. An erase sequence lasts several minutes.

Likewise voltage impulses are also used to program or to erase storage cells for rerecording on an EEPROM. The write/read cycles can be repeated up to 106 or 108 times respectively. The storage process is accomplished using a serial connection.

With a flash EPROM the storing of data is functionally identical with the case of an EEPROM. However the data are written and erased in blocks as in the case of a hard disk. Programming them is likewise time-consuming and complicated. The advantage of a flash EPROM is that the storage size that can be attained is not limited in size thanks to its simple and space-saving layout of its storage cells. The data are maintained up to ten years without power. A few typical applications of flash memory are the small storage cards in PCMCIA or compact flash format.

Primarily EEPROM are found in great numbers in RFID systems, making them important. Flash EPROMs are limited essentially to smart cards.

RAM solutions (DRAM, SRAM, FRAM)

A RAM is known as main memory in general speech. The main feature of a RAM is to write data on the storage component. However a source of uninterrupted power is needed; in the case of interruption to the power data are lost. RAM s have a chip to act as intermediate storage for data and programs, thus boosting the overall performance of the system through rapid access.

In the area of RFID systems so-called SRAMs (Static Random Access Memory) are used, which do not require that their storage content be regularly refreshed unlike the case of dynamic RAM (DRAMs). SRAMs' relatively high current demand is a disadvantage. Their relatively high price is another reason why SRAMs are being used less and less.

FRAM (Ferroelectric Random Access Memory) is a new development and has many advantages compared with conventional ROM: FRAM does not require any power for data maintenance. FRAM storage is compatible with that of common EEPROMs, but makes possible up to 10,000 times faster write and read processes than conventional EEPROMs (or even than flash technology). Data maintenance lasts over ten years even if the chip is exposed to extreme temperature fluctuations. With a guaranteed 1010 write and read cycles FRAM beats EEPROMs' performance with regard to this feature as well.

5.2.3 Energy supply to the transponder and data transmission

Active and passive transponders

Basically there are two types of transponder and hybrids of each type: active and passive transponders.

- Active transponders have their own source of energy to produce electromagnetic waves. Although they are battery-driven they do not wake up until they are sent an activation signal from a reader.
- Passive transponders, on the other hand, are supplied with energy by readers during a read sequence by means of radio waves. In comparison with active transpon ders they typically have a shorter ranges, but require more powerful readers for the energy supply to the transponder than active RFID systems do.

For the energy supply and communication from – or in some cases with – transponders two procedures are often used: the inductive coupling and the backscatter process based on the radar principle. However, first let us look at close-coupling systems which can also be supplied with energy due to the close distance between the transponder and reader by means of a capacitive coupling.

Capacitive coupling

The capacitive coupling is based on the plate condenser principle. The signal transmission takes place between two electrical conductors insulated from one another and connected in parallel both in the transponder and in the reader. Whenever an electrical signal produces a charge change on a conductor, the change affects the charge of the second conductor by means of an electrical field. The coupling capacity reached this way is relatively small, making this type unsuitable for the energy supply to microprocessors. Therefore such energy supply has to be provided inductively in addition.

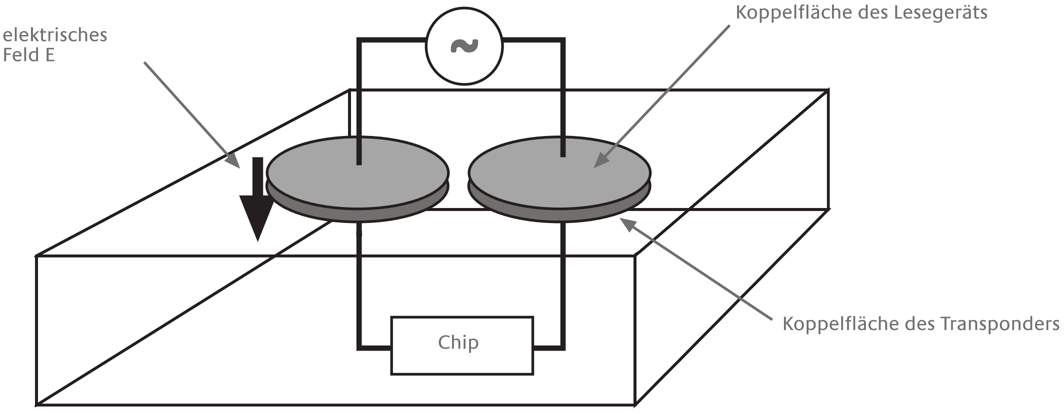


Figure 5-3: Capacitive coupling [Source: Fink 02]

Inductive coupling

Inductively coupled transponders are almost always passive transponders, so that the entire energy need for operation has to be provided by the reader. An inductively coupled transponder consists of an electronic data carrier and a large coil which serves as antenna. An electromagnetic field is created by the reader's antenna coil to supply energy to the transponder. Part of the field transmitted penetrates the transponder's coil antenna. A voltage is generated in the antenna coil of the transponder. This voltage is rectified and serves as the energy supply to the transponder. In preparation of the data transmission a condenser is connected with the reader's antenna in parallel, the capacity of which has been selected in such a way that a parallel resonant circuit is formed together with the coil inductivity of the antenna coil, the resonance frequency of which corresponds to the transmission frequency of the reader. the transponder's antenna also forms a resonant circuit with a condenser, which is tuned to the transmission frequency of the reader.

Whenever a resonant transponder is brought into the magnetic field of the reader's antenna, it derives energy from the magnetic field. The reaction of the transponder caused by that to the reader's antenna can be represented as transformed impedance in the reader's antenna. Switching a load resistor on and off on the transponder's antenna brings about a change in the transformed impedance and thus voltage changes in the reader's antenna. This has the effect of an amplitude modulation by the remote transponder. If the switching on and off of the load resistor is controlled by data, the data can be transmitted from the transponder to the reader.

In the reader the data are converted back by rectifying the voltage taken off the reader's antenna.

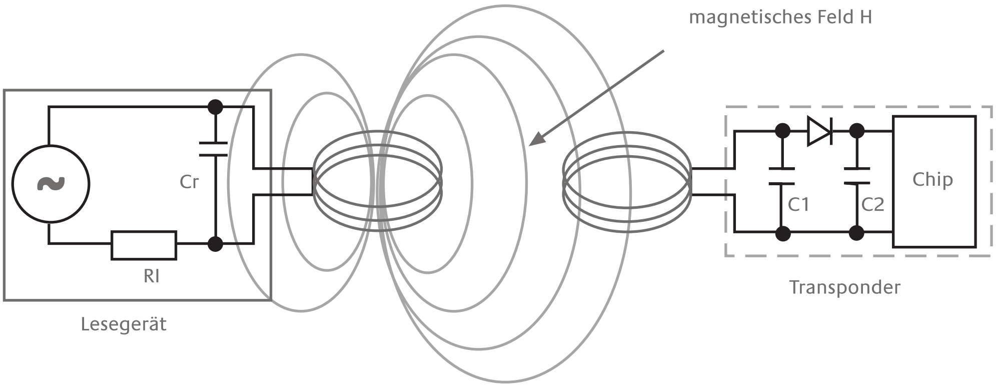


Figure 5-4: **Voltage supply to inductively coupled transponder from energy of magnetic alternating field produced by reader [Source: Fink 02]**

Backscatter procedure

The backscatter procedure is used mainly for long-range systems and is based on the principles of radar technology. The basic radar equation states that electomagnetic waves of materials that have an expansion of more than the half wavelength of the transmitted electromagnetic wave will be reflected. Electromagnetic waves are reflected especially well when the object which the wave hits starts to resonate.

In order to utilize this effect for RFID technology, a dipol antenna is designed both for the reader and for the transponder; the anntenna displays the resonance characteristics for the frequency being used in each case. As energy supply a certain transmission power is sent from the reader’s antenna. The power arriving at the transponder is available on the connections of the antenna and can be used as an energy supply for the transponder after being rectified.

Without a backup battery this technology reaches a range of approximately three meters at a transmission frequency of 868 MHz, and at 2.45 GHz can still reach a distance between transponder and reader of over one meter.

Part of the power arriving through the transponder’s antenna cannot be used for power supply and is reflected. How much of this power is reflected can be determined through the antenna’s characteristics. With the goal of data transmission a load resistor is connected in parallel to the dipol antenna in the transponder. If the load resistor is switched off and on in the rhythm of the bitstrom to be transmitted, an amplitude modulated signal is generated, which can be received by the reader’s antenna. This procedure is called “modulated backscatter”.

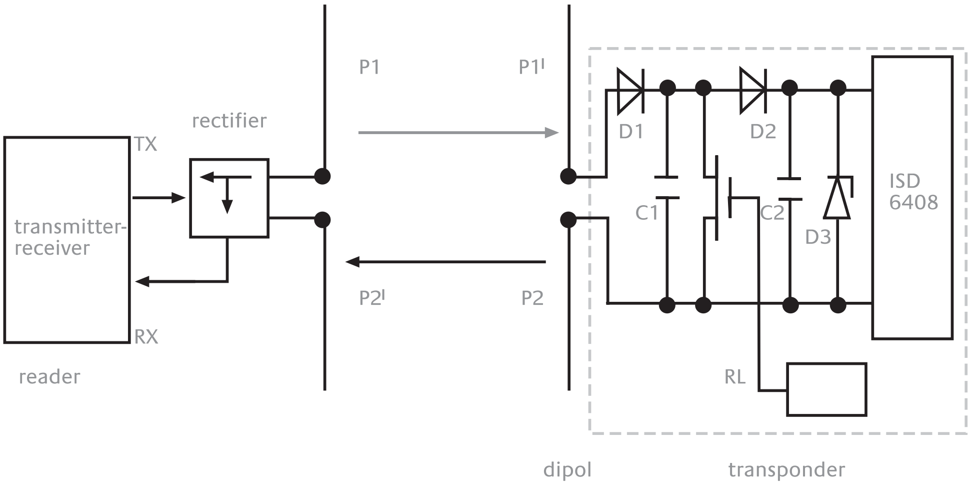


Figure 5-5: Principle of operation of backscatter transponder [Source: Fink 02]

Mode

Two basically different types of procedure are used to transmit data between the transponder and a reader duplex procedures including both full duplex (FDX) and half duplex (HDX) and sequential systems (SEQ). The full and half duplex procedures have in common that the energy transmission between reader and transponder is continuous, both in the uplink and in the downlink, independently of the data transmission. With sequential systems on the other hand the transponder is supplied with energy only in the pauses in data transmission between the tag and the reader.

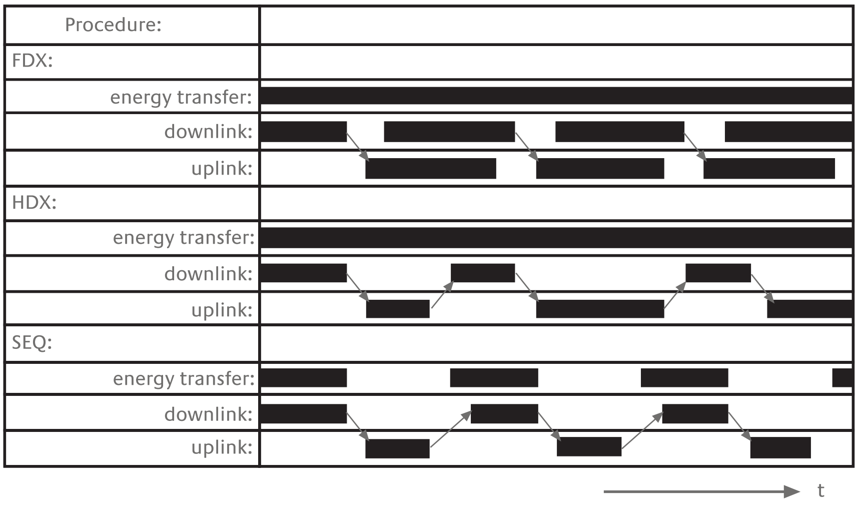


Figure 5-6: Chart showing temporal sequences in full duplex, half duplex and sequential systems. Transmission channel from reader to transponder is called downlink, reverse direction uplink [Source: Fink02]

5.2.4 Multiple access procedures and anti-collision procedures

General

A special challenge exists whenever more than one RFID tag is in the reader's range at the same time and each of them sends its identification number to the reader. Since all tags of a certain type transmit in the same frequency range, the signals overlay each other and the reader cannot identify any of the tags (collision). A reader must therefore have a selection procedure to ensure that the chips will send their information individually. In applications in which the presence of more than one RFID tag cannot be excluded, or in which that is even desirable (multiaccess), anticollision procedures are used.

The anticollision procedures used most commonly in RFID systems are based on the TDMA principle (Time Division Multiple Access). With this procedure, the entire transmission capacity available in the frequency channel is divided up among the individual tags sequentially (time multiplex). Transponder controlled procedures are relatively slow, since the reader has to repeat its request until all tags have been recognised with sufficient probability. With reader-controlled procedures on the other hand, the reader selects the individual tags one after the other in a rapid temporal sequence. In practice, the most successful transponder controlled procedure is called the Aloha procedure, and the most successful reader controlled procedure is called the tree-walking procedure.

The Aloha procedure

The transponder controlled Aloha procedure is based on a probabilistic querying of the identification numbers (ID numbers) of all tags in the reader's range. The reader transmits the exact same request command to all tags, telling them to identify themselves with their complete identification numbers. Each tag reacts to that with an individual random time lag and transmits its complete ID number. Since the data transmission of a tag is short compared with the duration of a request interval, only very seldom does a collision occur among a limited number of tags in the reader's range. By running through the request cycle multiple times all tags have a high probability of transmitting their ID numbers at least once without a collision. After a time (a matter of seconds), the reader will have recognised all the tags with a large probability. A few variations of this protocol have the reader switch off the recognised tags in order to reduce the probability of collisions in the successive request cycles. In this case, the ID numbers also have to be transmitted using the downlink and therefore could be heard by an eavesdropper from a greater distance. [Source: Vogt 02]

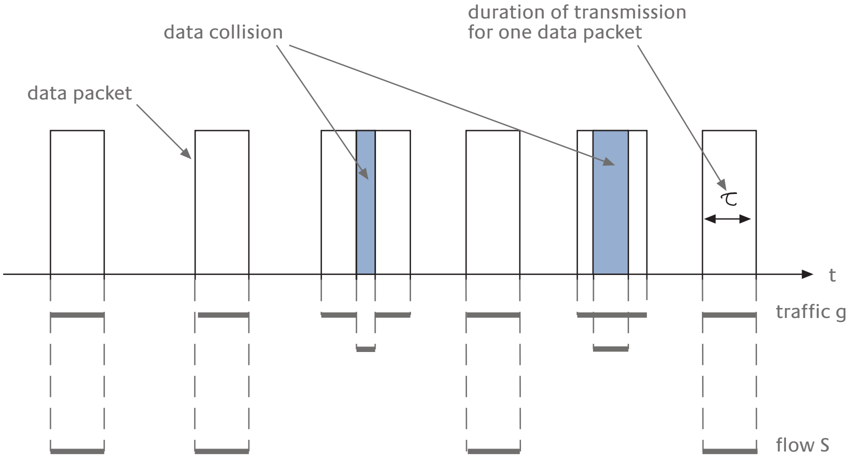


Figure 5-7: Definition of Traffic Volume G and Flow S in an Aloha system. 32. Several transponders transmit their data packets at random times. Sometimes there are data collisions and [Source: Fink 02]

Tree-walking procedure

Unlike the case with the Aloha procedure, tree-walking lets the reader actively control the selection of the tags. It carries out a deterministic search throughout the address space of possible identification numbers. The reader challenges all tags located in its range to transmit their IDs (REQUEST) beginning with the highest place of the ID number. If one assumes that the bit sequences received by the reader in the upper part of the ID number (higher value bits) often match, this procedure is relatively efficient. For example, the Electronic Product Code (EPC) proposed by the Auto-ID Center stipulates that the ID begins with the so-called “Company Prefix Index”, which is the same for all tags in many applications because it labels products from the same manufacturer. At the lowest place in the bit sequence, i, the ID numbers of the individual tags are different and a collision occurs (two tags send different bits at the same time on Place i).

Next the reader expands the query in that it selects a junction of the binary address tree at Place i and follows it next for a while. The reader only addresses such tags the IDs of which match the preselected prefix and the selected value at Place i. These tags answer with the rest of their IDs. Whenever further collisions occur at different places the process is repeated until only a single tag answers and no collision occurs any more. This tag can now be unequivocally selected by its ID number (SELECT) and read (READ_DATA). Afterwards, the active tag is switched off with the command UNSELECT.

Then the remaining tags are selected according to the same pattern starting with Place i of the first junction in the binary tree until finally all tags present in the reader’s range have been unequivocally addressed with their ID numbers. This procedure makes it possible to address individually a very large number of tags in the reader’s range.

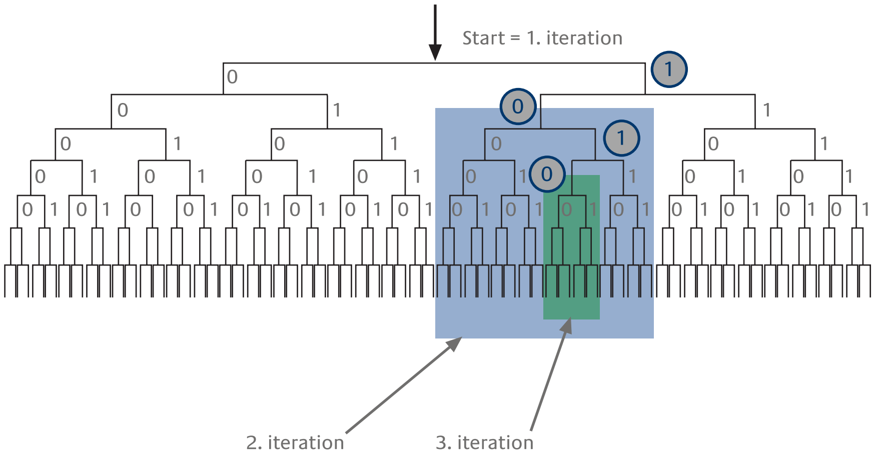


Figure 5-8: **Binary search tree. As search area gets smaller ultimately an individual transponder can be identified [Source: Fink 02]**

6. Classification of RFID systems

6.1 General

RFID systems can be classified according to their respective performance features. The groups obtained in this way can be broken down according to the performance of their respective components into low-end systems, medium-performance systems and high-end systems. Another classification scheme for RDID solutions is based on the respective range, meaning the maximum distance between transponder and reader. It usually distinguishes among close-coupling, remote coupling and long-range systems. The range is only regarded as a criterion independent of performance.

This classification scheme makes it possible to evaluate RFID systems according to the applications that can be based on them. Furthermore it makes possible an initial, survey-type evaluation of the questions connected with it having to do with information security and data protection.

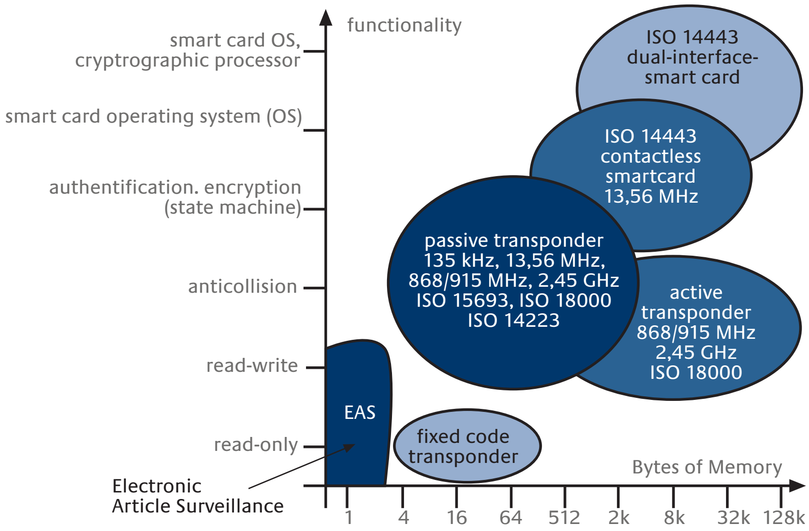

functionality
smart card OS, cryptrographic processor
smart card operating system (OS)
authentification. encryption (state machine)
anticollision
read-write
read-only
Electronic Article Surveillance
EAS
fixed code transponder
passive transponder 135 kHz, 13,56 MHz, 868/915 MHz, 2,45 GHz ISO 15693, ISO 18000 ISO 14223
active transponder 868/915 MHz 2,45 GHz ISO 18000
ISO 14443 contactless smartcard 13,56 MHz
ISO 14443 dual-interface-smart card
Bytes of Memory
1
4
16
64
512
2k
8k
32k
128k

Figure 6-1: Classification of RFID systems from low-end to high-end [Source: Fink 02]

6.2 Classification of RFID systems according to their performance

6.2.1 Low-end systems

One type of low-end system is comprised of so-called 1-bit systems, which have been used for many years now for simple surveillance or signal functions. These systems only indicate to a reader whether a transponder is present or not in its range. They do not have any integrated circuits and thus can be manufactured “for fractions of a cent”. For example 1-bit systems have been used for Electronic Article Surveillance (EAS) in retail operations for about 40 years.

A second type of low-end system is comprised of such RFID solutions that are not rewritable and thus can only offer data to be read. One does not need a microprocessor for this; these tasks can be carried out by a state machine. Encryption functions are typically not supported, so that any compatible reader can read the data on these transponders. Low-end systems are used mostly in the area of merchandise flows, identification of palettes, containers and gas cylinders and for animal identification.

One RFID product typical of low-end systems has been put on the market by Siemens. Their so-called MOBY R works in the 2.45 GHz range and overcomes a distance between transponder and reader of up to 300 meters. It has a 32-bit read-only code suitable for use in localization for example.

6.2.2 Medium-performance systems

The medium range of the performance spectrum is characterized by RFID systems with rewritable data memories (for example EEPROM in the case of passive, and SRAM in the case of active transponders) from z few bytes to over 100 Kbytes. IN this segment the variety of types is clearly the largest. Systems of medium performance may be equipped with either a state machine or a microprocessor. Usually anti-collision techniques are used in this class, in order to be able to selectively address more than one transponder in the view field of the reader. Medium performance systems can be equipped with authentification or cryptofunctions to protect them from eavesdropping.

For example, the Infineon my-d vicinity SRF 55V10P is equipped with a 10-Kbit-EEPROM in the range of 13.56 MHz and thus with a rewritable memory. Depending on antenna, the system gets ranges of up to 1.2 meters. It supports anti-collision and complies with ISO/IEC standard 15693 [cf. Infi 02].

6.2.3 High-end systems

In the high-end range there are mostly contact-less smart cards, each with a microprocessor and a smart card OS. The cards have more complex algorithms for authentication and encryption, which cannot be accomplished by a “hard-wired” state machine. The upper end of the high-end range is populated by dual-interface cards equipped with a cryptographic coprocessor. The working frequency typically lies around 13.56 MHz, the range below 15 centimeters (in the close-coupling or proximity range).

Such smart cards are used in areas with high security requirements such as electronic stock-exchange systems, ticketing and for payment functions.

Philips offers, for example, the SmartMX high-end system. The SmartMX complies with the ISO 14443 standard; it offers 72 kBytes of memory and ways to integrate further functionalities into the tag. It supports anti-collision. The data transmission rate can be as high as 848 Kbits/second. Asymmetric encryption techniques are supported with a cryptographic co-processor.

6.3 Classification of RFID systems according to their range

RFID systems can be subdivided into three categories by their ranges: close-coupling, remote coupling and long-range systems.

- Close-coupling systems have a range up to one centimeter. Close-coupling systems can work with almost any frequencies (from low frequency to 30 MHz), depending on the coupling used. If the coupling is inductive, the frequency usually lies between one MHz and ten MHz. The data transmission is done in close-coupling systems either through an inductive or through a capacitive coupling, the latter type being possible in cases of a very short distance between transponder and reader.
- Remote coupling systems have a range of up to about one meter. The typically work in the frequency range below 135 kHz and at 13.56 MHz. The coupling between the reader and transponder is done inductively. Remote coupling systems are subdivided into proximity cards (maximum 20 centimeters distance between the transponder and the reader) and vicinity cards (maximum one meter distance between the transponder and the reader).
- Long-range systems have ranges over 1.5 m to typically ten meters. In exceptional cases higher ranges are also possible: 100 meters or even 1 kilometer, as has been achieved in the frequency

spectrum around 5.8 GHz, which is currently in a very early developmental stage. The range of long-range systems is on the microwave scale, in the 868/915 MHz range and in the 2.45 GHz range. Long-range systems differ from the two systems described above through the energy supply of their transponders (active) and their data transmission techniques (backscatter).

6.4 The classification of the Auto-ID Center

The Auto-ID Center has specified the following classes of RFID tags:

• UHF	Cass 0	Auto 03]
• UHF	Class 1	Auto 02]
• HF	Cass 1	Auto 03b]

Transponders of the two UHF classes above work at a frequency between 860 MHz and 930 MHz according to the backscatter principle. Given a transmission power in the reader of four watts, a reading distance of up to seven meters is achieved. In Europe currently only 0.5 watts of transmitting power are allowed, making the reading distance much shorter. Both specifications provide for the tree-walking procedure as anticollision mechanism and support only read-only transponders. The specification also calls for a way to permanently deactivate a tag using a password protected “kill” command (see Section 7.7.6.1.). Complying tags are not allowed to respond in any way to signals from a reader after the kill function has been turned on.

UHF-Class-0 tags are written with the Electronic Product Code (EPC) during the production process and cannot be reprogrammed afterwards. UHF-Class-1 tags can be written once by the user with the EPC code, and they act as a WORM medium (write once read many). It is planned to combine the UHF classes into a single UHF-Class 1, Generation 2 [Source: RFID 03].

HF-Class-1 tags differ from the classes mentioned above in their frequency (13.56 MHz), and in the anti-collision mechanism used (the Aloha procedure). Apart from that, the same requirements are placed on transponders in this class as on those of UHF Class-1 tags. In particular a deactivation function (DESTROY command) is also planned for them.

7. Threat situation and inventory of common security measures

7.1 Overview

One of the goals of the present study is to investigate the future threat situation resulting from the application of RFID systems (within a time frame of three to five years), as well as to assess the effectiveness of security measures. The present Chapter describes the results of this phase of the work.

Sections 7.2 to 7.7 provide an overview of possible attacks and countermeasures. Section 7.8 contains an evaluation of the threat situation, especially with regard to the practicability and cost of the attacks and countermeasures. A list of the experts who were consulted regarding these matters can be found at the beginning of the study in the Section "Authors and Experts". Section 7.9 contains a brief description of the current availability of security measures.

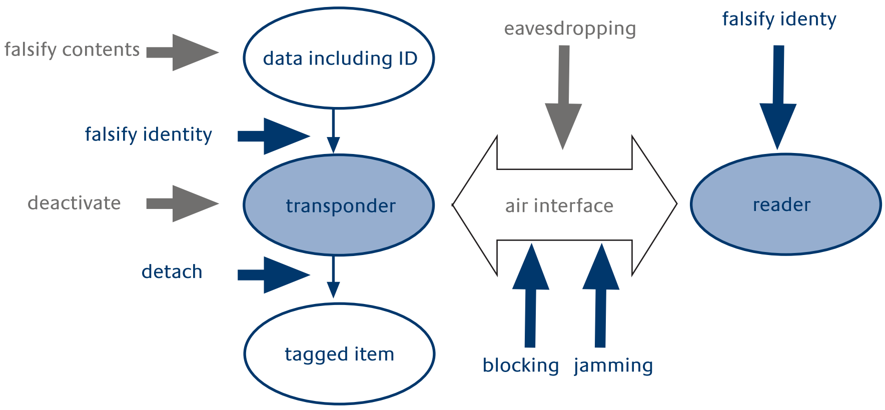


Figure 7-1: Basic types of attack on RFID systems

7.2 Basic types of attack

The purpose of RFID systems is to achieve better congruence between the virtual world of data and the world of real objects [Source: Flei 01]. It is therefore crucial for the integrity of RFID systems that three relationships are assured:

1. The relationship between the data stored on a transponder (tag) and the transponder itself. This must be a unique relation, because the transponder is identified solely by the data. The most important part of the data is a unique ID number (serial number). The identity may be additionally secured by storing keys or other security information on the transponder. It is imperative to prevent the existence of two tags bearing the same identity.
2. The relationship between the transponder and the tagged item which it is meant to identify (mechanical connection). This relation, too, must be unique in the sense that a transponder must never be assigned to different items while it is in use.
3. The relationship between transponder and reader (air interface). This relationship must be established in such a way that authorized readers can detect the presence of the transponder and can correctly access the data, while access by unauthorized readers is barred.

Figure 7-1 shows the basic types of attack resulting from these relationships, and they are explained in the following.

Falsification of contents

Data can be falsified by unauthorized write access to the tag. This type of attack is suitable for targetted 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 transponders 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.

Falsification of identity (transponder)

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 transponders with the same identity being in circulation.

Deactivation

This type of attack renders the transponder useless through the unauthorized application of delete commands or kill commands, or through physical destruction. 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.

Detaching the tag

A transponder 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.

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 [Source: FiKe 04].

Blocking

So-called blocker tags simulate to the reader the presence of any number of transponders, thereby blocking the reader. A blocker tag must be configured for the respective anti-collision protocol that is used.

Jamming

Data exchange via the air interface can be disrupted by passive means such as shielding or by active means (jamming transmitters). As the air interface is not very robust, even simple passive measures can be very effective.

Falsifying identity (reader)

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 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.

7.3 Types of attack according to their purpose

A person who attacks an RFID system may pursue various goals, which can be classified as follows:

1. Spying: The attacker gains unauthorized access to information.
2. Deception: The attacker deceives the operator or user of an RFID system by feeding in wrong information.
3. Denial of Service (DoS): The availability of functions of the RFID system is compromised.

4. Protection of privacy: Because the attacker believes that his privacy is threatened by the RFID system, he protects himself by attacking the system.

It is not possible to make a clear distinction between the various purposes. An attacker may, for example, spy out tag IDs in order to use them later with the intent to deceive. The types of attack listed above can now be assigned to their (primary) purposes (see Table 7-1).

It should be noted that in a typical context in which RFID systems are used, there are two parties with divergent interests [Source: HMM 04]. One the one hand, there is the operator of the RFID system, hereinafter referred to as the active party. The active party exercises control over the data of the RFID system and over the use to which the data are put. It is The operator is interested in the correct functioning of the RFID system. The passive party shares these interests only to the extent to which the advantages offered to him by the system outweigh the expected disadvantages. Consumer organizations in particular currently fear that RFID systems mean an additional threat to privacy. Some of the types of attack that have been mentioned, such as eavesdropping at the air interface, contribute to the potential threat, while others are capable of increasing privacy protection and of strengthening the passive party's means of exerting influence. The use of blocker tags is a case in point. An in-depth analysis of the interests of the parties participating in an RFID system, as well as of possible third parties, provides a necessary context for security strategies, but it cannot be performed in this study.

Henrici, Müller and Müller [Source: HMM 04] suggested an RFID framework which would operate without "destructive" elements such as blocker tags and which, according to the authors, would offer adequate privacy protection.

	Spying	Deception	Denial of Service	Protection of Privacy
Falsifying content		possible aim		
Falsifying identity (tag)		possible aim		
Deactivating		possible aim	possible aim	possible aim
Detaching		possible aim		possible aim
Eavesdropping	possible aim			
Blocken		possible aim	possible aim	possible aim
Jamming		possible aim	possible aim	possible aim
Falsifying identity (reader)	possible aim			

Table 7-2: Types of attack and their possible aims

7.4 Digression: Attack on the backend

A RFID system has to rely on the fact that the data which have been accessed by a reader are linked with other databases via additional communication channels. The security aspects in this so-called backend of the RFID system are not specific to RFID and therefore do not belong to the core topic of this study. Nevertheless, at the very least, let us provide an overview of conceivable attacks on the backend at this point, especially since it is feasible that, taking everything into account, the security risks are greater here than in the frontend area.

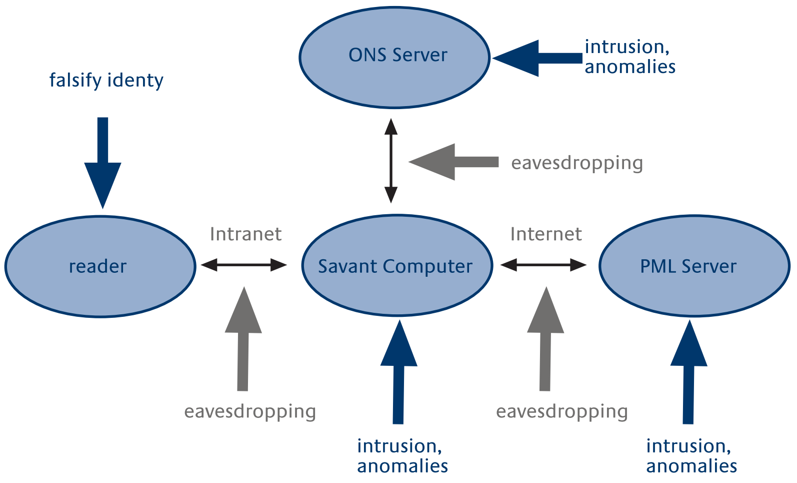


Figure 7-3: **Possible architecture of the backend of RFID systems and relevant types of attack**

Figure 7-2 shows a possible architecture for backend processing in an RFID system (based on the concept of EPCglobal, cf. [Source: EPC 04]). The reader is embedded in a network based on Savant software and uses a central Object Name Service (ONS). The Savant computer transmits every serial number that has been read to the ONS server and is given in return the address of a server which administers the data associated with it (PML server). The format used for these data is Physical Markup Language (PML).

In principle, all Intranet and Internet connections run the risk of being subject to eavesdropping, and all computers connected to the Internet are threatened by intrusion (hacking and cracking) and the introduction of software anomalies (mainly viruses and worms). This could also mean that the identity of a reader with authorized access to the backend might be falsified. However, as already mentioned, these are not security problems specifically linked to RFID, and they are therefore not dealt with in detail here. Attacks on the backend can be averted with the usual IT security procedures, which are easier to adapt to new requirements than is the case with security procedures implemented on the tags.

One must, however, remember that, for the very first time, thanks to RFID systems, large portions of the physical world can be represented in the virtual world in near-real time. Databases are being generated from which, in particular, movement profiles of objects and information derivable from them can be extracted which previously were not available in the same density. This means that the motivation of attackers as well as the potential extent of the damage following successful attacks could attain a new order of magnitude.

7.5 Threat to the active party

This Section examines the threat from the perspective of the active party, that is to say, the party that operates the RFID system.

In principle, the attacker could be the passive party (employees or customers), or it could be a third party (competitors, industrial spies, cyber-terrorists).

7.5.1 Spying out data

An attacker can spy out data in the following manner:

a) He can use his own receiver to eaves drop on the communication between tags and readers. In this case the distance could be greater than the standard reading distance (see Section 7.8.2).

b) He can use his own reader to read data from the tags. The device can be installed in a hidden place, or it can be used in a mobile manner. If the reader requires authentication, the attacker must be able to falsify the identity of the reader.

7.5.2 Feeding in false data (deception)

An attacker can carry out the following attacks for the purpose of deception:

c) He can change the contents but not the ID (serial number) of an existing tag. This is only possible if the data associated with the ID are stored on the tags themselves (and not in the backend), which for most applications is not necessary.

d) The attacker can emulate or duplicate tags (cloning) in order to trick the reader into accepting their identity. To achieve this, he must first find out at least the IDs (serial numbers) and, depending on the security procedures, also any passwords or keys.

e) The attacker can detach the tag from the tagged item in order to conceal the movements of the item from the reader, or to pass another item off as the original tagged item. Depending on the mechanical security measures in place, he will have to damage the tagged item to achieve his goal, which in many cases greatly diminishes the usefulness of the attack.

7.5.3 Denial of Service

An attacker has a large number of ways in which to impair the correct functioning of an RFID system and thus to undermine the congruence between the real and the virtual world which these systems seek to achieve:

f) Tags are destroyed by mechanical or chemical means (through bending, by applying pressure or tension loads, through the action of acid, etc.).

g) Tags are destroyed through the effect of electromagnetic fields, similar to the normal procedure for deactivating 1-bit transponders (theftproofing). In principle, this effect can be achieved by transmitters designed specifically for this purpose, but also by microwave ovens or powerful inductive sparks.

h) Tags are put out of action through the misuse of delete or kill commands. Such misuse presupposes the ability of the attacker to fake the identity of an authorized reading or writing device.

i) The battery of an active tag is discharged by a series of queries. This method does not work in the case of passive tags, because they derive their energy exclusively from the supply field provided by the reader.

j) A blocker tag simulates the presence of any number of tags to the reader in order to prevent the actually provided tags from being read.

k) Jamming transmitters prevent communication between reader and tag. In order to be effective over long distances, very powerful transmitters would be required. Such an attack would be easy to detect.

l) Reflecting objects are capable of cancelling an electromagnetic field.

m) The proximity of, for example, water, metal or ferrite leads to detuning of the field frequency.

n) Metal foils or bags fitted with metal strips shield the tags from electromagnetic fields.

Very little experience has been gathered so far on the practical execution of these attacks and the effectiveness of countermeasures. Some expert opinions are presented in Section 7.8.2.

7.6 Threat situation for the passive party

This Section describes the threat situation from the perspective of the passive party. This party might be, for example, a customer or an employee of the operator. The passive party uses tags or items that have been identified by tags, but the party has no control over the data which have been stored on the tags.

Any discussion on the risks posed to the passive party by RFID has so far been dominated by the topics of data protection or threats to privacy. In contrast, any other conceivable disadvantages, such as the technical risks being shifted from the active to the passive party, or the growing tendency to patronize the user [Source: cf. Hilt 04], are hardly ever discussed. At this point we simply want to mention the relevance of these questions. These aspects of the subject will be raised again in Chapter 10 when fictitious examples will be discussed.

Privacy can be threatened by the active party or by a third party. It is obvious that in the first case no attack on the RFID system is required, because the system is under the complete control of the active party. The active party might, for example, violate current data protection (privacy) legislation by passing on sensitive data without the knowledge of the persons involved.

In the second case, a third party attacks an RFID system in order to gain unauthorized access to data. The consequences for the passive party are very similar to those in the first case, as sensitive data get into the wrong hands without the knowledge and agreement of the persons concerned.

7.6.1 Threat to data privacy

Storing person-specific data in an RFID system can threaten the privacy of the passive party. We will deal here only with the RFID-specific aspects of the threat situation:

a) By eavesdropping on the air interface or by unauthorized reading of tags, a potential attacker has new methods at his disposal for gaining unauthorized access to data.

b) Apart from person-specific data, even potentially person-specific data could increasingly become the target of an attack. Although these data are anonymized or pseudonymized, the probability is high that they can be deanonymized later and therefore allow plausible conclusions to be drawn about individuals. With RFID, the temporal and spatial density of data traces left by individuals increases, thereby in purely statistical terms improving the chances of deanonymization.

c) The resulting high degree of congruence between the virtual and the real world, which is a declared goal of using RFID systems, may give rise to the urge on the part of active parties as well as third parties (e.g. also state regulatory bodies) to perform new evaluations which may not necessarily be in the interest of the passive parties. As the data become more easily accessible, the risk increases that databases will sooner or later be evaluated for purposes other than those originally intended, without the knowledge of the persons affected.

7.6.2 Threat to location privacy

Assuming that tags will remain in the possession of the same person over long periods of time, repeated reading of IDs (serial numbers) allows movement profiles (tracking) to be generated. This possibility becomes a threat to privacy, if and when RFID systems become a ubiquitous part of everyday life. Even if nothing but IDs are transmitted during the readout of RFID tags, while all other data are shifted to the backend, a threat to privacy can result. The more tags there are in circulation, the better the chances that tracking can be carried out. Tracking more than one person also allows contact profiles to be established.

Again, a specific characteristic of RFID is the possibility of eavesdropping on the air interface. On the other hand, the possibility cannot be excluded that attacks in the backend area pose a bigger threat to privacy than attacks at the air interface. Compared to the use of mobile telephones, the use of RFID tags generates more precise data traces, because not only the geographical location, but also the concrete interaction with existing firms and infrastructures can be determined.

7.7 Security precautions

7.7.1 Authentication

When authentication is carried out, the identity of a person or a program is checked. Then, on that basis, authorization takes place, i.e. rights, such as the right of access to data, are granted. In the case of RFID systems, it is particularly important for tags to be authenticated by the reader and vice-versa. In addition, readers must also authenticate themselves to the backend, but in this case there are no RFID-specific security problems.

7.7.1.1 Checking the Identity of the tag

When the RFID system detects a tag, it must check its identity in order to ascertain if the tag has the right to be part of the system at all. A worldwide and unambiguous regulation for issuing ID numbers, as proposed, for example, in the form of the Electronic Product Code (EPC), offers a certain amount of protection from falsified tags. At the very least, the appearance of numbers that were never issued or of duplicates (cloning) can be recognized in certain applications.

In addition, authentication may take place via the challenge-response system, in which the reader sends a random number or a time stamp to the tag (challenge) which the tag returns in encrypted form to the reader (response). The key used in this case is a jointly known secret by means of which the tag proves its identity. The decisive element in this procedure is the fact that the key itself is never transmitted and that a different random number is used for every challenge. As a result, the reader cannot be deceived by the communication being recorded and replayed (replay attack). This unilateral authentication procedure is defined as a "symmetric-key two-pass unilateral authentication protocol" in ISO Standard 9798.

An attacker would have to get hold of the key which is stored both on the tag and in the backend of the RFID system. In order to do so, it would be necessary to decode the response data that were transmitted in encrypted form, which is a very complex if not almost impossible task, depending on the length of the key. In principle, the key could also be read by physical means from the storage cells of the chip, but this would require very complicated laboratory methods, such as the "Focused Ion Beam" (FIB) technique. In this procedure, an ion beam removes very thin layers (a few layers of atoms) in separate steps so that the contents can be analysed microscopically.

A challenge-response method can also be used for the mutual authentication of reader and tag. In this case, the tag must also be capable of generating random numbers (see Section 7.7.1.3).

7.7.1.2 Checking the Identity of the reader

The simplest method of authenticating the reader in relation to the tag is to use password protection, i.e. the reader identifies itself to the tag by transmitting the password. The transponder compares this password with the password stored in memory. If both are identical, the tag grants full access to the stored data. Some products grant password protection for selected areas of memory.

In simple systems, all tags contain the same password in a protected area of their memories. In more sophisticated read-only systems every transponder is assigned an individual password by the manufacturer, which is then stored in its memory by means of a laser. Variable passwords are capable of providing better protection, but they only work with read-write transponders. The length of a typical password would be 8, 24 or 32 bits.

Password systems without encryption are regarded as a weak method of identification, because they allow eavesdropping on password transmission via the insecure air interface. In addition, short passwords can be cracked simply by systematic trial-and-error.

Password systems without encryption might be adequate in cases where the tag is addressed just once or where the danger of a password being discovered by spying is already low. If access is needed only a limited number of times, a list of once-only passwords stored in the transponder and in the back-end can also be used instead of a single password.

In contrast to cryptographic procedures, such password systems make few demands on the tags and can be implemented with simple read-only tags.

Improved security against unauthorized readouts is achieved by the hash-lock procedure. In this case, before a tag is written to for the first time, a so-called meta ID is generated from a key as a pseudonym for the tag. This is done with the aid of a hash function, the calculation of which is practically irreversible, and the meta ID is stored in the tag. From that moment on the tag is locked, that is to say, it reacts to the signals of a reader solely by transmitting the meta ID. To unlock the tag, the reader must retrieve from a backend database the key that belongs to the meta-ID and then transmit it to the tag. The tag applies the hash function to the key it has received and checks whether the result is identical with its meta ID. If this is the case, the reader is authenticated and the tag allows access to its data.

It would be almost impossible for an attacker to calculate back to the original key. Therefore in many practical deployment areas a meta ID is sufficient protection against unauthorized readout. However, during transmission via the air interface the secret key belonging to a meta ID can be spied out by an attacker who can later deceive the tag into recognizing a reader as authorized (replay attack). The hash procedure can be implemented for transponders even without using sophisticated cryptoprocessors [Source: Weis 03], so that this procedure can be used even for inexpensive transponders.

Maximum protection against unauthorized access to the tags is provided by authentication procedures with encryption according to the challenge-response principle (strong cryptographic procedures) mentioned above. However, these procedures presuppose that the tag can not only execute cryptographic algorithms but can also generate random numbers. In the case of tags which fulfill these requirements and can therefore check the authorization of the reader at a high security level, it is not worthwhile to make compromises when the reverse problem occurs (authentication of the tag to the reader), because the processing capacity of the reader or of the backend does not constitute a bottleneck. Consequently, in the case of high-performance transponders strong mutual authentication procedures are appropriate (see Section 7.7.1.3.).

7.7.1.3 Strong mutual authentication

ISO Standard 9798 defines various challenge-response procedures for strong authentication in the case of contact smart cards and RFID systems, including mutual authentication according to the “three-pass mutual authentication protocol”.

When a tag receives a "get challenge" command from a reader, it generates a random number A and sends it to the reader. The reader in turn generates a random number B and with it and the random number A generates an encrypted data block (token T) on the basis of an encryption algorithm and a secret key K. The data block is then returned to the tag. Since both sides use the same encryption algorithm and since the key K is stored on the tag, the tag is capable of decrypting the token T. If the original random number A and the random number A’, which has now been decrypted, are identical, this proves the authenticity of the reader. The procedure is now repeated in order to authenticate the tag to the reader. In this case, a second token S is generated in the tag and is transmitted to the reader. If the decrypted random numbers B and B’ are identical, then the authenticity of the tag vis-à-vis the reader has also been proved.

In this procedure no secret keys are ever transmitted via the insecure air interface. Instead only encrypted random numbers are used, which gives a high degree of protection against unauthorized access. Nor can recording and subsequently replaying the initializing sequence (replay attack) gain access to the tag or the reader.

Apart from the authentication procedures based on symmetrical cryptography, which are described here, procedures based on asymmetrical cryptography are also conceivable for use within RFID systems.

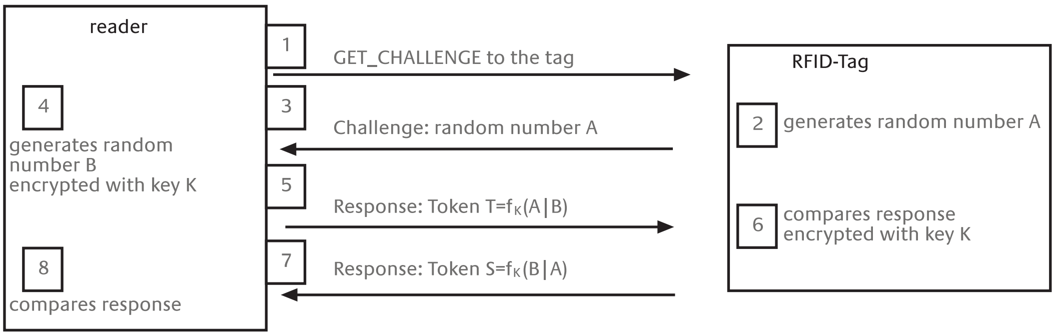

reader
1
GET_CHALLENGE to the tag
RFID-Tag
4
3
Challenge: random number A
2 generates random number A
generates random number B encrypted with key K
5
Response: Token T=f_K(A|B)
6 compares response encrypted with key K
8
7
Response: Token S=f_K(B|A)
compares response

Figure 7-4: Challenge-response procedure for mutual authentication [Source: FrSt 2004]

7.7.2 Encryption

Encryption of the data being transmitted is one method of protecting against anyone eavesdropping on communication via the air interface. Encryption is closely linked with authentication. If a transponder is designed for strong cryptographic procedures, not only strong mutual authentication but also secure encryption of the data that are subsequently transmitted can be achieved. In particular, the three-pass authentication procedure described above can be used to generate a joint temporary key (session key) from the random numbers of the initialization sequence to encrypt the data which will subsequently be transmitted.

If, however, the transponder does not support strong cryptographic procedures, only weak authentication is possible. For the same reasons, reliable encryption of subsequently transmitted data is then not possible either.

The most effective protective measure against an attack involving eavesdropping at the air interface is, however, not to store any contents on the tag itself and instead to read only the ID of the tag. The data associated with the tag are retrieved from a backend database. This measure, which is most often recommended in the technical literature and which is assumed by EPCglobal [EPC 04], offers the additional advantages that less expensive tags can be used, the memory for the associated data in the backend is practically unlimited, and the usual procedures for data management and IT security can be employed.

The problem of protecting the air interface against eavesdropping is thus limited to the authentication procedure and the transmitting of the ID number. The authentication problem is solved by applying the authentication procedures (see Section 7.7.1.), and eavesdropping to obtain the ID does not constitute a threat in many applications, for example in a production process. In the case of widespread applications, however, eavesdropping on the ID may threaten the location privacy of the persons carrying tagged items and may thus raise data protection problems. In such situations countermeasures such as eavesdropping-proof anti-collision protocols and pseudonymizing of the tags could offer a solution (see the following Sections).

For applications where relevant contents have to be stored on the tags themselves, only strong encryption procedures can provide reliable protection against eavesdropping.

7.7.3 Anti-collision protocols that are safe from eavesdropping

With anti-collision protocols based on a binary tree search (tree walking) (see Section 5.2.4), the ID numbers of the tags can be deduced from the signals of the reader, even from a considerable distance [Source: LLS 00]. For this reason, alternatives to the tree-walking procedure have been suggested which would preclude the extraction of ID numbers through eavesdropping on the downlink (data transmission from reader to tag).

Neither of the measures mentioned have any influence on the possibilities that exist for obtaining ID numbers through eavesdropping on the uplink (data transmission from tag to reader). Their usefulness is derived from the fact that, because of the low transmitting power of the passive transponder and because of the superimposition of the strong signals from the reader, the uplink can normally only be monitored at a shorter distance than the downlink. However, this evaluation is called into question by more recent investigations conducted by the BSI, at least for inductively coupled transponders in the 13.56 MHz range [Source: FiKe 04].

7.7.3.1 Silent tree-walking

This modification of the tree-walking procedure was suggested by Weis et al. [Source: WSRE 03]. Instead of actively "calling out" in clear text the next branch in the binary tree, the reader merely transmits to the tags in the reading field the request for them to transmit the next bits of their ID numbers. The reader interrogates the areas of corresponding bit sequences of all tags in descending order until a collision occurs at point i. At this point the reader branches off the query of the sub-trees by means of a SELECT command. Then, in contrast to normal tree walking, it is not the entire already known section of the address space that is transmitted, but rather an XOR value made up of the current bit at point i together with the preceding bit. The tags in turn form an XOR value out of this particular value and their own bit and compare the result with the next digit of their ID number. If there is a match, they are selected and transmit the next bit. An attacker operating from a distance, who can only eavesdrop on the downlink from the reader to the tag, does not find out the complete ID number. Those areas of the ID numbers where no collision occurs remain hidden to him, so that the attacker cannot find out the selected sub-tree, nor can he, by reversing the XOR function, ascertain the bit values transmitted by the reader.

In contrast to normal tree walking, this procedure cannot be implemented with read-only tags, because a dynamic memory is needed. This makes silent tree-walking more expensive than simple tree-walking.

7.7.3.2 Aloha procedure with temporary IDs

The specifications of the Auto ID Centre for Class 0 tags contain an alternative procedure to tree walking in which the ID numbers of the tags are not transmitted on the forward channel (downlink), which is subject to eavesdropping [Source: Auto 03]: Instead of identifying themselves with their ID numbers, the tags initially identify themselves with a random number which is newly generated in each reading cycle and serves as a temporary ID number. The reader uses this number in order to mute a recognized tag individually. After all the tags in the reading field have been recognized, their actual ID numbers are queried by transmitting the temporary ID. With this procedure, an attacker eavesdropping on the downlink can merely detect the random numbers used for temporary identification. As a precondition for this procedure, tags must have a random number generator and also possess a function for being muted.

7.7.4 Pseudonymization

Pseudonymization can mask the identity of a tag so that only authorized readers can find out the "true" identity of the tag. The hash-lock procedure described above (see 7.7.1.2.) is based on pseudonyms (meta IDs) being assigned. However, since a tag retains the same meta ID over its entire lifetime, this procedure does not offer any protection against the tracking of tags. The hash-lock procedure can thus contribute to the protection of data privacy but it does not help to improve location privacy. For this reason, several extensions of the hash-lock procedure have been suggested.

7.7.4.1 Randomized hash-lock

This procedure, proposed by Weis et al. [WSRE 03], is based on the dynamic generation of a new meta ID every time a readout event occurs. For this purpose, at every activation the tag generates a random number r which is hashed with the true ID number of the tag. The random number and the hash value h are transmitted to the reader by the tag. In order to calculate the true ID number of the tag, the operator of the reader must know all the ID numbers belonging to the application in question. The reader or its server now generates the hash values of all known ID numbers, using the random number generated by the tag, until a corresponding hash value is found. At that point the ID number of the tag has been found.

If there are a large number of tags, this procedure is not really practicable. But despite these limitations it is of interest for use with an RFID system, because it can be implemented with minimal cost. However, it presupposes that the tags have a random number generator.

7.7.4.2 Chained Hashes

Ohkubo et al. [Source: OSK 03] suggest the chained hash procedure as a cryptographically robust alternative. At every activation the tag calculates a new meta ID, using two different hash functions. First the current meta ID is hashed in order to generate a new meta ID which is then hashed again with the aid of the second function. It is this second meta ID that is transmitted to the reader. For the purpose of decoding, the reader must hash until a match with the meta ID transmitted from the tag has been found. The advantage of this procedure is that it is not sensitive to repeated attempts to spy out the meta ID during transmission via the air interface. An attacker would not be able to back calculate the meta IDs that have been spied out, with the result that the anonymity of all preceding database entries (log entries) of the tag in question is preserved.

7.7.4.3 Procedure by Henrici and Müller

Henrici and Müller [Source: HeMü 04] propose a procedure which makes possible the mutual authentication of tag and reader, as well as encryption of communication, and which also ensures the protection of "location privacy". In addition, no keys or other usable data are stored for any length of time on a tag, thus making physical attacks on the chip hardware uninteresting. The procedure gets by with a minimum exchange of information and is also resistant to interference on the transmission channel (air interface).

In order to ensure location privacy, the tag ID is changed regularly. The tag never discloses the current ID but only its hash value. The latter is calculated by the tag on the basis of in each case new transaction numbers which are synchronized with the back-end of the reader. These features prevent attacks such as replay attacks and detect information losses. Two entries per tag are stored in the backend database, because the possibility of losing the last message from the backend to the tag must be taken into account. The more complicated data management and synchronization in the backend area do not, however, represent any significant limitation, because sufficient resources exist here. By contrast, relatively modest demands are made regarding the hardware of the tag. The chip must be capable of calculating hash values, whereas a random number generator is not needed.

The scalability of the procedure makes it interesting for mass deployment. Assuming mass production, the authors of the procedure estimate the implementation costs at 0.5 euro cents per tag. This means that the procedure can be implemented economically even for low-end tags.

7.7.5 Preventing readout

In contrast to most other everyday electronic products, RFID tags do not have an on/off switch. Therefore they can be activated from outside at any time without the owner even noticing that this has happened.

So-called blocker tags were developed [Source: JRS 03] as a method of temporarily preventing the authorized or unauthorized reading of a tag.

7.7.5.1 Use of blocker tags

A blocker tag is a transponder or a piece of equipment with a high degree of functionality that pretends to be a transponder and simulates all possible ID numbers to a reader. By constantly replying to every demand by the reader to transmit data, a blocker tag makes it impossible to scan the tags that are simultaneously present in its environment. The tags that are actually present are effectively hidden within a mass of virtual tags (in practical terms, several billions of tags). Juels et al. have suggested equipping blocker tags with two aerials so that any prefix singulation can be answered simultaneously with 0 and 1. This kind of blocker tag can effectively block readers that function according to the binary tree procedure.

In order to prevent blocker tags from causing a complete blockage of all RFID applications in practice, procedures have been proposed which would allow blocker tags to block only certain areas of the ID address space [Source: JRS 03]. In this way protected address spaces can be set up where reading is blocked without other applications being impaired.

The reliability of passive blocker tags is poor. Since a passive blocker tag is activated through the energy of the electromagnetic field of the reader to be blocked, the reliability of the protection is restricted by the random spatial orientation, by shielding effects and by the distance between the blocker tag and the reader. In addition, the user is unable to ascertain that the blocker tag is functioning correctly.

Unwanted interference from desired RFID applications in the vicinity cannot be excluded and also cannot be directly detected.

7.7.6 Permanent deactivation

Permanent deactivation of a transponder at the end of its use phase is the most reliable method of protecting it from future misuse of any kind. On the other hand, permanent deactivation also prevents any advantages from being derived at a later date from RFID – e.g. in the case of smart labels the use of data for exchange, repair, reselling or recycling.

7.7.6.1 Kill command

A kill command enables the anonymization of transponders by making the readout of tags permanently impossible. This protects persons carrying tagged items from being surreptitiously identified and thus from being tracked.

A kill command was already included in the Auto ID specification [Source: Auto 02] published in 2002. The current EPCglobal specification of the Auto ID Center defines an 8-bit kill command protected by a password. According to the specification, once they have been deactivated by the password-protected kill command, conforming tags may no longer react to the signals of a reader [Source: Auto 03].

The procedures discussed so far are based on deactivation by software technology. This means that theoretically the future reactivation of a tag would be possible.

The kill command is being discussed as a possible means of deactivating smart labels on consumer goods at the point of sale. However, consumers are hardly able to check whether the labels have actually been permanently deactivated. From the point of view of data protection, the effectiveness of the kill command remains questionable, because kill procedures used up to now delete merely the variable memory cells in the transponder but not the unique ID number. In addition, deactivation by means of a password is not very practical if, after shopping, consumers must deactivate the tags one by one and manually.

7.7.6.2 Field-induced deactivation

Electromagnetic deactivation of the hardware via a predetermined rupture (burnout) point, as used in known anti-theft systems (1 bit transponders) would also be feasible but it is so far not being offered.

7.7.7 Transforming fair information practices into RFID protocols

Starting with the principles of "Fair Information Practices (FIP)" which are the basis of, among other things, the European Data Protection Directive 95/46/EC [Source: EC95], Flörkemeier et al. propose measures which are meant to create transparency regarding the operators of a reader and the use to which data are put [Source: FLS 04]. Proceeding from the assumption that current RFID protocols were optimized above all according to technical performance criteria and costs but not with regard to privacy protection, the proposals suggest modifications of current RFID protocols which would be easy to implement. Basic principles of FIP regarding purpose, limited usage, transparency and responsibility can be implemented through relatively minor changes in existing RFID protocols.

This also means that queries by readers must not remain anonymous but must show the unambiguous ID of the reader. If data protection principles are violated, the operator of the reader could then be identified and held responsible. Also, in each case the purpose of gathering the data should be communicated by the reader, for example a readout of serial numbers for marketing purposes. RFID transponders could be programmed in such a way that they only respond by giving their serial numbers when asked to provide the desired declaration of purpose, e.g. for payment.

The additional information about the operator of the reader and the purpose of the data gathering could be decrypted with the aid of a special display device and made visible to the owner of the tags. In this way, the user of the tags is to a certain degree given the chance of checking the function of the tags and of understanding the use to be made of the data that have been read out. The advantage of this procedure is that relatively minor additional effort is required in order to implement it in existing RFID systems. The transparency thus created could contribute to retaining or regaining the trust of the passive party.

7.8 Evaluation of the threat situation and discussion of the security measures

7.8.1 Overall evaluation

The experts were initially asked for their general estimate of how relevant security questions are in the case of RFID applications. The following points emerged:

- At the present time, any threat caused by attacks on RFID systems is very minor compared to the technical difficulties involved in using these systems in practice.
- The threat potential might increase if RFID systems were employed on a massive scale. Their widespread use might trigger temptations to attack the systems or to evaluate the information in a way that compromises privacy.
- Wherever RFID systems have repercussions on physical safety (hospitals, safety-critical spare parts, personal identification), IT security is of particular importance.

- On the whole, privacy is threatened less by attacks on RFID systems than by their normal operation.
- Opinions differ regarding the additional risks to privacy caused by RFID; they range from zero risk (everything is already possible using existing systems) to very high risk (tracking through RFID as a new kind of surveillance).
- Security measures increase not only the fixed costs but also the variable costs of RFID systems. In the case of security procedures, too, costs can only be reduced through high-volume use.

7.8.2 Evaluation of individual types of attack and discussion of countermeasures

The results of expert assessments have been collected in Table 7-2 and will be explained below. The attacks listed correspond to the attacks (a) to (n) described in Section 7.5. The costs that the attacker must incur as well as the costs that arise from countermeasures are essential elements in any evaluation of the mid- to long-term risks arising from the attacks. We can only make a qualitative estimate of these costs. The estimates given in Table 7-2 have been derived from the technical preconditions of the attack in question, or of the countermeasures. Countermeasures that are incorporated on the tag can often be cheaply implemented during large production runs. In this context, additional costs for security measures which are in the same order of magnitude as the costs for the system without additional security are designated as medium-range costs. High-cost countermeasures are those that cannot be implemented in practical terms without a generational change in technology.

Eavesdropping on the communication between the tag and the reader

Eavesdropping on the air interface is in principle possible. The risk increases with the maximum reading distance needed for the regular reading process. In the case of transponders with a very short range, the risk is small.

In the case of inductively coupled systems (below 135 kHz, 13.56 MHz) eavesdropping on the downlink is possible over a distance of up to several tens of meters, whereas the uplink can only be eavesdropped on over a much shorter range, namely approximately up to five times the maximum specified reading distance. These are theoretical estimates which are based on the relation between the transmitting power of the reader and of the tag. In their experiments, Finke and Kelter have shown that eavesdropping on the communications of RFID cards according to ISO 14443 (13.56 MHz, operating range 10 to 15 cm) is possible at a distance of up to at least two meters [Source: FiKe 04]. In that study by the BSI the difference between the transmission power of the reader and that of the tag proved to be not very important for eavesdropping purposes. It would be advisable to carry out more investigations regarding the possibilities and conditions for eavesdropping on inductively coupled tags.

In the case of backscatter systems (868 MHz and 2.45 GHz) eavesdropping on the downlink is possible up to a distance of 100 to 200 m, at a power output of 2 Watts; with the help of a directional aerial, this type of eavesdropping is possible up to a range of 500 to 1000 meters. The distances at which eavesdropping can be carried out on uplinks are shorter by two to three orders of magnitude and are therefore in the range of just a few meters. The fact that these data are so imprecise reflects the lack of reliable knowledge. Here, too, we are dealing with theoretical estimates which still need to be validated by systematic experiments.

In general, when eavesdropping occurs from a distance there is a problem in spatially allocating signals, because signals from different sources are superimposed on each other. This makes eavesdropping from a long distance even more difficult.

The costs for the attacker are high, since in every case professional equipment and know-how for decoding the data are needed. It should be remembered that building a normally functioning RFID system configuration is also not a trivial matter, because its reliability depends on a multitude of influencing factors (reflections, shielding, signal-to-noise-ratio, etc.). The conditions for an eavesdropping attack from a great distance would be even less favourable, especially at high bandwidths such as 106 – 848 Kbit/s in systems according to ISO 14443.

Countermeasures:

- Shift all data except the ID to the backend. This is also to be recommended for reasons of data management.
- Shield zones where readers are being used against electromagnetic radiation (metal foil wallpaper)
- Encode data transfer.

Under normal conditions, the costs for countermeasures need not be high in order to provide good protection against eavesdropping at the air interface.

Unauthorized reading of the data

This kind of attack requires a reader that can be deployed covertly, without being noticed. For the customary reading distance, this is feasible without incurring unreasonable costs. The attacker has to acquire a reader and possibly take the trouble of surreptitiously installing it. Software products are already being advertised which are used on mobile readers and are capable of reading and writing on simple tags, e.g. in supermarkets (Klaß 04).

The possibilities of such attacks are very limited due to the short range involved and can therefore be prevented in a controlled environment. Special manufacturing of readers with longer ranges is only possible within narrow physical limits and at great expense. In the case of inductively coupled systems, the range can be approximately doubled, but only with considerable effort. One meter is regarded as the definitive upper limit in the case of inductive coupling.

In the UHF range, transmitting power is limited by law to two Watts, which enables readers to operate at a maximum distance of three to five meters. In order to read at a distance of ten meters, a transmitting power of about 30 Watts would be needed, and for reading at a distance of 20 meters, as much as 500 Watts of transmitting power would be required. This is the kind of power put out by broadcast transmitters and would not be practical for a covert operation. Increasing the reading distance is also complicated by the fact that the weak signal of the tags is more and more "overwhelmed" by the stronger signal of the reader. For functional reasons alone, many RFID applications will use tags with very short reading distances, for example smart cards or banknotes.

Thus, the chances of surreptitiously reading passive transponders are spatially very limited. The situation is totally different where active transponders are concerned, but most of the time it is not necessary to use active tags for identification purposes (a typical application is finding the location of objects). As a result, these applications normally do not come under the RFID category.

Countermeasures:

- Shift the data to the backend
- Detectors which recognize the power field of the reader
- Authentication: Various methods of authenticating the reader with respect to the tag are conceivable (e.g. according to ISO 9798. see Section 7.7.1.).

The costs of the countermeasures may be low, if the desired goal can be achieved by using only a few detectors. A weaker variant could also be to conduct a random search for readers. Authentication would raise the unit price of tags significantly in cases where otherwise simple read-only tags would be sufficient. According to expert estimates it can be expected that mass-produced tags using the challenge-response procedure will remain three to five times more expensive than the simplest tags.

According to Infineon, however, the price difference should not be greater than 20 per cent.

Unauthorized modification of data

In the case of re-writable tags the possibilities for unauthorized modification of the data as well as the countermeasures are the same as those in the case of unauthorized readout (see above).

If, on the other hand, read-only tags are used, unauthorized modification of the data is intrinsically impossible. This must be weighed against other security disadvantages of the read-only tags, which do not permit any encryption and at best allow only weak authentication (password without protection against replay attacks).

Cloning and emulation

In the case of cloning, the data content of a tag is read out or discovered in some other way in order to write a new tag with the data. This tag is then used to simulate the identity of the original tag.

In addition, it is conceivable to employ devices having a high degree of functionality which are used to emulate any kind of tag with a given data content. Such an emulator could be relatively small (although larger than the tags). If it is possible each time to bring the emulator manually close to the reader, highly flexible means of falsification become available: Someone removes an item from a stream of products; its tag is read using a portable reader (which may also be integrated into the emulator); next, the person goes to the intended reader where, with the help of the emulator, he unobtrusively simulates that the item has passed this point.

A duplicated tag could be used in similar fashion, for example by taking an item off a "smart shelf" and replacing it with the duplicate, so that the intended theft protection does not take effect.

Because cloning and emulating require prior readout or eavesdropping, the countermeasures are the same as those used against these attacks (see above). Both types of attack must be prevented in order to exclude the possibility of cloning and emulation taking place.

Another countermeasure could take the form of plausibility checks in the backend which detect duplicates (e.g. because these crop up at different locations).

Detaching the tag from the tagged item

This attack appears trivial, but that is precisely why it should also be borne in mind. Each RFID system depends on the tags being present on the intended items. "Switching" tags (as is also done nowadays with price labels) with fraudulent intent or merely with the intention of creating confusion is an obvious manipulation.

The mechanical manipulation does not involve any special requirements and therefore tends to be cheap to perform.

Countermeasures:

- A tight mechanical bond between the tag and the tagged item ensures that removing the tag will also damage the product (e.g. when the tag is woven into textiles or embedded in plastic parts).
- In some applications, tags can be fitted in such a way that they are difficult to find or are inaccessible.
- In the case of active tags, an alarm function is also conceivable: A sensor determines that the transponder has been manipulated. It stores this information and transmits an alarm to a reader as soon as one comes within range.
- Where tagged items which have a high value or some sort of security relevance are concerned, additional features (e.g. a barcode or an inconspicuous mark) may be provided on the item so that, if neces sary, a manual check can be performed to see whether the tag is attached to the cor rect item. The correlation between the additional features and the tag ID is stored in the backend.

Mechanical or chemical destruction

RFID tags can be mechanically or chemically damaged. The antennae in particular are vulnerable.

Countermeasures:

- A close mechanical connection between the tag and the tagged item may also help to make it difficult to destroy the tag with out damaging the item.
- In some applications, tags may be atta ched in such a way that they are difficult to find or are inaccessible.

Destruction by exposure to an electro-magnetic field

Destruction by exposure to an electromagnetic field is standard practice in the case of anti-theft EAS tags (1-bit transponders) which are deactivated at the point of sale. Although the deactivation could be carried out with relatively simple means also by the customer while in the store, this does not seem to happen in practice.

This type of deactivation is fundamentally possible in the case of all inductively coupled tags, even when no predetermined rupture (burnout) point is provided, as in the case of EAS. Normally, Zener diodes or internal stabilizing circuitry limit the voltage that is induced in the antenna to the intended operating voltage. However, if the voltage induced in the coil exceeds the load limit of the voltage stabilizing system, the chip may be irreversibly destroyed. Only limited protection is possible against over-voltages because the ability of the stabilizing circuitry to absorb excess energy through its surface (heat removal) is limited in the chip. In general, a field strength of at least 12 A/m is required.

Because of the high field strength that is required, this attack can only be carried out at very close range. The same holds true for UHF tags.

Because the field strength decreases with the cube of distance, a transmitter with a very large antenna and a very high power output (broadcast transmitter) would be needed for the mass destruction of tags at several meters distance. This would be scarcely practical for an attacker to accomplish.

In principle, tags could be destroyed with a microwave oven, but not reliably so. If the tag is closely connected to the item bearing it (and that is a good reason for destroying it in a microwave oven) the severe heating of the tag might damage the product.

In addition, there is good reason to suspect that induction coils and high voltage switching events occurring in the near vicinity would induce sufficiently high voltage peaks in the tag to damage the chip. Experiments on this topic are at present being conducted at the EMPA.

Self-healing fuses might be considered as a possible countermeasure against the destructive effect of an electromagnetic field. So far, these have not been included in the standards. However, this countermeasure would not alter the fact that the capacity to absorb superfluously induced energy is limited by the surface area over which the heat can be given off. Therefore, in principle, there is no absolute protection against destruction by exposure to an electromagnetic field.

Destruction by misuse of a kill command

If, for data privacy reasons, tags are equipped with a kill function that partially or totally erases the data content, this function can be misused.

One countermeasure is to provide authentication for the kill command (e.g. password protection). Relatively complicated organizational measures are required in order to communicate the password to authorized persons (e.g. the purchaser of the item bearing the tag), but to keep it secret from others. This procedure is comparable to issuing a chip card with a PIN.

Discharging the battery (only in the case of active tags)

In the case of active tags which have a back-up battery, the latter can be discharged by causing the tag to transmit frequently in response to a rapid sequence of queries.

A possible countermeasure in this case would be a "sleep mode" which forces a pause after an interaction has occurred. This would limit the number of possible interactions per unit of time. Similar functions exist already to prevent duplicate readouts.

Blocking

In contrast to the use of jamming transmitters, the use of blocker tags is not forbidden by law, because due to their passive design they are not transmitting systems. However, their use could be forbidden in the standard business conditions, e.g. of supermarkets. But this would not prevent blocking for the purpose of committing fraud.

One advantage of blocker tags is in principle the fact that their jamming range is scalable and they can be configured for certain address spaces. As a result, privacy protection can be selectively adjusted.

However, it is precisely these individual adjustments that permit people to be tracked, so that the actual goal of ensuring location privacy becomes absurd.

The blocker chip available on the market from RSA is effective only in the tree-walking anti-collision procedure. However, blocker tags may also be developed against the Aloha protocol. In principle, there is no absolute protection against blocking within a given protocol. Since various protocols are in use, the user of the blocker tag must either carry several such tags with him in order to cover all the possible protocols, or he must use a single (slightly larger) blocker device that copes with all the protocols.

The only countermeasure against blocker tags is to ban their use in the standard terms and conditions of business – there are no technical countermeasures that can be taken.

Jamming transmitters

Effective interference of operation at a distance calls for powerful transmitters. Operating such jamming transmitters is illegal and it is difficult for technically inexperienced persons to obtain them: But radio amateurs do have access to this technology.

Close-range jamming is possible using weaker transmitters or also through interactions with other electronic devices (interferences, protocol collisions), but it is difficult to employ such effects reliably in a targetted manner.

Countermeasures:

- Detect jamming transmitters by performing random measurements or by using permanently installed field detectors.
- Adopt a frequency division (duplex) method (as in Bluetooth) in future generations of RFID. This admittedly very far-reaching measure would also control the increasing problem posed by normal jamming sources.

Field cancellation

Cancellation zones are a normal phenomenon in the UHF range, but are difficult to model. Therefore it seems unlikely that an attacker will succeed in using this effect in a targetted manner, e.g. by setting up reflectors.

There are no general and preventive countermeasures. If targetted field cancellation does, however, become an element of attacks, it will be necessary to find countermeasures tailored to each individual case.

Frequency detuning

This attack is carried out by bringing relevant amounts of, for example, water, metal or ferrite into close proximity of the field or the tag antenna. It might even be enough simply to cover the tag with the hand. However, frequency detuning is less reliable in its effect than shielding and no less obvious.

In principle, it is feasible to counter this type of attack by employing active frequency control. However, the technical effort required seems disproportionate because other, easier forms of attack, such as shielding, are not prevented by this measure. In addition, under certain circumstances, the high frequency licensing requirements for such systems would be infringed.

Shielding

Tags can be shielded by wrapping them in metal foil (e.g. aluminium foil) or by placing them in aluminium-coated freezer bags, or in handbags equipped with metal strips.

As a countermeasure, it is possible in the case of inductively coupled systems to use improved reading stations which are less sensitive to shielding. In particular, several antennae at different angles can make shielding difficult. There is no reliable protection against shielding.

Attack	Cost	Countermeasures	Cost

Eavesdropping on communication between tag and reader	high	Shift data to the backend Shielding Encoding	medium
Unauthorized reading of data	medium to high	Detectors Authentication	medium
Unauthorized modification of data	medium to high	Read-only tags Detectors Authentication	low to medium
Cloning and emulation	medium	Recognizing duplicates Authentication	medium
Detaching the tag from the tagged item	low	Mechanical connection Alarm function (active tags) Additional features	low to mittel
Mechanical or chemical destruction	low	Mechanical connection	gering to medium
Destruction through field effect	medium	Self-healing fuse (only limited effectiveness)	low when series-produced
Destruction through misuse of a kill command	medium	Authentication	medium
Discharging of battery (only active tags)	medium	Sleep mode	low when series-produced
Blocker tag	low	Banned in standard business conditions	low
Jamming transmitter	medium to high	Measurements, Frequency Division (Duplex) (FDD)	medium to high
Cancellation of fields	low (but difficult)	none	-
Field detuning	very low	Active frequency control	medium to high
Shielding	very low	Improved reading stations (only limited effectiveness)	medium

Table 7-1: Attacks on RFID systems and the respective countermeasures

7.8.3 Assessment of the privacy threat and a discussion of the counter measures

The results of the expert assessment are compiled in Table 7-3 and will be discussed below. Where the expert opinions diverge, the various standpoints are described in the text.

The general relevance of RFID in terms of the threat posed to privacy or data protection is a controversial topic. Some of the experts whom we asked do not see that there is any such relevance. Their reason for saying so is that, even without RFID, a very large number of data traces are already being generated by credit card payments, mobile telephone calls and customer cards. RFID would not add anything of significance to these databases, which even today are scarcely used.

Other experts see an RFID-specific privacy threat in particular in the possible future ways of tracking people, and they categorize this as a relevant risk of this technology, especially when the tags end up in the possession of the consumer. In many cases the latter will have to weigh up the opportunities and risks, because the more sophisticated and data-intensive future applications such as "Supply Chain Recording" or "Product Life Time Recording" might be of relevant use to him – for example, as regards the transparency of the supply chain (origin, social and ecological aspects) as well as in the case of leasing, maintenance, repair, resale or recycling.

Eavesdropping on communication between tag and reader

This is an attack that threatens the active and passive party in the same way.

The countermeasures are therefore essentially identical (cf. Section 7.4.2):

- Shift the data into the backend
- Shielding
- Encryption of the data transmission

These measures should, however, be implemented in such a way that the passive party has authorized access to the data that concern it. Otherwise, shifting the data to the backend or encryption would reduce the transparency of the system for the passive party, which would be contrary to that party’s need to have control over its own data.

The expense incurred for these security measures is considerably increased by the need to administer access rights.

A further countermeasure may take the form of the passive party protecting itself by (legitimately or illegitimately) attacking the RFID system, as was described in Section 7.3.2.

Unauthorized readout of data

Here again, this is an attack that threatens both the active and the passive party in the same way.

Countermeasures:

- Detectors that display the energy supply field of a reader may also be used by the passive party.
- If authentication procedures are used, the passive party should be given the access rights to the data that concern it. Otherwise the authentication procedures would reduce the transparency of the system for the passive party, and that is contrary to that party’s need to have control over its own data. The expense incurred for this security measure is considerably increased by the need to administer access rights.

A further countermeasure here, too, may take the form of the passive party protecting itself by (legitimately or illegitimately) attacking the RFID system, as was described in Section 7.3.2.

Tracking of people

Opinions vary on the risk that persons might be tracked by RFID.

Here is consensus that tracking using covert reading processes (eavesdropping, unauthorized readout) is rather unlikely and it is more probable that regular data capture will form the basis for establishing movement profiles. This view is justified by pointing out, among other things, the technical difficulty of performing covert readouts (see Section 7.3.2).

However, opinions differ on the contribution made by RFID to the risk of people being tracked.

On the one hand it is argued that data that would permit such tracking are already being collected today (e.g. through customer cards), but they are not being used for this purpose. No RFID applications which would contribute anything decisive in this area are being planned, nor would they be practical. In particular, no firm is currently considering collecting RFID data outside the logistics chain. Hypothetical applications such as auto-checkout in the supermarket will not be used on a large scale in the next 10 years. The costs of a tag (>5 euro cents) and technical difficulties at the physical level prevent tags from being profitably used for this application. Nor would enterprises wish to jeopardize their reputation and the trust of their customers. The aim of the present rationalization efforts is solely to optimize the supply chain all the way through to the shelf in the store (smart shelf). And even then, RFID labels will probably only be used on individual high-value products, whereas in most cases the labels will be used simply on the delivery package (e.g. pallet). This does not give rise to any additional risk of people being tracked through goods. Even if one wanted to use RFID for tracking purposes, it would be very difficult to derive movement profiles from the extremely fragmented data. It would be enormously expensive to generate an overall picture. There is no economic interest in doing so. Even the data captured currently by customer cards for the most part turn into data graveyards because it is not worth drawing up customer profiles.

On the other hand it is pointed out that if RFID is used on a widespread basis, significantly more events (even if not every purchase of a cheap mass product) will be digitally recorded, and more data traces will be generated that also offer more opportunities for evaluation. This will create new desires, e.g. in government agencies, to perform the evaluations. In addition, retailers are interested in the movement profiles of customers within their stores. Covert readout will remain the exception, but it cannot be completely ruled out. If RFID tags are not definitively deactivated when products are discarded, It might be possible to draw conclusions about the point and time of sale and also about the purchaser of the product by reading data from the tags in the garbage. One particular property of RFID compared with other identification systems is that this technology has the potential to limit the otherwise anonymous nature of the waste disposal process. Furthermore, storing biometric characteristics on transponders is an especially delicate matter.

One possible countermeasure would be to use variable ID numbers, e.g. based on the extended hash-lock procedure (see Section 7.7.4).

Threat	Countermeasure
Eavesdropping on communication between tag and reader	Shift into backend with authorized access by the passive party Shielding Encryption with authorized access by the passive party Attacks for self-protection (see Table 7-2): Detach the tag Destroy the tag Blocker tag Jamming transmitter Field cancellation Field detuning Shielding
Unauthorized readout of data	Detectors in the possession of the passive party Authentication with authorized access by the passive party Attacks for self-protection (see Table 7-2): Detach the tag Destroy the tag Blocker tag Jamming transmitter Field cancellation Field detuning Shielding
Tracking of people	Variable ID numbers Attacks for self-protection (see Table 7-2): Detach the tag Destroy the tag

Threat	Countermeasure
	Blocker tag Jamming transmitter Field cancellation Field detuning Shielding
Manipulation of data to the disadvantage of the passive party	Authentication with authorized access by the passive party Detection of duplicates
Improper evaluation of the data	No technical countermeasures

Table 7-2: Privacy threats due to RFID systems, and corresponding countermeasures

Manipulation of data to the disadvantage of the passive party

Not only unauthorized reading, but any type of manipulation of the data by a third party may be a threat to the passive party, particularly if initially the latter has no means of monitoring such manipulation.

Adequately secure authentication procedures are needed in order generally to prevent third parties from being able to access the data. In order to prevent manipulation, it is especially important for the passive parties themselves to have authorized access to the data that concern them, in order to be able to verify that they are correct.

In this case, also, legitimate or illegitimate self-protective attacks on the RFID system by the passive party, as described in Section 7.3.2, could be regarded as an additional countermeasure.

7.9 Availability of the security measures

Table 7-4 lists the transponder products supplied by the major manufacturers. For the purpose of compiling the Table, the transponders were classified as follows on the basis of the manufacturers' data sheets:auf der Basis von Datenblättern der Hersteller wie folgt klassifiziert:

Type1: Low end (ID label with state machine)

Type2: Medium-performance systems

Type3: end (Smart card with microprocessor)

The Table makes no claim to completeness. Nor can it be guaranteed that the technology listed is up to date, because the market is changing rapidly.

At the time when this study went to the press, it did not appear that any transponders with a kill function or any mid-range transponders capable of calculating hash functions without a cryptoprocessor were available on the market.

Name	Standard	Type	Storage capacity	Frequency	Password	Authenti-cation	Encryp-tion
Atmel							
AT88SC0104CRF	ISO 14443 Type B	3	1 Kbit	13,56 MHz		•	•
AT88SC0204CRF	ISO 14443 Type B	3	2 Kbit	13,56 MHz		•	•
AT88SC0404CRF	ISO 14443 Type B	3	4 Kbit	13,56 MHz		•	•
AT88SC0808CRF	ISO 14443 Type B	3	8 Kbit	13,56 MHz		•	•
AT88SC1616CRF	ISO 14443 Type B	3	16 Kbit	13,56 MHz		•	•
AT88SC3216CRF	ISO 14443 Type B	3	32 Kbit	13,56 MHz		•	•
AT88SC6416CRF	ISO 14443 Type B	3	64 Kbit	13,56 MHz		•	•
AT88RF001	ISO 14443-2 Type B	2	256 bit	13,56 MHz	•		
AT88RF020	ISO 14443-2 Type B	2	2 Kbit	13,56 MHz	•		
T5552	ISO 11748 / 785	2	992 bit	125 kHz			
T5557		1	330 bit	125 kHz	•	•	•
T5554		1	224 Kbit	125 kHz	•		
TK5561A-PP		2	128 Kbit	125 kHz			
EM Microelectronic							
EM4469/4569	ISO 11785,11785	2	512 OTP Option	125 kHz	•		
EM4450/4550	ISO 15693, 18000-3	1	1024 bit	125 kHz	•	•	•
EM4055	ISO 15693, 18000-3	1	1024 bit	125 kHz	•	•	
EM4056	ISO 15693, 18000-3	1	2048 bit	125 kHz	•		
EM4170		2	256 bit	125 kHz	•		
EM4034		1	448 bit	13,56 MHz			
EM4035		2	3200 bit	13,56 MHz			
EM4135		1	2304 bit	13,56 MHz			

Name	Standard	Type	Storage capacity	Frequency	Password	Authentication	Encryp-tion
Infineon							
SLE 66CL160S	ISO7816+14443 A+B	3	16 Kbyte + 1,3k RAM	13,56 MHz			•
SLE 66CL80P	ISO7816+14443 A+B	3	8 Kbyte + 2,3k RAM	13,56 MHz	•	•	•
SLE 66CLX320	ISO7816+14443 A+B	3	32 Kbyte + 5k RAM	13,56 MHz	•	•	•
SRF 55V02P	ISO15693	3	256 byte + 32 byte Admin	13,56 MHz		•	•
SRF 55V10P	ISO15693	3	1024 byte + 256 byte Admin	13,56 MHz		•	•
SRF 55V02S	ISO15693	3	256 Byte + 64 Byte Admin	13,56 MHz		•	•
SRF 55V10S	ISO15693	3	1024 Byte + 256Byte Admin	13,56 MHz		•	•
SLE 55R01	ISO 14443 A	3	128 byte + 32Byte Admin.	13,56 MHz		•	•
SLE 55R04	ISO 14443 A	3	616 Byte + 154 Byte Admin	13,56 MHz		•	•
SLE 55R08	ISO 14443 A	3	1024 Byte + 256 Byte Admin.	13,56 MHz			
SLE 55R16	ISO 14443 A	3	2048 Byte + 256 Byte Admin	13,56 MHz			
SLE44R35T	ISO 14443 A	3	1024 Byte + 256 Byte Admin	13,56 MHz			
SLE44R35S	ISO 14443 A	3	1024 Byte + 256 Byte Admin	13,56 MHz			
Philips							
HT1DC20S30	ISO 11785	2	2048 bits	125 kHz		•	•
HT2DC20S20	ISO 10536.1	2	256 bits	125 kHz	•	•	•
HT2MOA3S20	ISO 14443 A	2	256 bits	125 kHz	•	•	•
PCF793XAS	ISO 14443 A	2	128 – 768 bits	125 kHz		•	•
Mifare MFO IC U1X	ISO 14443 A	3	64 Byte	13,56 MHz		•	•
Mifare MF1 IC S50	ISO 14443 A	3	1024 Byte	13,56 MHz		•	•
Mifare MF1 IC S 70	ISO7816 / 14443 A	3	4096 Byte	13,56 MHz		•	•

Name	Standard	Type	Storage capacity	Frequency	Password	Authenti-cation	Encryp-tion
Mifare MF3 IC D40	ISO7816 / 14443	3	4096 Byte	13,56 MHz		•	•
Mifare ProX P8RF6X	ISO7816 / 14443	3	4 – 16 KByte	13,56 MHz		•	•
SmartMX P5Sxxxx		3	10 – 72 KByte	13,56 MHz		•	•
SmartMX P5Cxxx		3	10 – 72 KByte	13,56 MHz		•	
Texas Instruments							
RI-TH1-CB2A	ISO15693	3	2 Kbit	13,56 MHz			•
RI-TRP-B9WK-xx	-	2	88 bits	134.2 kHz	•	•	•
RI-TRP-V9WK		2	50 Byte	134.2 kHz	•	•	•
RI-TRP-BRHP-xx		2	88 bits	134.2 kHz			•
TMS37122		3	-	125 kHz			•

Table 7-3: Availability of security functions such as password protection,further authenification and encryption on RFID transponders

Table 7-4: Availability of security functions such as password protection,further authenification and encryption on RFID transponders

8. Areas of RFID Application

8.1 Overview of application areas

Accelerated by technical developments and the associated gains in performance levels, particularly due to falling costs in processor manufacturing, RFID now plays an influential role in many of today's applications and has also created a platform for new applications in the future. Potential application of RFID systems can be identified in practically all business sectors and the spectrum of application areas under discussion is constantly growing. Widespread use of the technology has previously been dampened by its relatively high implementation costs. These include the costs of hardware procurement, additional software components and – often neglected – expenditures for the organizational adjustment to new or modified business processes. [Source: Prog 04]

An intense discussion of RFID systems is currently underway in the retail sector. The commercial companies Metro Group, Wal-Mart and Tesco were among the first players to have adopted and implemented advanced RFID technology. Pilot projects have particularly focused on the potential of RFID systems for lowering costs and optimizing business processes. A study conducted by A.T. Kearney estimates that retailers can lower their warehousing costs by up to five percent and their labor costs by up to ten percent by employing RFID technology. For the German retail trade, this corresponds to an annual figure of approximately six billion euro. [Source: ATKe 04] In addition to retailers, logisticians also anticipate an increase in the economic advantages offered by RFID in the further automation and optimization of their business processes.

Current market data and reports on the use of RFID systems are frequently selective, relate merely to individual economic sectors and fail to provide a comprehensive survey of the market. There exist no conclusive official statistics but instead only market analyses conducted by various consulting agencies. The databases, surveying methods and market ranges employed are quite varied, not always transparent and thus not comparable to one another. Consequently, the current state of RFID diffusion, sales and market shares remains vague from a national as well as international viewpoint. Over the course of recent years, RFID technology has successfully occupied certain niche markets. Its future use as a mass market technology depends not least on the success of ongoing pilot projects conducted by pioneer users.

RFID technology is a typical cross-section technology whose potential application can be found in practically all areas of daily life and business. In principle, it functions as a means for identifying objects. From a cross-industry viewpoint, the following areas of applications can be distinguished:

- identification of objects
- document authentication
- maintenance and repair, recall campaigns
- theft-protection and stop-loss strategies
- access authorization and routing control
- environmental monitoring and sensor technology
- supply chain management: automation, process control and optimization

In the following, the status quo of RFID technology use will be shown on the basis of the above constellation of cross-industry applications. No application-based treatment will be made of the risks and threats posed by RFID systems, which would go beyond the scope of the present study. Such a treatment would be a task best left to the operators of the application concerned. It could be based on the threat potential discussed in Section 7 as well as the technical measures outlined for overcoming potential threats.

8.2 Identification of objects

Real-world applications of contactless RFID systems in the area “Identification of objects” can be found, for example, in the fields of animal identification, container identification and waste disposal systems. Other relevant fields also include the unique identification of goods as well as person identification.

Electronic identification systems have been employed in livestock husbandry (e. g. cattle, sheep, pigs) for over 20 years. A transponder equipped with the identification data is attached to the animal by tagging or injection. The required international standards for animal identification were passed in October 1996. The International Organization for Standardization (ISO) reached an agreement specifying the code structure (ISO 11784) and technical transmission (ISO 11785). The worldwide unique identification number is a 15-digit number comprising a three-digit country code and a 12-digit national animal ID. [Source: Texa 04] For positioning the transponder on or in the animal, there are at present three methods available: transponder injection, the bolus, and the electronic ear tag. The bolus is a ceramic or plastic cylinder that contains a transponder and which is placed in the reticulum, or first stomach, of ruminants. The electronic identification of livestock must conform to internationally approved injection sites to insure rapid animal identification and the reliable removal of transponders at the slaughterhouse.

Animals are generally marked on the left side. For ruminants and pigs, the scutulum cartilage at the base of the ear have proved to be reliable and painless sites. For horses, the most common site is the left side of the neck at the height of the fourth cervical vertebra. [Source: Idel 98] The field of animal husbandry employs passive RFID systems. The chip is activated by the reader’s radio waves (134.2 kHz) only during the scanning of the ID information by mobile or stationary systems. No batteries are needed for the transponder.

The potential uses of RFID animal identification systems are the rapid, automated and electronic identification of animals, the forgery-proof and unique marking of animals as well as the seamless industry-wide tracking of animals from birth to the slaughterhouse or the final sale of the meat. In light of recent developments concerning BSE (bovine spongiform encephalopathy) and other animal epidemics, this is an important factor in providing reliable documentation on the origin of meat intended for human consumption, which have become a primary criterion for consumers in Germany when purchasing meat. [Source: Hand 04] It is also possible to link the electronically stored ID features with other data concerning an animal’s movements and health (e. g. for providing each animal with an individually optimized feed ration for breeding purposes). Also of note is that, in comparison to traditional methods such as tattooing or branding, electronic marking is considerably more animal-friendly and ensures instant data retrieval. [Source: Vere 04]

The European Commission tested the electronic identification of animals in the course of its study IDEA (Electronic Identification of Animals) conducted from March 1998 to December 2002.

In the study, which investigated the practicability of various tagging systems for ruminants (cattle, buffalo, sheep and goats) in the six EU countries Germany, France, Italy, Netherlands, Portugal and Spain, approximately one million livestock animals were electronically marked by means of electronic ear tags, subcutaneous chips or a rumen bolus. For comparing transponder type performance, approximately 390,000 cattle, 500,000 sheep and 29,000 goats were fitted with a selection of tested and certified electronic tags, rumen balls or injected transponders. The proper functioning of the attached or inserted transponders was verified on one hand by readings made after one day, one month and then on an annual basis, and, on the other hand, by monitoring animal movement (e. g. during slaughtering and after transponder removal). The results of the IDEA project demonstrated that monitoring process is considerably improved by the electronic identification of livestock and that there are basically no technical obstacles to the introduction of RFID systems for cattle, buffalo, sheep and goats. The project also subjected RFID technology to a wide range of external conditions: intensive and extensive management, transport within Europe and beyond its borders, various slaughtering methods as well as extreme environmental conditions in the north and south of the European Union.

[Source: Euro 03] But the studies also revealed some disadvantages of electronic animal identification. Electronic ear tags, for example, get lost just as often as traditional ear tags. Rumen boluses in calves may lead to medical complications. Furthermore, RFID technology is susceptible to electromagnetic noise on farms. [Source: Hand 04]

The aim of the new ordinance is to improve animal health, monitor their movements and to review subsidies – thus offering improved consumer protection in the EU. Under the new ordinance the marking of sheep and goats with transponders complying to ISO 11784/85 will first be optional and then, after a transitional phase ending on 1 January 2008, mandatory for all EU member states having a sheep and goat population greater than 600,000. The ordinance provides for the collected information to be consolidated in a central database in every member country. Farm registries will also contain information documenting which farms individual animals come from and where they are shipped. Up to now, registries have only documented the movements of entire herds. With the introduction of electronic identification, registries will also feature more detailed information than presently recorded: gender, line, and genotype (if known), births and deaths of animals and their movements to and from the farm. A special shipping document will contain information relating to the starting and destination stations of animal transports as well as data concerning the total number of animals shipped. The shipping document will also contain data for identifying individual animals. A database containing all farm information (operator, species, number of animals) is to be established by the middle of 2005. At the same time, information relating to movements of groups of animals will be recorded. The conclusions of the IDEA project will form the basis of further guidelines and methods for implementing electronic identification which will be adopted by the “Standing Committee for Food Store Chains and Animal Health”: guidelines and methods promoting accurate technical implementation, testing methods, acceptance criteria for devices as well as support for the assimilation of databases and communication protocols. [Source: pres 03]

Comparable efforts can be presently observed in North America. In Canada, electronic identification has been mandatory since January 1, 2005 and in the USA, prompted by the latest BSE incidents, mandatory electronic identification of livestock is also under discussion. [Source: Phil 04]

A new networked RFID system of animal identification using electronic ear tags has been developed in Germany by United Information Systems for Animal Husbandry (VIT), based in Verden, and the Weser-Ems Chamber of Agriculture in the course of the project “Innovative Technologies for Cattle Identification” (ITeK-Rind). Its goal is to make the legally stipulated quality assurance and proof of origin requirements in the cattle industry more streamlined, reliable and quicker to implement. Cattle should be identifiable by a chip placed in their ear and the data transmitted to a central computer of the Origin Information System (HIT) in Munich. In a first test phase, the system has been employed since August 2003 at the Infeld experimental farm of the Weser-Ems Chamber of Agriculture as well as at three cattle fattening facilities and a slaughterhouse. The cattle wear RFID labels with a 15-digit ISO identification number. All animal movements are thus recorded automatically. The data are not only transmitted to the central HIT database but also used at the slaughterhouse with the aid of readers and communication technology. The project is sponsored by the Central Marketing Association of the German Agricultural Science Foundation as well as by the curators of the Dairy Producers Promotion Fund of Weser-Ems and Hannover-Braunschweig. [Source: Flei 04] The second project phase, started in the summer of 2004, is to expand mobile data communications so that animal information reports can be sent off wirelessly from every site of the participating farms. In addition, data is to be made available from outside databases (VIT internal as well external), for example performance data or breeding information. The enlistment of further actors (slaughterhouses, consultants, veterinarians) into the system will also ensure the development of an all-inclusive mobile information system. At the same time, the project will be expanded to include approximately 15 additional farms which will employ and test the information system under real conditions. [Source: Via 04]

Another area of RFID application is the identification of dogs using an injected microtransponder, particularly in light of the increasing obligation for certain races of dogs to wear a chip. As early as January 1, 2003, a state canine law in the German Land of North Rhine-Westphalia has stipulated the deployment of microchips for identifying dogs above 20 kilograms in weight or taller than 40 centimeters at the shoulder. This law is under legislation in other federal states in Germany. Starting in July 2004, the European Union will require dogs to have chips upon entry into the EU, the same requirement will take effect in Switzerland at the end of 2004.

The miniaturized chip is injected subcutaneously by means of an syringe. The official in charge can read the number with a simple reader and check the central database as to whether the dog in question should be leashed, wear a muzzle or be subject to the dog tax. [Source: Buch 04]

RFID technology has already been in use for years in the field of electronic container identification. Gas cylinders and chemical containers containing toxic substances must be accurately labeled and uniquely identifiable. High-quality containers and bottles on hire are increasingly equipped with RFID transponders and can thus be immediately localized at every point of delivery. In contrast to barcodes, transponders have a much greater memory capacity. In addition to the container number, they can also store, for example, the owner, the date of the next quality inspection, contents, volume or maximum filling pressure. The use of recordable transponders makes it possible to update data while observing read-and-write access privileges. Furthermore, in comparison to conventional barcode labels, transponders are able to withstand such hostile environments as extreme temperatures, dirt, humidity, irradiance, and acids. The employed transponders are inductively coupled in the container identification and operate at frequencies below 135 kHz. Since a transmission method for the transponder for container identification has not yet been standardized, different systems are on offer on today’s market. [Source: Fink 02]

Ever increasing costs for direct and indirect waste disposal open up new opportunities for RFID technology in the field of waste management. Waste disposal costs are costs which, on one hand, can be arranged by contract with the cooperating waste management firms, and, on the other hand, include workflow management costs for each party involved (processing of weight cards, delivery receipts, invoices, compilation of waste statistics, balancing waste figures). These costs are expected to increase even further as the verification process becomes more complex.

It was against this background that a number of German administrative districts – for example in the Bavarian districts Hof, Erlangen-Höchstadt, Mühldorf am Inn, Kehlheim and Heiligenstadt – introduced RFID applications operating at frequencies below 135 kHz with the aim of optimizing process flows or achieving a fairer, user-specific billing system. Here garbage cans are equipped with a transponder and thus with a unique ID number. This ID number is assigned data relating to the house site and container size. This makes it possible to determine the owner of a specific garbage can, thus eliminating anonymous garbage cans in the future. The transponders feature a passive RFID transponder for identification by the garbage truck. A reader on the vehicle recognizes the transponder and the garbage can’s disposal data (frequency, time of emptying) is stored on a smart card in the garbage truck’s on-board computer. At the end of the shift, the data are transferred to a readout station of the waste management plant. From there the data are transferred to the billing office at the district administrator’s office, where they are evaluated. Some municipalities already offer their residents the service of billing garbage removal by weight. By virtue of the robust transponders on the garbage cans and scales on the garbage trucks, each household is billed for the precise amount of waste it produces. For municipalities, this also offers the advantage of being able to keep precise track of the garbage truck routes. They are also able to monitor more closely the reciprocal costs of external waste disposal firms and optimize the routes covered by the garbage trucks. [Source: Land 04]

Some of the basic advantages of electronic trash can identifications are improved container logistics and management, decreased risk of services being abused by false garbage can registration (in future no cans can be put out for emptying which have not been registered at the district waste management division), simplified billing statements, new opportunities in quantitative data acquisition, creating a more individual and flexible system (customers can in part determine how often they wish to make use of the service “garbage collection”) and ways for customers to reduce their fees by separating their garbage and avoiding excess garbage.

Structural changes favoring the use of electronic identification technology can also be seen in health-care services and the pharmaceutical industry. This includes, for example, the marking of medical products such as blood plasma and specimens. In this application sector, RFID technology is to help lower costs and save on personnel while maintaining quality standards and improving services. One of the main advantages offered by the use of electronic identification in health-care systems in terms of business management is the saving of time: transponders in the lab coat pockets of physicians and nursing staff can automatically authenticate the user in a time-saving manner. Another advantage is its potential for lowering costs: inventory management of equipment and materials equipped with transponders can be made more reliable and efficient. The direct result is a reduction of costs associated with ordering systems and the monitoring of equipment. Furthermore, identification systems for ensuring the quality of medical products are being tested. Thus, active transponders attached to blood bags, for example, can record any change in temperature and protect patients from being administered out-of-date blood supplies. [Source: ACG 04]

A RFID system is currently being tested as part of a pilot project at the pediatric intensive care unit at the Mainz University. Health-care systems elsewhere in Europe have already gained practical experience in this field. For example, at the Rotterdam Clinic transponders are employed to facilitate logistic flows and the handling of materials that are required on a day-to-day basis. Each staff member has three or four lab coats which are washed in a laundry on a rotating basis. When a lab coat gets dirty it is fed into the system. Within ten seconds a freshly laundered coat is issued. This measure is meant to achieve significant time savings in issuing lab coats and providing the laundry with sound statistical data. [Source: Euro 04]

In Sweden a new RFID system was recently developed for attaching to pharmaceutical packaging and is already being employed in a field test. The 32 kilobyte chip can, according to the Cypak manufacturing firm, collect, process and exchange extensive amounts of encrypted data. [Source: ORF 04a]

A RFID technology is also already employed by a number of professional laboratories for managing their large stocks of tissue and blood samples. Equipping pharmaceutical products consistently with RFID transponders would considerably reduce abuse and misapplications. Patients could be warned if they have been taking too much or too little of a medicine. The visually impaired, according to a scenario of Sun Microsystems, could be provided with an output device that could issue such instructions as: “This is aspirin. Take two tablets daily”. [Source: Hill 03a]

The electronic identification of objects in principle opens up new opportunities for organizing the physical environment for the blind and visually impaired, and possibly for the elderly as well. The object of the RFID-based “TagIt” system is thus devoted to making it much easier for these target groups to identify and find books, boxes, articles of clothing, electronic devices, CDs, medication, etc. The employed labels are passive transponders and therefore not very cost-intensive. For example, in order to find a book, users must first enter the search term into the system and pass the RFID reader along the shelf. As soon as the system has detected the searched item, it issues a corresponding signal. [Source: DrLi 04]

The unique identification of merchandise at any time offers potential gains for in-house business measures not least for retailers but also for their business partners along the entire value chain. The logistics chain in today’s merchandise management has taken on increasingly global and complex aspects. Since retailers in general are primarily concerned with optimizing their logistic flows, this area of application will be discussed under “Supply chain management” in Section 8.8.

RFID technology is not only employed for the identification of animals, containers and goods, but also for person identification. In a pilot project conducted by Siemens Business Services in New York’s Jacobi Medical Center, more than 200 people were fitted with a RFID armband. A transponder, only 1/2 square millimeter in size, was integrated in the armband. The RFID system is to support the rapid and precise treatment of patients. Patient data are stored on the transponders which are read by a physician with a RFID-compatible mobile computer, such as a PDA or a Tablet PC. When the patients are admitted to the clinic, their data are stored in an electronic file. The patient is then given a transponder. A W-LAN connection provides the physician with automatic access to the database and he can download all patient-related information to the minicomputer. [Source: ORF 04b]

In Taiwan RFID technology is similarly employed for combating the life-threatening form of atypical pneumonia SARS (Severely Acute Respiratory Syndrome). The patients and the clinic staff wear RFID transponders on their bodies. RFID readers are installed on doors and at other important positions of the building for route control purposes. This is an effective method for the precise tracking of possible infection paths in case of need. [Source: Zeid 03]

As of October 2004, the Japanese city of Osaka is to introduce a RFID system for the unique person identification of pupils at a school. It involves the fixed attachment of tags to either satchels, name tags or school uniforms, which is mandatory in practically all of Japan. According to the plans of the local school authorities, appropriate RFID readers for identifying labels on the satchels will automatically keep track of when each child appears in class and where the child is presently located. Other readers are to be set up at locations which teachers and parents regard as undesirable areas for school children. As soon as a child does enter such an area, the appropriate information can be sent to the parents by e-mail or mobile phone. [Source: Heis 04a]

8.3 Document authentication

At present a variety of approaches are being tested worldwide concerning the integration of personal transponders in personal identity cards and passports. These transponders are employed to implement electronic forgery-proof mechanisms, thus ensuring a broader scope of verification measures as well as storing biometric features – such as the face or fingerprint – in the identification system (e.g. passport). The current trend favors a networking of various identification characteristics in multi-biometric platforms in order to compensate for the drawbacks posed by individual technical procedures.

The European Union (EU) has resolved to incorporate biometric features in its passports and other personal documents starting in 2005. The EU Council has planned on specifying its proposal in more detail by the end of 2004. The first European countries are starting to prepare its practical implementation. Germany’s Bundesdruckerei, which up to now has supplied 62 million EU passports, is currently engaged in such preparations. At the CeBIT 2004 trade fair it unveiled a passport with an embedded transponder as well as the corresponding readers and checking devices. The so-called “verifier terminal” has already been sold in a few European countries, as well as in Asia, for conducting field tests. [Source: Borc 04a]

The Office of Technology Assessment at the German Parliament (TAB) estimates the costs for introducing biometric passports with RFID transponders at approximately 670 million euro. Taking running costs into consideration, the financial requirements increase by 610 million euro annually. The U.S. General Accounting Office calculates start-up costs of approximately 8.8 billion US dollars for launching biometric passports in the USA, followed up by annual costs of approximately 2.4 billion US dollars. In addition, it will also be necessary to take into account the costs for the biometric visa. These have been estimated at 2.9 billion US dollars for initial investments and subsequent costs of up to 1.4 billion US dollars per year. [Source: TAB 03]

The International Civil Aviation Organization (ICAO) has made an in-depth assessment of the IT security problems with respect to passports and has drawn up corresponding security specifications [Source: ICAO 04a]. These relate in particular to anti-forgery measures and the relevant means for developing authenticity checks and accessing biometric data. The ICAO engages in establishing international standards for travel documents. The UN authority has drawn up a proposal that, starting in 2006, all countries may issue travel documents whose biometric data can be read via a transponder at a distance of up to ten centimeters.

Face recognition is the biometric method decided on by the ICAO. According to the ICAO specifications, passport photos in the EU are supposed to be stored as biometric data on RFID transponders. Countries have the option of storing additional biometric features in the passport or in a national database. [Source: GinO 04] .

According to the ICAO, the transponder in the passport should have a memory capacity of at least 32 kilobytes [Source: ICAO 04b]. 20 kilobytes are required for the raw data set of one face, which can be reduced to only 16 kilobytes by JPEG compression. To make it possible for countries to operate with different systems of extraction, the ICAO has specified that the passport must contain the original data instead of a template, i. e. that no data be reduced to the parameters of a given feature space. With respect to additional biometric features, on the other hand, templates may be stored as an alternative. Ten kilobytes are needed to store data for each finger. The template, in this case the image of the characteristic points of a fingerprint (minutia), is between 250 and 750 bytes in size. Storage of the original iris data takes up 30 kilobytes, while the template requires 512 bytes. In addition to these biometric data, the transponder must also store personal data – such as name, date of birth, place of residence, etc. – as well as any additional remarks such as “embassy staff ”. Due to its greater data memory requirements, the US Department of the Interior, in contrast to the ICAO, prefers a 64 kilobyte chip. Up to now, however, there has been no manufacturer who mass produces such chips. With its SLE 66CLX320 Infineon has a 32 kilobyte chip ready for series production and has announced a 64 kilobyte chip for September 2004. Philips has already produced a small batch of 72 kilobyte chips for passport prototypes and claims that it is ready to start mass production immediately. [Source: Schu 04a]

The Ministry for Internal Affairs in the Netherlands – which is in charge of issuing passports and identity cards – has started the project “2B or not 2B” aimed at examining the integration of biometric data in travel documents. Up to 15,000 volunteer test persons in six municipalities are given a passport in which biometric data has been stored on a RFID chip. The biometric data recorded in the test document are verified when the passports are given out. In compliance with the requirements of the International Civilian Aviation Organization ICAO, fingerprints and face identification are employed as the identification systems. The test passports are checked by the border control security system of the Canadian firm BioDentity, which is also utilized by the Bundesdruckerei in its automatic border control system. [Source: Borc 04b, MBZK 04]

8.4 Maintenance and repair, recall campaigns

Firms operating in various branches of business are also increasing their use of RFID transponders for customized and automatic maintenance and repair services as well as for recall campaigns.

For example, RFID transponders can be used for tool identification and the associated maintenance management. This is basically to ensure that tools are used at the right work station and that workplace requirements are observed accordingly. Plant equipment such as tools are increasingly regarded in plants and companies as the key to quality, staying on schedule, and economic efficiency.

In the past, developmental work was primarily invested in tool optimization, whereas today, with the spread of 1:1 batch production, the main focus is on process optimization. The many individual project development phases must ultimately be coordinated intelligently with a diverse array of deadlines, data and modification information in an business environment of ever-shorter periods of product development and product lifetime. Besides the potential to be realized in lowered costs and greater security, the field of tool design and construction will also face new demands, including those posed by the extension of product guarantee to 24 months as stipulated by the new EU law of obligations. In the future, toolmaking plants will be bound to establish clear-cut definitions for their wearing parts and their lifetimes. The toolmaker will then only assume liability if professional servicing has been observed and documented. [Source: ISK 03] In light of these developments, one can expect a greater use of RFID in this branch.

The firm Flugzeug AG, for example, has tested a toolbox whose tools are equipped with RFID transponders. The toolbox itself is provided with a RFID reader. The transponders contain the serial number of the tools as well as the number of the associated toolbox. The main function of the toolbox is the automatic monitoring of its contents using RFID technology. In this way, the application can immediately determine if foreign tools have been inadvertently placed in it. In addition, the application records the frequency of tool use on the basis of how often tools are taken from and returned to the toolbox. These data are evaluated in the tool management system. On the basis of this information, the system informs mechanics when tools have to be replaced or serviced. The application runs in the background and relieves mechanics of their traditionally time-consuming inspections, since the RFID-supported system alerts them only when the need arises. [Source: StFl 04]

Airbus, one of the world's leading aircraft manufacturers, also uses RFID labels on tools for improving the maintenance process. Precision tools for repairing highly-sensitive aircraft parts are used not only by Airbus but also leased to maintenance firms. The RFID-labeled tools not only instantly provide all important information for their identification and localization but also information concerning their entire life cycle – making it possible to schedule routine calibration and tool maintenance tasks in an effective manner. A process loop exists between Airbus, the tool maintenance firms and customers and its status is monitored with the help of RFID. If it becomes necessary to have the tools serviced, an instruction is issued to send them to them to the workshop. [Source: SAP 04]

Recall campaigns, which are still relevant today, are expensive for firms and also quite a source of annoyance for customers. In the year 2001 alone, Germany saw 113 recall campaigns in the automotive sector. Well known to the public is the example of the tire manufacture Firestone, which was forced to initiate one of the biggest recall campaigns in history following a series of fatal accidents involving Ford Explorer vehicles equipped with Firestone tires.

In 2000 the manufacturer recalled 14.4 million delivered tires on account of a production error leading to possible abrasion and blow-out risks. At the same time, 6.5 million products of this batch are still in use today. Also in consequence of this incident, US authorities reacted by establishing more stringent quality protection requirements. [Source: ZDNe 04]

Thus the National Highway Traffic Safety Administration (NHTSA) introduced a regulation requiring vehicle manufacturers to equip their cars with a tire pressure control system. Until October 31, 2006 automobile manufacturers may freely choose any one of the systems on the market. To date there are two control systems available, which are also offered by German automobile suppliers. The so-called "direct" control system and its precision measurement directly monitors tire pressure. The device warns the driver if one or more tires reaches a potentially dangerous low pressure. In the second variant, the so-called "indirect" tire control system, the tire rotation rate is monitored by a sensor. Underinflated tires have a smaller diameter and therefore rotate faster. The drawback of this quite economical variant is that tire behavior is monitored only by making a comparison with the other tires of the same car. The system would therefore fail to report a synchronous deterioration of several tires. On March 1, 2005 the NHTSA is to announce which system shall be mandatory after October 31, 2006. [Source: Mark o. J.]

The tire manufacturer Michelin has stated that it plans to be the first firm to provide tires embedded with RFID transponders as a standard feature. Starting in 2005 this technology can be acquired as an accessory in new cars equipped with Michelin tires. The memory of the miniaturized electronic part can be provided with new information by radio signal and can therefore store the vehicle identification number or other data along with the tire number. Information can be retrieved using the appropriate devices at distances up to approximately 60 centimeters. This means that age, tire pressure, road conditions and other information can be automatically conveyed to the car's on-board computer. The electronics are provided by Fairchild Semiconductor and Philips under license of Intermec Technologies. [Source: Inno 04a]

German Railways (DB) is testing RFID for improving the quality of its maintenance services. The site of the pilot project is a repair plant in Duisburg. In cooperation with Symbol Technologies, Euro I.D. has been testing the use of a RFID system for the overhaul and maintenance of railroad cars. The aim of this project is the safe acquisition of servicing data. Data had previously been stamped on axle sleeves, but since they tended to break off the axle, all acquisition data were missing at the next scheduled maintenance. Transponders should prove helpful in this field. Thus, recordable transponders were attached directly to the axle shaft of the railway car and written with all data acquired in the course of repair. The basic data are recorded electronically only once. All data can be read and supplemented from various maintenance sites. The use of RFID should eliminate the source of error inherent in manual data entry. [Source: Euro 04]

In addition, the identification of foodstuffs represents an important area of RFID application for the efficient control of product recall campaigns. In the interest of consumer protection, the European Union enacted Regulation (EG) No. 178/2002 laying down the general principles of food law. The regulation requires all participants in the “foodstuffs” supply chain to ensure the traceability of their products by December 31, 2004 and to provide the competent authorities with this information upon demand. Furthermore, the regulation obligates all companies to recall foodstuffs which fail to meet legal food safety requirements. Grounds for recall apply even to suspected cases. [Source: ECR 04]

Since the chips feature a 96-bit ID number, they can convey the individual serial and product number in addition to the manufacturer and product names – conventional barcodes are generally used to encode the product designation and manufacturer – and the production path of products can be tracked on the basis of RFID technology, a feature which is increasingly required by law. At the same time, perishable goods can be assigned a use-by date and their current storage place, thus letting supermarkets know if and how many products approaching the use-by date are on their shelves. Such information can be used to launch special sales campaigns, for example, or to shift goods to the “pole position” on the shelf to enhance their rapid sale. [Source: Sinn 04]

8.5 Zutritts- und Routenkontrolle

Magnet cards or smart cards – whether used as an ID to enter rooms or buildings, as a prepaid card for making calls with a public telephone, for example, or as a credit card – have now become a commonplace item. Typically, these cards must be inserted in a terminal which then makes the connection to other IT applications, such as time registration or cash withdrawals from credit accounts. Contactless data acquisition is possible with today’s RFID systems, thus enhancing the performance features of known card applications. The transponder frequently takes the form of the plastic card familiar to many users, but key chains and armbands can also be used. Electronic identification card systems typically operate at 13.56 MHz. The readers must be installed to insure a maximum reading distance of one meter. The systems typically operate in the mid-performance range: besides performing the actual identification, they are also capable of writing in order to update data when necessary or to support the multifunctional processes of the RFID system.

Contactless access authorization systems have already established in today’s market for vendors wishing to provide rapid identification of individuals or to cut down on lengthy control procedures. The cost-effectiveness of RFID systems becomes particularly attractive when individuals must repeatedly pass access control points. A typical field of application for many years has been the use of electronic access control systems at holiday resorts, which are usually combined with a digital “purse”.

For example, the Austrian region of Nassfeld/Sonnenalpe – as in many other holiday resorts – implemented an RFID scheme during the 1999/2000 season which incorporated a large number of various tourist service providers such as operators of hotels, ski lodges, ski lifts or gondolas. The idea was that guests should be able to move about the region during their entire stay without having to use cash or contact credit cards.

A total of 715,000 euro was invested in establishing 80 reading devices, ten standard cash systems and 50 offsite points of sale in hotels, accommodation services, ski rental shops and ski schools. Services could also be booked over the Internet or by cellular phone networks and then stored on the transponder at every point of sale. A regional radio network was established for this purpose which connected over 40 PC transmission and receiving stations with a central server that stored the guests’ data.

Two different types of transponders were used in card format: cards in the frequency range of 122.8 kHz were used as multi-application cards (including their use as a “hotel key”), cards operating at 13.56 MHz were only used as a ski pass. The memory capacity of the 13.56-MHz cards is 2048 bit.

The 13.56 MHz data carriers have an up- and downlink speed of up to 26 kbit/s, the 122.8-kHz cards only three kbit/s. Although the card format does conform to ISO 7810, having the typical smart card size of 85.6 by 54 millimeters, the actual RFID system is not an ISO data carrier. The maximum reading and writing distance is 40 centimeters for both cards.

Anticollision methods are possible in principle, but were not implemented due to an “extreme drop in hardware performance” of the reader. Since guests in the ski areas usually maintain an average distance of 80 centimeters from the reader, the number of transponders in the recognition zone is also limited. To detect errors in data transmission, the cyclic redundancy check (CRC) was employed. On most of the data carriers used, it is possible to configure a number of authorization levels (e. g. ski pass on the first level, hotel key on the second level). Authorizations are stored and protected by password. The stored data are encrypted for each level.

The scheme’s operators attribute the high rate of customer acceptance primarily to the system’s convenience. Using the ski lift, for example, no longer involves the cumbersome search for one’s ski pass. Should the card be lost, it can be quickly blocked and a new one issued. If there is a long waiting line at one point of sale, services can be purchased at another point of sale. For service operators, potential savings can be realized by quicker access flows, thus eliminating waiting lines at ski lifts, for example, by reduced expenditures on personnel for access control, or by the rapid processing of transactions for all participating service providers. On the basis of this, the data of the central marketing server can also contribute to optimizing the line of services offered by providers or by the target sector as a whole. The application makes it possible to evaluate in detail individual customer data, the demand for services, and total sales volume. This produces a great quantity of personal data which are quite conducive to generating a precise profile of personal preferences and favorite sites, as well as to tracking a customer’s path during his or her stay in the region. Precise route tracking of the data carrier can be made at every point of sale (facilities used, elevation gains, etc.). These data can be used to optimize lift loads, infrastructure improvement, etc. Programs are presently being developed that would present a graphic representation of customer flows, thus making it possible to inform the ski guest of crowded ski slopes, for example.

The capability to adapt transponder performance features to the requirements of the area of application is illustrated by another example of access control taken from the field of recreational activities. Customers in a fitness center are given armbands equipped with a heat-resistant transponder that can also be worn in the sauna. Its impact-resistant design also enhances its performance range. [Source: Euro 04]

Another prominent example of RFID-based access control systems is being planned during the run-up to the 2006 World Cup soccer games. During the 2006 World Cup games in Germany, all admission tickets will be provided with a transponder and the entrance points at all twelve soccer stadiums will each be equipped with RFID readers. This is meant to prevent ticket forgeries and ensure that tickets are sold only to legitimate fans and not to known rowdies. [Source: Pößn 04] The admission tickets for the event will be chiefly sold over the Internet. The purchaser first receives a certificate that confirms his claim to a ticket. Four to six weeks prior to the start of the World Cup the personalized admission tickets are sent out by mail – but no longer as an insured letter. The data is transferred to an electronic admissions system. Lost tickets can be blocked and reissued. Ticket holders entering the soccer stadium hold their admission card up to the reader and their data are matched with the electronic admission system. After the 2006 World Cup, this concept will be used by stadium operators for Bundesliga soccer matches and other large public events. [Source: ECIN 04, Heis 04b]

The performance features of the RFID-based access control systems outlined here are characteristic for other areas of application, such as the ticketing of recreational events (theater, concerts, sporting events). RFID systems facilitate the issuing of tickets for individual events or for such events as world championships, where admission to a number of events or for a particular period of time can be stored on an electronic ticket. The ticket can be issued directly at the point of sale with the appropriate writing devices. In case of loss, the ticket can be blocked and reissued. Individual control is no longer required during admission and tickets are harder to forge.

Another main focus of RFID application is authorization checks for entering limited-access areas. These have been established primarily in business firms, but are also being increasingly discussed for public spaces, such as airports. Authorized persons are given a personalized transponder which can be embedded in various forms. Authorization can be selectively applied, thus allowing access to the general premises as well as permitting or blocking access to specific areas by employing the appropriate readers on doors and possibly in gate systems. In this area of application, additional RFID functions are also implemented on a regular basis. Recording the time of access or hours worked is typical in the corporate sector.

In (high) security areas the data stored on the transponder can also encompass biometric features of autoidentification such as facial geometry, fingerprints and the structure of the eye's iris. In general, the use of biometric features in the autoidentification field includes the export of the biometric data from the RFID memory chip of the identification documents, the import of biometric features using the appropriate sensor technology and the matching of the data with the already stored data sets. The basic purpose is therefore to compare the measured biometric data with the biometric reference data stored in the electronic document.

The identification of objects, persons or different sites also lends itself to systems for progress and route control. A relatively new area of application is that of recording the times when persons are present at diverse sites and to track their movements. In light of the increasing use of subcontractors and outsourcing, RFID makes it possible to perform an indirect inspection of the services performed, on one hand, and to keep track of the precise times for accounting these services. For example, the city of Dresden has installed transponders at selected service sites, such as bus stop shelters and playgrounds. Contractors are provided with mobile readers which are used to store the performed services at the site. The data are to enable the city of Dresden to improve the planning of outsourced services and optimize them further. This system employs smart cards whose performance features correspond to those of the electronic access IDs discussed above. [Source: Euro 04]

Route control is being utilized more and more in the field of baggage and parcel transport. Airlines, for example, have introduced systems for identifying baggage pieces by RFID. In addition to baggage routing, parcel routing is another area of application that is already in widespread use today. The reason for this is that the RFID system is operated on an in-house basis. There is generally no need to establish interfaces to other business players. The application merely requires the use of simple tags, which are assigned an ID number at the start of the process. No further data import is necessary. Identification can also be established at a conveying rate of up to four meters per second. The 13.56 frequency range is employed. Progress is controlled by a central database which is updated when the object passes a new control point. Thus, not only the parcel service operator but also customers can track the delivery of their order per Internet.

The deployment of RFID for letters and packages is the focal point of a seven-year pilot project initiated by the "International Post Corporation" (IPC) in May of 2004. The IPC is a federation of 23 European, American and Asian postal companies which also includes the Deutsche Post of Germany. IBM has developed software for the scheme which is designed to administer the coordination of postal deliveries. In the course of the pilot project, each year 3,000 test users will send half a million letters and parcels, each equipped with an active RFID tag, between 26 countries. The active transponders employed operate mainly in the ultrahigh, or microwave, frequency range. These RFID system are characterized by an identification range of up to one-hundred meters, but are relatively expensive and, because of the transponder's battery, can be operated only in a limited temperature range. [Source: Sili 04]

Another very powerful solution in the ultrahigh frequency range using an active read/write transponder has been employed since 2002 by Deutsche Post in Germany for the identification of vans and containers. This application is also suited for use in inclement surroundings. 66 read/write units and 11,000 transponders were installed in 33 postal centers. Every vehicle and container is equipped with a transponder. The ID number of this tag cannot be altered. Furthermore, its 56 kilobytes of information can be rewritten up to 100,000 times. Readers are installed at nodal points, such as the entrance to freight centers. According to the manufacturer Identec Solutions (product: i-Q series), the simultaneous identification of thousands of items is ensured by anti-collision methods. Due to its robust construction, the transponder is also suited for industrial applications. Once electronic identification has been made, drivers are given a printout that informs them of the ramp where the shipment must be delivered or received. In addition, the system has an access control feature. This RFID solution thus provides a real-time view of the number of delivery vans and containers on site. Should modifications become necessary in the supply chain, these procedures can be promptly implemented by the central database system. [Source: Kric oJ]

The RFID solution described above is also used by the Volkswagen automobile manufacturer for identifying vehicles as well as for tracking and tracing operations involving distances of up to 100 meters. At the Wolfsburg plant, vehicles are prepared for pickup. Once their production has been completed, vehicles are equipped with a transponder containing the vehicle identification number and a list of tasks to be completed. The vehicle can be easily found by the transponder’s activation of blinking LEDs in a mobile reader. Services are automatically recorded on the transponder as they are performed, for example when entering the car wash installation. The transponder also supports process flow control at the car plant. For example, the dimensions of automatic transport systems are adapted to the car wheel positioning. The RFID tag can be reused. [Source: Iden 04]

In other countries cars are equipped with RFID technology for testing automatic collection of highway tolls, for example. In the course of a pilot project conducted in South Africa, vehicle license plates were fitted with passive RFID tags which could be read at a distance of six meters. In the test, four vehicles were each provided with two RFID tags behind the windshield and driven past a RFID reader. Readers can register up to 7,200 RFID tags per minute. In order to simulate high-volume traffic conditions, vehicles were driven past the readers one after the other, abreast and even in opposite directions at speeds between 80 and 100 kilometers per hour or even greater. Even at speeds of approximately 250 kilometers per hour, the readers continued to record the RFID tags with no problems. The RFID tags proved to be very temperature-resistant during testing, as they operated smoothly at temperatures between -40° and +85° Celsius. [Source: SEC 04a]

RFID technology has also been tested in public transportation. For example, busses in Edinburgh, Scotland were equipped with RFID transponders. As soon as busses approach a traffic light, it automatically turns to green. With this system, public transport vehicles have been able to reduce the time previously needed to complete their routes by ten percent. [Source: Hill 03b]

8.6 Theft protection and stop-loss srategies

Also under discussion is the use of RFID systems for protecting against theft and reducing loss. For example, RFID is employed by airlines not only for routing control but also for reducing the volume of lost luggage and for finding lost bags more quickly. Delta Airlines, for instance, transfers between 35 and 85 million pieces of luggage per year. Although less than one percent of this volume is misdirected, the associated costs amount to 100 million US dollars per year. By contrast, the investment costs for implementing a RFID system are estimated at 25 million US dollars. [Source: tecc 04]

Airlines are also planning on using RFID to prevent losses in their container and storage management systems. At present they are faced with problems of inventory management but also those concerning the return of containers hired out to third parties. The localization functions of RFID are to be employed to improve asset management. Such systems are also used in other branches, such as the automotive sector.

RFID solutions have been used extensively for many years in car anti-theft technology, which interrupt either the ignition, the starter or fuel pump, and which are deactivated by an RFID transponder in the car key. In this field Siemens has developed solutions which control access to buildings or the use of motor vehicles by means of a “smart key” integrated in a mobile phone in conjunction with a reader. The familiar car key of today is no longer needed. Mobile phones can also be used in another functions – as an electronic purse, as a ticket in local public transport systems, or as a scanner for reading tags for data acquisition. In this regard, Siemens has been testing a combined RFID-NFC technology (Nearfield Communication – see also Section 10). [Source: Gole 04]

Another area of application in asset management is the office environment. RFID systems are used, on one hand, as an anti-theft device, particularly for high-value mobile devices such as laptops, and on the other hand for locating files or for the control of pneumatic delivery systems. For example, American law offices use electronic labels to identify their documents. The labels are marked with a write device and attached to the document. So-called tracking pads are employed in the secretary's office or filing department to control the documents before they are sent out. This information is stored in a central database which can also be queried to track the documents. Mobile readers support inventory or the location of lost documents. The 3M company, a provider of tracking solutions in this field, claims that the RFID system can immediately track 95 percent of documents (file accuracy). In contrast, a practical example using a well-established barcode solution would yield only an accuracy of 65 percent. [Source: Malo 04] The use of RFID systems in pneumatic delivery systems is aimed at avoiding the number of misdirected letters. In addition, canisters can be automatically routed back to the sending station. With the help of database applications, it is possible to control and optimize canister cycle times.

A telecommunications firm in Hong Kong localizes office furnishings practically in real time. The fixtures are provided with transponders which can be located by employees using a PC or mobile phone. In principle, this can also be used for computer-aided inventory without manual control. The system is also used to optimize company resources. [Source: Comp 04c] Comparable RFID solutions are also used for anti-theft measures or to reduce the amount of losses in the retail trade. In this field, 1-bit systems have already been used for roughly 40 years for electronic theft protection, known as electronic article surveillance (EAS). The signal sent by these systems to the reader conveys only the presence or absence of a transponder in the scanning field. Nowadays quite common, these security labels – such as those attached to clothing – must be set to "zero" at the cashier in order to prevent the triggering of an alarm when the item is carried out of the store. (see also Section 8.8 "Supply chain management").

These solutions can be achieved in a more "intelligent" manner with today's RFID systems, i.e. if necessary, the transponder can be hidden in the item by the manufacturer and provided with detailed product information in order to prevent shoplifters from switching price tags, for example. Typically, such solutions are not limited to theft protection, but are employed to make product information more easily available, thus optimizing inventory procedures for e.g. retailers. But they can also be used – as tested by the fashion company Prada – to provide customers with additional product information, which can then be displayed onscreen in the store.

The use of hidden transponders also provides new opportunities for protecting small animals, breeding animals or protected species against theft, mistreatment or loss. By using injected microtransponders it is possible to give an animal an identification that is distinctive, non-detachable and tamper-proof worldwide. Pubic authorities, veterinarians, animal shelters, national and international breeders associations, universities and zoos are able to identify admitted animals with a reader and compare it to the information stored in a central database. In this respect, transponders are employed within the scope of the Washington treaty on the protection of species, officially known as the Convention on International Trade in Endangered Species of wild Fauna and Flora (CITES). CITES is a key instrument in binding international law that is in force in over 150 contracting states. [Source: Euro 04]

RFID-based technology can also be used to identify run-away or stolen pets and determine their actual owners. In principle, from a medical point of view, practically all pets can be identified with transponders. In dogs, cats and rodents, the chip is applied subcutaneously to the left side of the neck by a veterinarian using a sterile disposable applicator.

After injection of the transponders, the pets must be registered in various databases. Those of relevance include, for example, the German central pet registry, TASSO and IFTA (international registration). Readers are available in animal shelters, in many veterinarian practices, at border crossing points and in general at exhibitions, tournaments and auctions. [Source: Katz 04]

8.7 Environmental monitoring and sensor technology

For monitoring environmental conditions using RFID, two types of applications are conceivable:

- Tags can be used to support the monitoring of fauna by being attached to the animals and read by reading stations installed in the wild. This method can also assist in drawing a number of conclu sions relating to other parameters of sur rounding conditions.
- Tags are provided with sensors which measure such environmental parameters as temperature, humidity or the level of pollutants. These sensor tags are put in stationary or mobile objects and read eit her intermittently or at the end of the anticipated life cycle.

Neither approach is yet employed directly for environmental monitoring, but there are related fields of application which demonstrate the practicability of these methods.

In Sweden, for example, what is known as a “lachsracet” (salmon race) has been held in the Vindelalven river since 1997 and is open to the public. Here microtransponders were subcutaneously applied to a total of 50 salmon weighing between 4.4 and 11.5 kilograms. Encased in bio-compatible glass, the transponders have a diameter of 2.2 millimeters and a length of 11.5 millimeters. As the salmon make their way upstream, they are guided through narrow artificial channels, such as fish steps, where a reader having a range of 38 centimeters reads and records the code of the fish. The transponder requires no battery. As the salmon swim past the reader, their identification data is read. Since this data is issued only once on a worldwide basis, every fish migrating upstream in the Vindelalven river can be unmistakably registered as it passes the antennas. A series of 25 readers was installed along the Vindelalven from its source to its mouth. Prominent sponsors have been found for the “salmon race”, where bets are placed on individual fish. The 50 salmon sponsors include the crown princess Victoria, the transponder company Trovan-Transponder, DaimlerChrysler Industries, various operators of hydropower plants, municipalities, banks, sporting goods manufacturers and machine construction firms, fishery associations, as well as Ericsson and Microsoft, who provided financial support to the project. [Source: AOLm 04]

Sensor-equipped chips are increasingly used to monitor specific effects of the environmental on goods in transit. For instance, a chip manufacturer in Dresden orders temperature-sensitive photochemicals from a supplier in Amsterdam. To avoid exposing the chemicals to high temperatures during transit and their resulting spoilage, the manufacturer employs digital temperature loggers. These are put in a shipping container, where they keep permanent track of the ambient temperature. After the measured data are read, they are converted to a XML format. Upon arrival at the plant, the values can be immediately fed into the MySAP PLM system. Spoiled goods can thus be detected at once and returned. Furthermore, the site and cause of damage can be determined for documentation in any liability cases. [Source: Fleis 02]

The Swiss Federal Institute for Materials Testing and Research (EMPA) is currently developing a project for installing RFID transponders with sensors in bridges and road surfaces for the purpose of collecting data on mechanical and environmental parameters that can be read while driving by.

8.8 Supply chain management: automation, control and process control and optimization

One area of RFID applications that is frequently mentioned is supply-chain management. In practice, a “supply chain” is a network of different firms cooperating with each other to make a product and deliver it to the end customer. With today’s emphasis on reduced stock levels and the implementation of the “just-in-time” principle, the control and monitoring of the supply chain has become a key to success. Difficulties in production, with suppliers or during transport of merchandise can have serious consequences for downstream processes.

Against this backdrop, RFID technology is seen as a very promising solution for creating the transparency needed to implement a more efficient control of logistical process flows. The basic idea is to develop the potential for rationalization within the cross-sector value creation chain and to organize the overall flow of materials, information and financial resources with the greatest efficiency possible. With RFID technology, it is possible to track products and materials in real time down to “batch size 1” throughout the entire logistics network. The radio labels attached to the merchandise provide information on the products as well as the time and place of their movements.

After the IT consultant group LogicaCMG announced the impending breakthrough of RFID technology in April 2004, a more cautious assessment of its market chances was made a few months later by Booz Allen Hamilton in a joint study with the University of St. Gallen. [Source: Booz 04] The empirical study entitled “RFID Technology: New Motor of Innovation for Logistics and Industry?“ was conducted worldwide with over 30 leading companies from Germany, France, Austria, Switzerland, Great Britain and the USA. The group was dominated by providers in the fields of transport and logistics as well as clients in the automobile industry. According to the results of the study, the use of RFID pays off in those branches where the utmost in process reliability is needed in order to meet strict documentation requirements and in addition where a closed logistics cycle ensures the reusability of the hitherto costly tags. This applies primarily to the automobile industry. In contrast, the study shows that open systems, which form the basis of applications in commerce and the consumer goods industry, are not yet capable of yielding a fruitful cost-benefit ratio due to high investment costs in tags, reader infrastructure and system integration.

Nevertheless, the retail industry, which is under intense competitive pressure, is at present still intent on employing RFID technology in their logistics systems in order to realize its comprehensive potential in lowering costs. On the whole, according to a study conducted by A.T.Kearney, RFID provides two advantages for merchandise management: the reduction of inventories and thus the reduction of warehousing costs and tied-up capital, and the reduction of personnel costs in shops and warehouses. [Source: ATKe 04]

According to current forecasts made by Soreon Research concerning the development of the RFID market in the commercial sector, the next four years should see an overall growth of the RFID market in Europe from just over 400 million euro (2004) to 2.5 billion euro (2008). Germany is expected to be the leading RFID market in Europe with a volume reaching 600 million euro in 2008. Analysts anticipate a drop in transponder prices in the coming years brought on by the use of lower-priced materials in production and savings realized through large-scale production. One of the underlying reasons supporting the anticipated growth in the market is that retailers will use tags not only on pallets and cartons but, starting in 2006, will also increasingly apply them to individual products at the point of sale. Soreon Research assumes that by 2008 about five percent of all products retailed in Europe will feature a RFID tag in addition to the bar code or in place of it. European retailers (EU 15) market over 260 billion items per year. [Source: Sore 04]

Developments in commerce can be represented by the global drivers of RFID technologies: Metro, Wal-Mart and Tesco.

The “Future Store” of the METRO Group Future Store Initiative – a collaboration of the METRO Group with SAP, Intel, IBM and other partner companies from the fields of information technology and the consumer goods industry – has been set up in the North Rhein-Westphalian town of Rheinberg as a pilot project for supermarkets with a package of technological innovations. Implemented at the Future Store is a fully integrated system in the areas of inventory management, information systems and point of sale. The long-term goal is to accelerate structural change in retailing, establish uniform standards for commerce worldwide and to create a wireless network incorporating the entire supermarket. Even the manual barcode readers at cash registers are to be replaced by electronic readers on the shopping cart. Antennas and displays continually record the goods placed in the shopping cart and relay the final results to a payment system. The data of the RFID tags are stored in a central computer, known as the RFID flow of goods system. All partners in the logistics chain – i.e. in retailing, central purchasing, warehousing, distribution and production – have access to this database. The pilot project also tested fully-automated “self-service cashier stations”, where customers pass their shopping items over a 360-degree scanner to record the price. The scanned items are then placed in a bag which is automatically weighed. If the resulting weight deviates from that of the scanned items, an automatic warning is sent to an employee at the information desk. If the weights match, the tags are cancelled and the goods are booked from the merchandise management system.

The world’s fourth-largest commercial enterprise, the Metro Group, has by now opened a “RFID Innovation Center” in Neuss, where marketing lines, technology partners and suppliers can prepare themselves for the introduction of RFID technology before Metro integrates them into the supply-chain process. The METRO Group will probably be the world’s first commercial company to replace conventional barcodes with RFID transponders throughout the entire supply chain. The first phase of the rollout is scheduled for November 2004 with an initial 20 suppliers, which in Germany is to be successively expanded to include about 100 suppliers, eight warehouses, and 269 sites of the Metro Cash & Carry, Real and Kaufhof distribution channels. According to plans, by the start of 2006 a total of 300 suppliers will deliver pallets equipped with radio chips to the distribution centers of the Metro Group. [Source: Com 04b]

The introduction of RFID systems at the Metro Future Store has already resulted in considerable uncertainty among consumers. Because the Metro Group issued a customer payback card with a transponder without informing consumers, it has drawn heavy criticism from data privacy advocates. Furthermore, the “Association for the Promotion of Public Mobile and Immobile Data Traffic" (FoeBuD) has criticized that the RFID tags contained in the price tags still function after leaving the store. As a result, the Big Brother Award in the category “consumer protection” was awarded at the end of 2003 to the Metro Group for its “Future Store Initiative”.

Last year at the Cambridge branch of the British supermarket chain Tesco, all packages of Gillette Mach3 razor blades were provided with RFID tags. Because of its high price and good chances of being sold on, Gillette’s “Mach3” razor blades are, according to the manufacturer, “the most coveted item of British shoplifters”. The company loses approximately 30 million US dollars per year through shoplifting. [Source: Hand 03, McKa 03] According to Tesco spokesmen, the now concluded pilot was meant to gain new knowledge in the field of merchandise logistics. However, the organization “Consumers Against Supermarket Privacy Invasion and Numbering” (CASPIAN) claimed that the supermarket manager also installed anti-theft devices and secretly photographed customers who handled the razor blade packs equipped with radio labels. It also said that cameras were posted at the checkout counter to film all customers wishing to leave the store with a RFID-secured item. CASPIAN then called for a worldwide boycott of Gillette. [Source: Heis 03]

The big player in the US retail sector, Wal-Mart, has concluded its pilot program for introducing RFID labels in its stores and distribution network, claming that it has encountered no problems and that it plans on implementing the technology on a wider basis. Wal-Mart initially tested RFID technology only in the Dallas area. In the test, RFID-tagged cartons and pallets for 21 products provided by eight suppliers were sent to the distribution center in Sanger, Texas, which then distributed them among seven local “Super Centers”. By January 2005 the company intends on having its top-100 suppliers switch to RFID technology. Wal-Mart is presently organizing a conference with 200 large-scale suppliers to discuss the further expansion of the RFID program. [Source: Com 04a]

The use of RFID technology in optimizing business processes is also becoming more frequent in the area of industrial manufacturing. Transponders are attached to the parts to be produced, which not only enables data to be read but also to be written to the data carrier. In addition to the identity of the part, transponders can also document its actual status (e. g. stage of processing, quality-control data), as well as its past and future status (desired final state).

Since the automobile industry produces exclusively to order, with two ordered vehicles rarely matching one another exactly, automatic material flow control has become the most crucial requirement in this branch for ensuring smooth operations. In addition, the ever-greater cost squeeze faced by the automobile industry in the production of new model ranges encourages the continual reduction of process-related costs. On one hand, this objective is achieved by increasing automation in production and logistics. On the other hand, attempts are made to ensure a reliable production supply while making constant reductions in on-site inventory. RFID technologies are primarily employed in the area of chaotic production systems.

Thus, DaimlerChrysler in the USA and Volkswagen in South Africa have already started to equip each bodyshell still in a very early stage of production with a transponder which remains with it throughout the vehicle's entire life cycle. The distinctive coding controls the manufacturing process (coordinating the appropriate assembly components, choice of color, type of motor, etc.). Later the transponder ID number can be used to identify the vehicle in the service points, e.g. for reliable information concerning the assembly component versions for procuring spare parts. In addition to the direct identification of the vehicle, transponders are also provided in the transport skids. This requires the use of robust transponders, since they are continually subjected to temperatures of approximately 220° Celsius during heat treatment of the paint finish. The chaotic production of different types of vehicles on one assembly line depends crucially on the reliable identification of the supplied assemblies and components. To this end Opel of Belgium has marked workpiece supports as well as mounting devices with transponders. The resulting advantages: no delivery of wrong parts, optimized assembly line flow, no retooling or waiting times, more efficient production and an optimal flow of information to the service points. [Source: Euro 04]

Aiming at optimizing the overall logistic process, a large-scale automobile manufacturer in Baden-Württemberg, in conjunction with a number of suppliers, has implemented a RFID-based solution for container management. Here the supplier uses a read-write device to record container-specific information, such as quantity, article code, container ID, etc., on the responder, which is fixed to the carrier. All production-relevant data are thus associated with the container. After the individual containers are loaded on a trailer, the data collected by the reader is consolidated in a delivery slip, which is also written to a transponder attached to the trailer. Once the truck leaves the supplier's depot, the delivery slip data are automatically received by antennas installed at the depot exit and forwarded to the automobile maker as advance information. At the same time, the supplier uses the electronic delivery data to book the shipment out of his own inventory management system. As the truck enters the premises of the car plant, the delivery slip data are already read at the gate by installed antennas and transferred to the incoming-goods system. When the truck is unloaded at receiving, the individual containers are read by an antenna installed at the transfer point. These data are checked with the delivery ship and sent to the inventory management system. The incoming containers are then sent by driverless transport systems to the individual consumption sites. To ensure equipment availability, a security check is made before each transport. When containers arrive at an automated cell, a check is first made of their identity and proper materials before they are cleared for deployment. Deployment continues if the check is positive, the driverless transport system confirms the completed driving order and the quantity of items read by the transponder is booked out of the inventory management system. The use of RFID was able to reduce logistics costs by 15 percent per year. A further reduction of ten percent is expected through further optimized procedures in the process chain. Evaluations made of container cycles have also shown that the exact determination of the number of required containers is capable of reducing investment costs by up to ten percent. [Source: Mose 04]

The automobile industry in particular employs the RFID system OIS-P. OIS-P operates at a frequency of 2.45 GHz. It can read and write data from distances of up to ten meters. Its strong points are its resistance to electromagnetic disturbances, its robust design and the high heat-resistance (235° Celsius) of its data carriers. The data carriers can store up to 32 Kbytes and are preeminently suited for use in automobile production, i.e. bodyshell work, paint coating and final assembly. [Source: Baum 04]

Some manufacturers of sports and racing cars (NITEC, Porsche) also provide transponders on all employed assemblies to ensure complete tracing of all steps in production and quality control as well as to provide controls for guarantee claims. All information relating to every step in production and assembly can be retrieved, and all steps and processing details can be stored and called up when needed. [Source: Euro 04]

RFID systems are increasingly used for optimizing logistics at such transportation hubs as ports or airports. At the Port of Hamburg's Container Terminal Altenwerder (CTA), the loading, temporary storage and onward shipping of standardized containers is already almost completely organized by a computer program. Seven semi-automatic gantry cranes at the quay precisely place the containers on 35 driverless trucks which – directed by transponder – each head for one of the 11 storage blocks. The routes of the automatic vehicles on the CTA premises are planned and controlled by a computer. A close network of transponders embedded in the asphalt continually monitors the position of the vehicles in the area between the quay and storage, which measures 100 by 1,400 meters in size. Nearly 12,000 transponders are to be embedded in the asphalt by the end of 2005 and provide constantly updated position data to a total of 65 computer-assisted, automatic vehicles. [Source: Enge 03]

Another exemplary application in the field of industrial production is being implemented by the computer manufacturer Dell. At its production sites in China, RFID tags are used to control final assembly, installation and packing, as well as the shipping of the computers. This has increased Dell's productivity and – as claimed by Dell itself – boosted its image as an innovative company. [Source: LePh 04]

Thus RFID offers new application opportunities not only in the optimization of supply chains, but also in their monitoring. TK-LOG Tiefkühllogistik, a provider of logistics for frozen food manufacturers, has been participating in a project conducted since the end of 2003 for implementing a RFID-based automated monitoring of the temperature course of goods in the cold chain. Here the course of transit and temperature is to be monitored and controlled for frozen goods from the manufacturer to the supermarket frozen section, thus ensuring the quality of the products. In addition to TK-LOG, project participants include the IT provider massex systemhaus as well as Langnese Iglo and Lupo. Every transport tool, every pallet and every roll container was provided with active RFID transponders with integrated temperature sensors for recording ambient temperatures along the logistics chain to the final transfer of goods to the customers. The plans provide for the transponders to be written with an electronic pallet contents slip at the TK-LOG shipping department and to start temperature recording upon shipping. With the help of an RFID-compatible reader, the product temperatures for each thawing class are simulated on the basis of the recorded ambient temperatures and the observance of the cooling chain confirmed by signature on the electronic display. For incoming goods, mobile RFID readers were chosen to collect the transponder data. The data are visualized for this purpose. [Source: MASS 04]

Sponsored by the Federal Ministry for Economics and Labor, the Cologne University Trade Research Institute (IfH) and the Research Institute for Management and Beverage Logistics (FIM) at the Research and Teaching Institute for Brewing in Berlin are presently studying the prospects of RFID for optimizing the logistics of reusable containers for small and medium-sized firms. Running until June 2005, an analysis will be made of the technical possibilities of using RFID technology in the distribution of returnable crates of a brewery among retailers as well as the redistribution of the empty containers. Most relevant to this commercial field is the multi-accessing of pallets. Another focus of the study was its possible applicability to other classes of goods and trade branches with closed cycles. In the course of the field study, the frequency range of 13.56 MHz was chosen. The rewritable transponders correspond to the ISO-15693 standard and were attached to the beverage crates with individual identification. The maximum distance of the readers was 1.5 meters. Circulation data were collected in a number of central databases. The application operates independently of existing IT systems for merchandise or inventory management. A link to the control system of the bottling line was made only at the brewery. The data of the individual processing points could then be evaluated such that a closed cycle for the beverage crates was produced.

The Fraunhofer Institute for Factory Management and Process Automation (Fraunhofer IFF) has established a testing and development laboratory for RFID technologies at its Magdeburg site. The "LogMotionLab" was opened in June of 2004 and provides industry, commerce and service providers with a wide array of RFID technologies for practical testing. It also presents the possibilities of using RFID technology for monitoring and controlling logistic processes. Interested parties may borrow mobile components from the laboratory upon request. The goal of the laboratory is especially aimed at testing, modifying and finally evaluating the use of RFID technologies on a practical scale, particularly for logistic processes. For that reason, the laboratory also provides two material flow systems which transport goods on a conveyor belt and on metal rollers. Objects fitted with transponders travel along this 15-meter stretch at high speeds and, if necessary, in endurance tests lasting for days. Studies are made, for example, on how much data can still be correctly acquired at what speeds and how transponders react to temperature, vibrations, jolts, chemicals and electromagnetic effects. [Source: Mylo 04]

Total RFID market in trade in countries of the EU 15, in millions of items

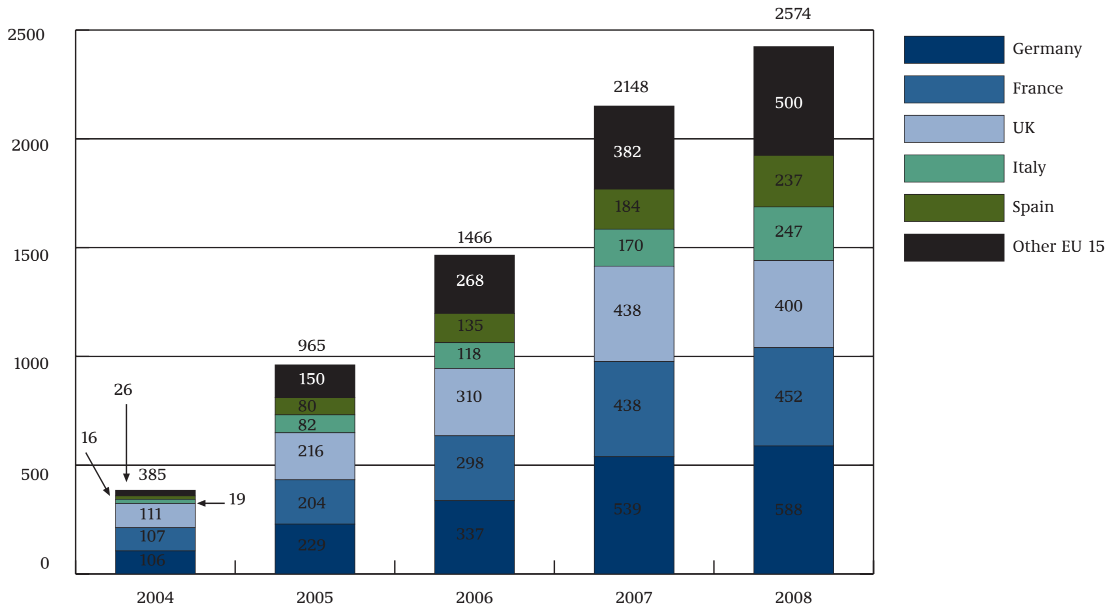


Figure 8 2: Gesamtmarkt RFID im Handel nach Ländern EU 15 [Quelle: Sore 04]

9. Factors facilitating or inhibiting the use of RFID

RFID technology has been used for various experimental purposes for a number of decades and has managed to establish itself in some areas of the marketplace. A variety of new applications are being tested in pilot projects. Depending on the varying surroundings and the general data concerned, the entire spectrum of RFID systems have been employed with varying technological complexity. In the process, a number of facilitating and inhibiting factors can be generalized with respect to their influence on the further spread of RFID applications. RFID systems compete with other automatic identifications systems, such as barcode, OCR and smart cards. The individual procedures differ with respect to the central performance parameters of the Auto ID systems (see Table 9.1.).

Parameter/System	Barcode	OCR	Smart card	RFID
Typical amount of data (byte)	1 ~ 100	1 ~ 100	16 ~ 64k	16 ~ 64k
Data density	low	low	very high	very high
Machine readability	good	good	good	good
Human readability	limited	easy	impossible	impossible
Susceptibility to dirt/liquids	high	high	possible (contact)	none
Influence of (optical) barrier	total failure	total failure	possible	none
Influence of direction and position	slight	slight	very high	none
Wear and tear	limited	limited	limited	none
Procurement costs / auxil. reading devices	very low	Medium	Low	medium
Unauthorized copying or modification	easy	easy	difficult	difficult
reading rate (incl. data carrier operation)	low ~ 4 s	low ~ 3 s	low ~ 4 s	very fast ~ 0,5 s
reading rate (incl. data carrier operation)	0 … 50 cm	< 1 cm (scanner)	direkter Kontakt	0 … 5 m, microwave

Table 9-1: Characteristics of selected Auto ID systems by comparison [Source: according to Fink 02, modified]

The results of the online survey conducted in August 2004 for this study also point to clear differences in the assessment of the relative strengths and weaknesses of Auto ID technologies as compared to barcode, smart card (contact), OCR and RFID. The surveyed experts were asked to evaluate these technologies with respect to the parameters “cost”, “performance”, “cost-benefit ratio”, “reliability” and “information security” ranging from “+2” (clear strength) or “+1” (strength) to “0” (neutral, i. e. neither strength nor weakness) to “-1” (weakness) and “-2” (clear weakness) (see Figures 9-1 to 9-5).

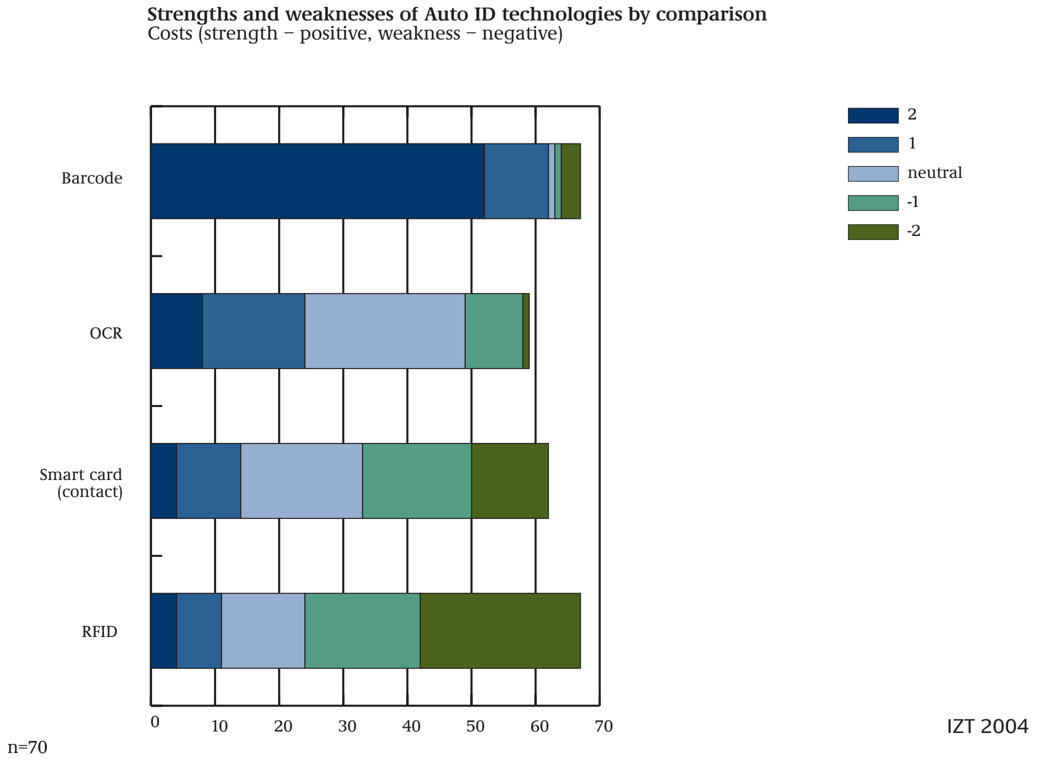
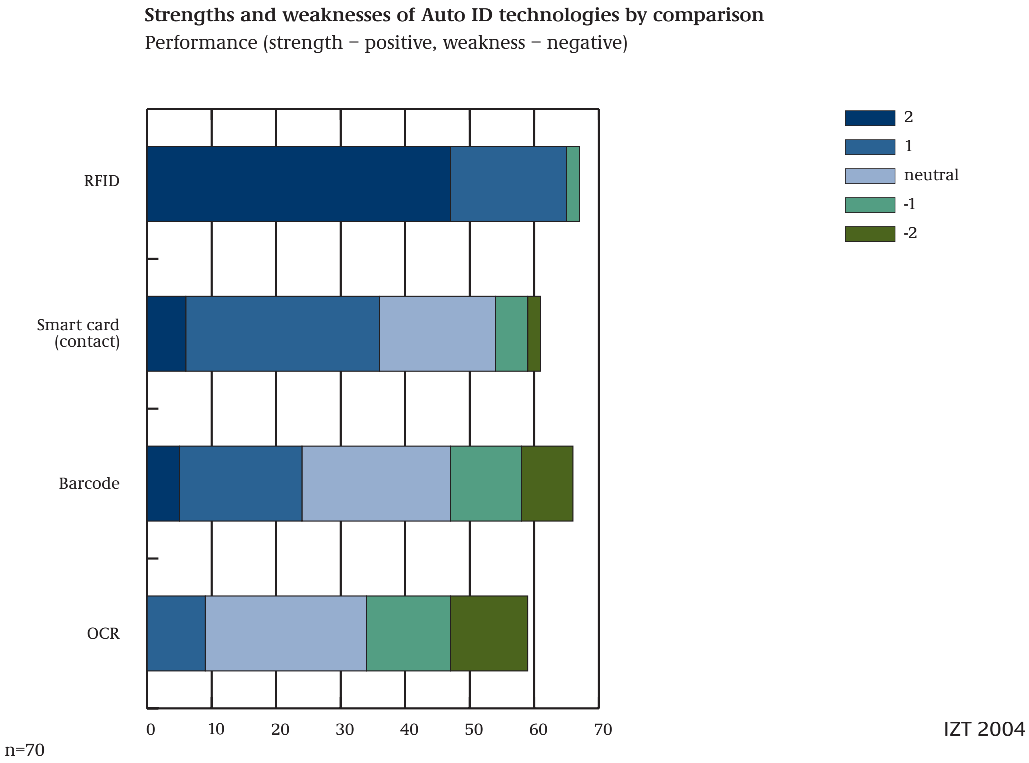


Figure 9-1: Strengths and weaknesses of Auto ID technologies by comparison – Costs

Compared to other Auto ID systems, RFID systems excel above all in their performance, as seen, for example, in the typical quantity and density of data to be processed, the readability of the data carriers and their machine read rate, or even the resistance of the data carrier to such external factors as water and dirt. 93 percent of the surveyed experts assessed the performance of RFID systems as a strength, with at least two-thirds of the respondents (67 percent) rating it as a clear strength (see Figure 9-2).



Strengths and weaknesses of Auto ID technologies by comparison
Performance (strength – positive, weakness – negative)

IZT 2004

Figure 9-2: Strengths and weaknesses of Auto ID technologies by comparison – Performance

RFID systems have the advantage that they require no intervisibility between transponder and reader, and that they are capable of multi-accessing and reading through various materials. Furthermore, some types of transponder can be rewritten a number of times. This gives them a greater range of application compared to barcode technology (e.g. their suitability for the logistics of returnable containers).

Figures 9-4 and 9-5 clearly show that the surveyed experts also regarded functional reliability and information safety as an essential strength of RFID systems in comparison to the other listed Auto ID technologies barcode, contact smart cards and OCR (total strength: 79 and 80 percent, respectively; clear strength: 41 and 30 percent, respectively). It is above all this particular range of performance that encourages the use of RFID systems.

Among the drawbacks of RFID technology are the high costs for procuring and deploying RFID systems, the present low degree of standardization, as well as the uncertainty as to whether corporate users will accept RFID in the future and whether RFID systems can be successfully linked economically and technically with existing data processing systems and structures. Thus, a total of 66 percent of the interviewed experts regarded accruing costs as a weakness of RFID technology, with at least 33 percent viewing it as a clear weakness (see Figure 9-1). Because of the high performance of RFID, its high costs were relativized in the assessment of the cost-benefit ratio. Its cost-benefit ratio was evaluated by 29 percent of the respondents as a weakness and by 11 percent as a clear weakness (see Figure 9-3).

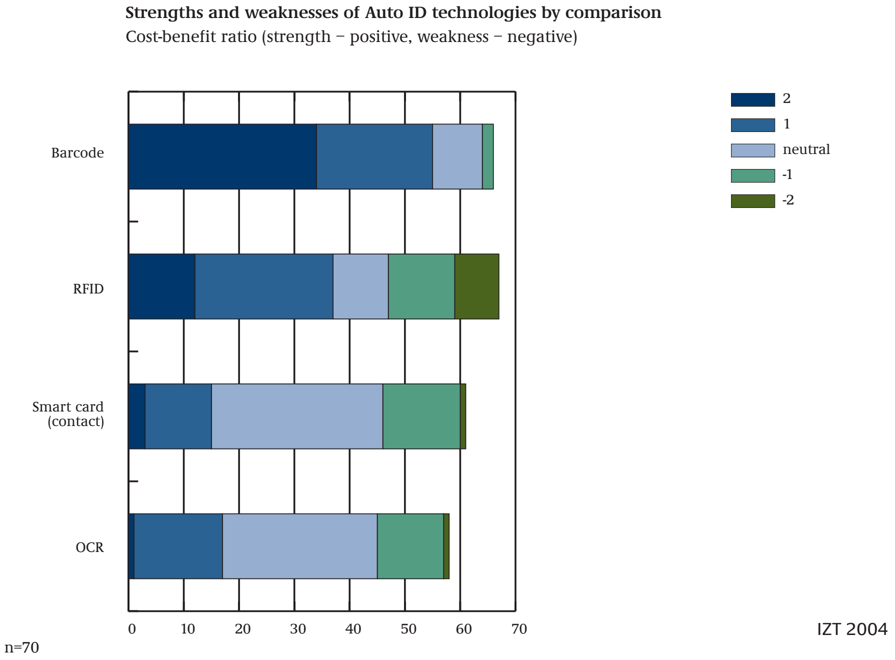


Figure 9-3: Strengths and weaknesses of Auto ID technologies by comparison – Cost-benefit ratio

The strengths of barcode technology, on the other hand, are found primarily in its relatively low costs and favorable cost-benefit ratio. Thus, 89 percent of the surveyed experts evaluated the required deployment costs for barcode as a strength and 74 percent as a clear strength in comparison with smart cards, OCR and RFID (see Figure 9-1). The cost-benefit ratio of barcode was evaluated by slightly more than three-fourths of the respondents as a strength (79 percent), with slightly less than half of those interviewed (49 percent) evaluating it as a clear weakness (see Figure 9-3).

Other advantages of barcode are its relatively high degree of standardization and its high acceptance among users. Among the drawbacks of barcode are its intervisibility requirement, its relative susceptibility to soiling and its inflexibility with respect to subsequent modifications. Nevertheless, the performance of barcode technology was considered a weakness by only 27 percent of the respondents, and a clear weakness by 11 percent (see Figure 9-2).

One feature of OCR systems cited as a significant advantage was the possibility of using optic data collection as a control or in an emergency. The results of the online survey show that in comparison with the other Auto ID technologies, OCR technology was accorded the least overall strength. However, the required deployment costs of OCR technology was evaluated by 59 percent of the respondents as a strength and by 23 percent as a clear strength (see Figure 9-1). Low performance was regarded as the main disadvantage of OCR systems. Thus 36 percent of the respondents evaluated the performance of OCR technology as a weakness and 17 percent as a clear weakness (see Figure 9-2).

One of the advantages of contact smart cards is that the data stored on them can be protected against unwanted (read) access and manipulation. No air interface is required. The test results of the online survey demonstrate that a relatively high degree of information security is attributed to the contact smart card. Thus 64 percent of the respondents evaluated the “information security” parameter of the smart card as a strength, and even 30 percent as a clear strength (see Figure 9-5). The evaluation of the reliability of the contact smart card was also clearly positive in comparison to the other Auto ID technologies on the survey. Over half of the respondents evaluated the reliability of the smart card as a strength (56 percent), with one-fifth (20 percent) of them considering it a clear strength (see Figure 9-4).

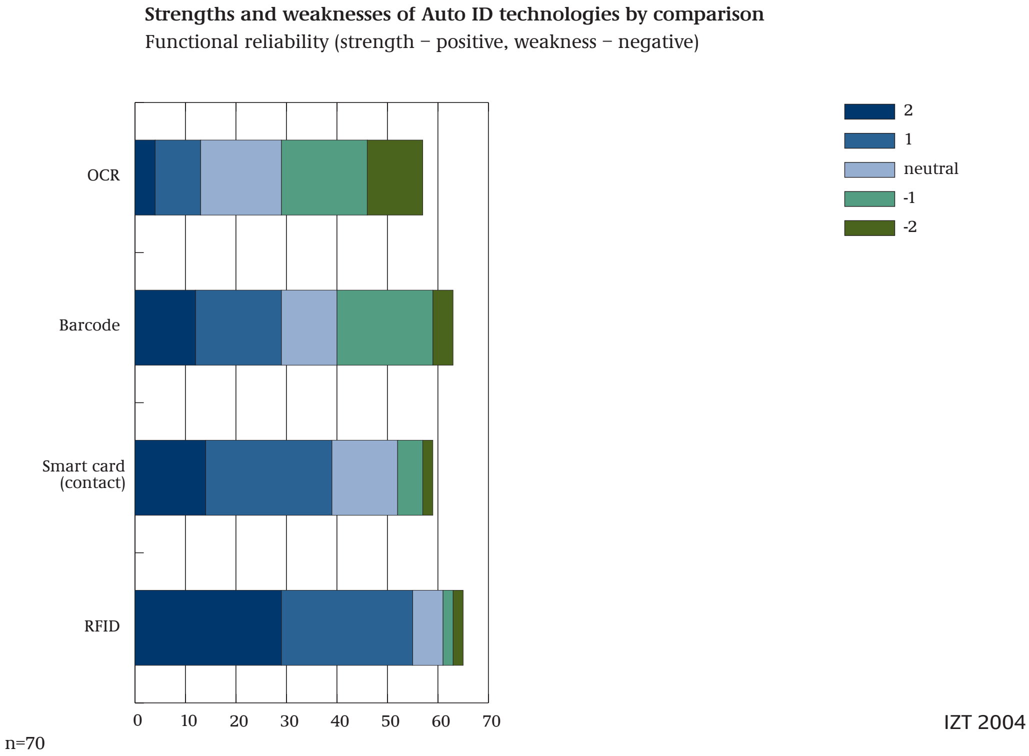


Figure 9-4: Strengths and weaknesses of Auto ID technologies by comparison – Functional reliability

On the other hand, the smart card’s susceptibility to wear, corrosion and soiling was seen as a disadvantage. Above all, frequently used readers and smart cards result in high costs due to failure. In addition, freely accessible readers (e. g. in telephone booths) cannot be protected against sabotage. 41 percent of the surveyed experts evaluated the necessary deployment costs of contact smart cards as a weakness in comparison to the other Auto ID systems, and 17 percent considered such costs to be a clear weakness (see Figure 9-1).

The special functionalities of transponder technology play an essential role in developing its economic potential. High-end transponders in particular offer enhanced opportunities for automation in mass production processes and also feature faster rates of data transfer, which in turn make more complex application possible. Transponder technology can be integrated practically anywhere (e. g. in products, packaging, shipping units, cargo). Its greater memory size, the ability to handle multi-applications and not least user comfort are some of the advantages of contactless RFID systems.

But even underlying economic conditions and legal regulations facilitate the deployment of RFID systems.

Underlying economic conditions

From an economic perspective, tight costs and the competitive pressure in international markets support the wider use of RFID systems. New prospects can be seen above all in those fields and branches of application in which productivity gains are expected through increased automation. The use of RFID increases the overall transparency of the supply chain and cuts down on transaction costs for businesses. But even the increasing integration of markets encourages the use of RFID systems. This use is primarily aimed at developing competitive advantages through the systematic assessment and control of complex logistical relationships in the value creation chain. Last but not least, RFID technology is to support the mass production of products that are specially tailored to customer wishes by having machines adapt automatically to the production requirements at hand (mass customization).

This process involves not only the specification of the finished product but also detailed information on how individual production machines are to be configured to produce this specific product.

Legal regulations

Due to the increasing number of legal regulations affecting a broad range of applications, RFID-based solutions will become more attractive to business. In the wake of EU regulations, they have attracted the keen attention of business players in the fields of logistics and agriculture, including all upstream and downstream phases in the value chain (e. g. traceability of foodstuffs, protection against epidemics). Furthermore, increasingly strict standards regarding quality, safety measures and documentation have accelerated the use of RFID systems in diverse sectors for the maintenance of technical installations (e. g. vital safety components in air conditioning and ventilation systems). The marking of chemical starting materials is also subject to a variety of requirements and has therefore become progressively supported by RFID systems: in addition to the usual product designation and use-by dates common to other branches, legal regulations also stipulate, for instance, notices concerning the hazardous materials, storage and transport, as well as a detail list of ingredients.

In contrast, the widespread use of RFID systems is presently inhibited by the following factors.

Technical problems

Difficulties in RFID-based data acquisition are heightened when conducted in the vicinity of metal or liquids: individual frequency ranges are disrupted and problems arise in the identification of bulk packaging. More than two-thirds of the experts of RFID systems surveyed in this study regarded problems arising in the vicinity of metal or liquids as a “very high” or “high” inhibiting factor, and more than half of them evaluated problems with bulk packaging in the same manner (see Figure 9-6).

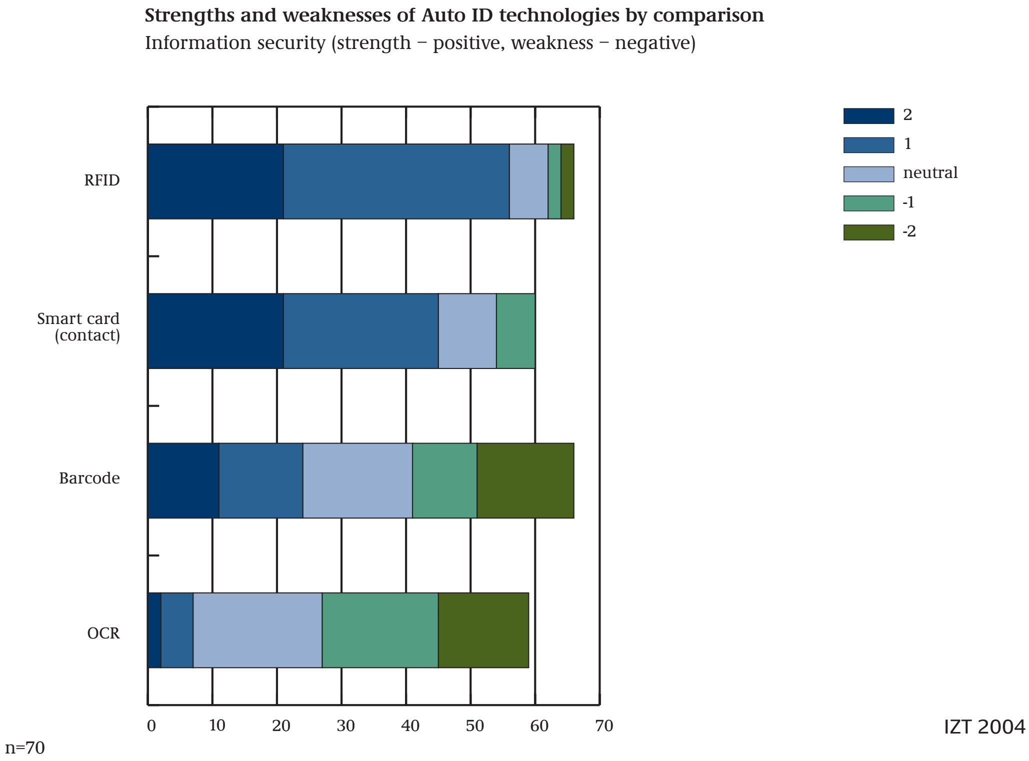


Figure 9-5: Strengths and weaknesses of Auto ID technologies by comparison – Information security

Also cited as inhibiting factors were lengthy readout times of several seconds, shadowing effects between almost identical bursts, as well as radio interference effects and frequency shifts due to the presence of inadvertently placed metal objects. These effects must be selectively reviewed for choosing the right RFID solution.

Insufficient standardization

Although progress is being made in the international standardization of RFID, many sectors still lack international standards, which poses a considerable obstacle to the implementation of industry-wide applications. Worldwide standardization is an indispensable prerequisite for OEMs of hardware and software being able to rely on a dependable technical framework and eliminate present problems faced by users of components from different manufacturers. Against this backdrop, the primary obstacle from an economic standpoint is the lack of standards.

At least 60 percent of those surveyed in this study are of the view that incompatibility problems between transponders and readers of different manufacturers can be expected (see Figure 9-6).

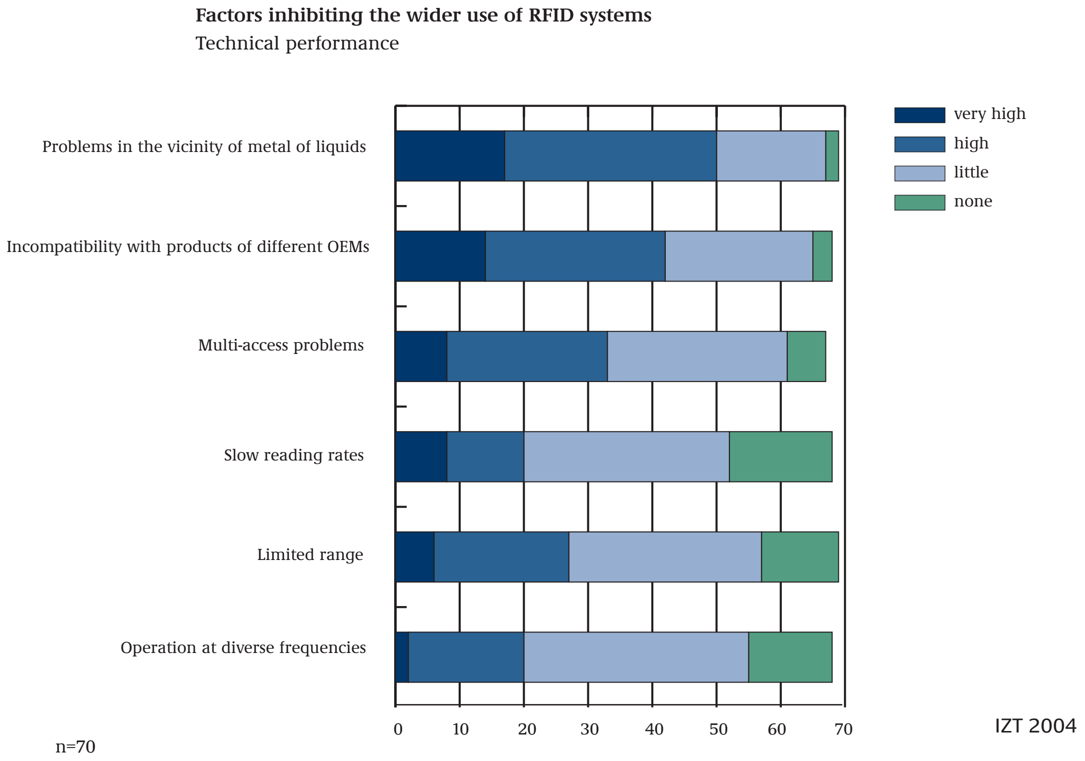


Figure 9-6: Factors inhibiting the wider use of RFID systems – Technical performance

There are a number of separate OEM-dependent solutions on today’s market whose respective software and hardware are in many cases incompatible with other solutions. A similar situation exists in the field of data models: although the Electronic Product Code (EPC) is the preferred cross-industry standard – particularly in North America – standardization in this sector of RFID technology of is not yet complete.

Another related field is the regulation of frequencies. At present, for instance, the goods of multinational corporations must be equipped with transponders operating at different frequency ranges. Although UHF and microwave transponders are gaining in importance, the required bandwidths are not available for commercial use in Japan and in parts of Europe.

Two-thirds of the surveyed RFID experts considered the lack of sufficient harmonization in the area of frequencies and transmission performance to be a high or very high inhibiting factor (see Feature 9-7).

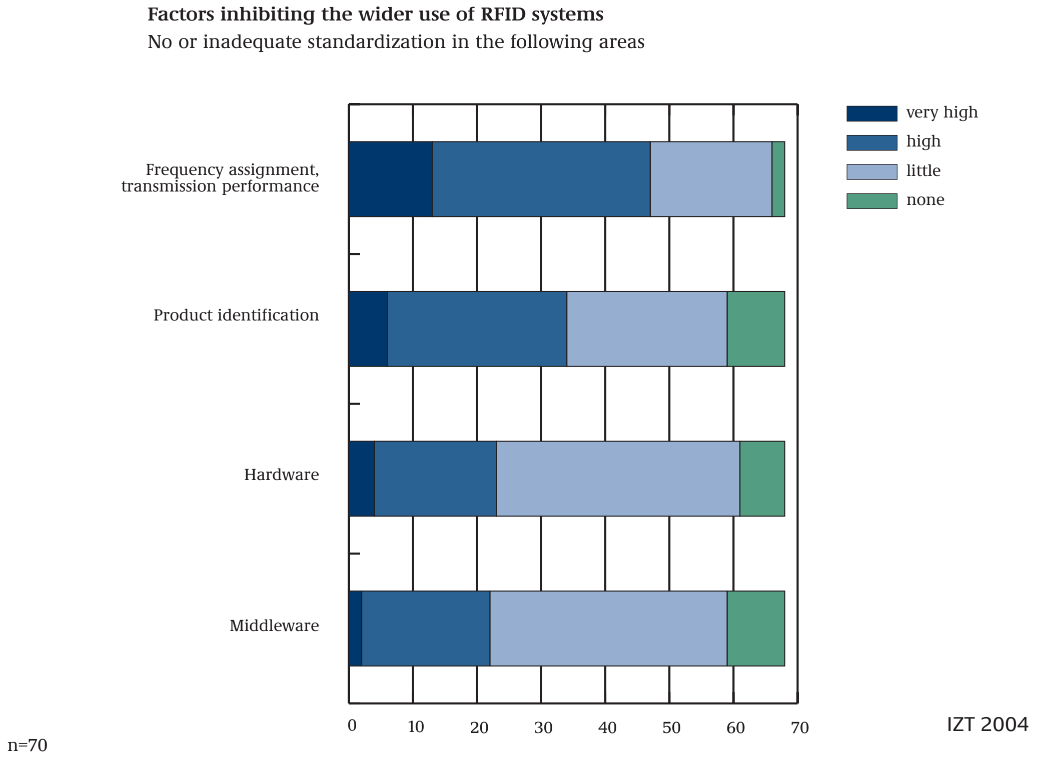


Figure 9-7: Factors inhibiting the wider use of RFID systems –Insufficient standardization

High costs of transponders and FID integration

In 2003 the average price of a transponder, which was partly influenced by relatively low production quantities, was 91 euro cents for a passive HF transponder and 57 euro cents for a passive UHF-RFID transponder [Source: Ward 04]. For many companies, passive transponders will be of no interest until the unit price drops to ten euro cents [Source: Höni 03]. Even though market researchers assume that the price of a passive transponder will drop to well under ten euro cents in the near future, the present high costs per tag continues to inhibit the use of RFID for mass market products [Source: Booz 04].

The procurement costs per transponder and reader were considered by almost a third of the survey's respondents as being the greatest inhibiting factor (29 percent in both cases) on the cost side (see Figure 9-8). In addition to these procurement costs, considerable investments must be made in the infrastructure of the RFID system. These include costs for collecting, processing and evaluating the acquired data as well as for providing an computer network. Added to these are the costs of reorganizing business processes. The start-up phase is typically characterized by a parallelism of RFID and conventional systems. These underlying conditions inhibit the introduction of RFID systems, particularly in small and medium-sized companies which already have an Auto ID system.

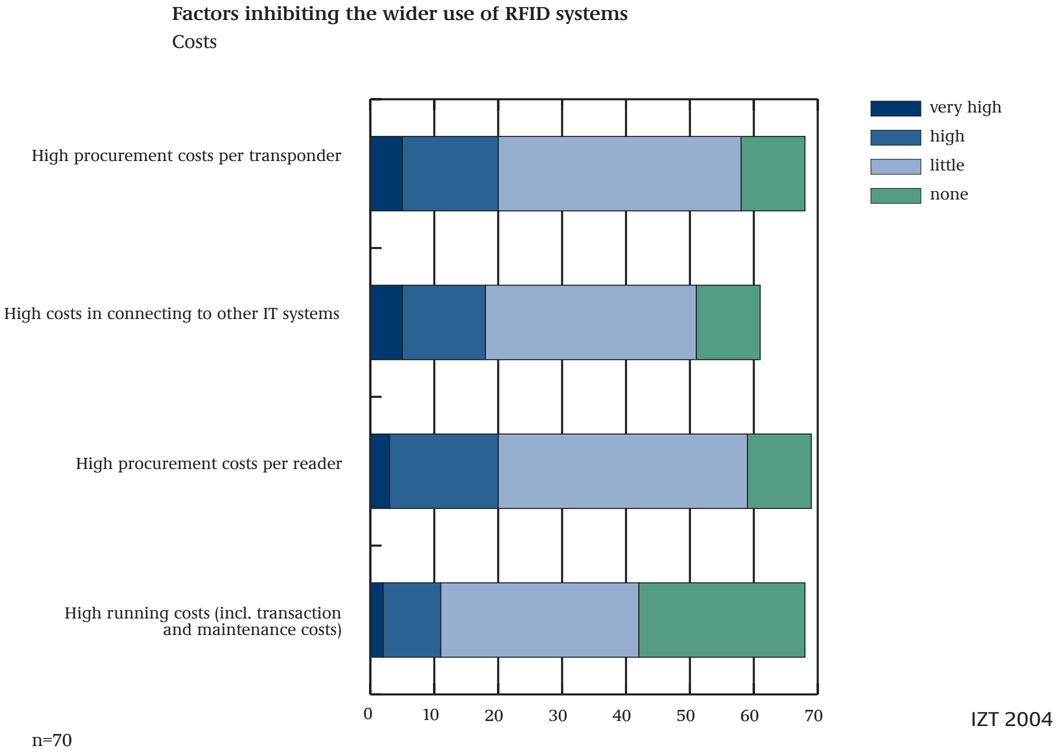


Figure 9-8: Factors inhibiting the wider use of RFID systems – Costs

Information security

RFID systems create a new dimension in providing reliable data on object movements, thus improving the congruency between the virtual world of data and the world of real objects on which the data are based. Economic processes will not only make use of this congruency but will increasingly take it for granted. A logical consequence of this development is the growing dependency of employed processes on the integrity of RFID data. This entails obvious risks which can only be checked by adequate information security. It is difficult at present to access the prospects for ensuring such security, as the future development of RFID remains relatively open.

However, previous experiences in the field of IT security do show that even procedures originally considered quite secure can become insecure in the course of their scientific and technical development due to the discovery of previously unknown gaps. Because of the large investments made in RFID technology, which should be viewed more as an infrastructure than as an individual application, and due to the fact that the essential data carriers (tags) are distributed in great number, subsequent changes to the security protocol of RFID systems will entail very high investment expenditures. In practical terms, they can only be realized when a new generation of the technology is introduced. The latent risk that significant investments in infrastructure could be jeopardized by security problems is thus an inhibiting factor for RFID systems.

Open issues concerning data protection and privacy

The progressive implementation of RFID systems is being keenly followed by the public and mass media and is a topic of controversial discussion. From a social point of view, guarantees of privacy and various aspects of data protection play an ever-increasing role in this controversy (catch-words: “naked customer” or “naked citizen”). Civil rights organizations have published a common position paper on the use of RFID and the associated risks posed to data privacy. [Source: FoeB 04].

The signatory organizations acknowledged that there can be justified interests in the use of RFID on the part of business but, in light of the considerable risks involved, they called for dealers and manufacturers to observe a voluntary moratorium on the use of RFID for consumer goods until all risks were reviewed in a comprehensive technology assessment that would propose possible counterstrategies.

According to the surveyed RFID experts, consumer concerns regarding data privacy were seen by more than a third (36 percent) as a very high or high inhibiting factor (see Feature 9-9).

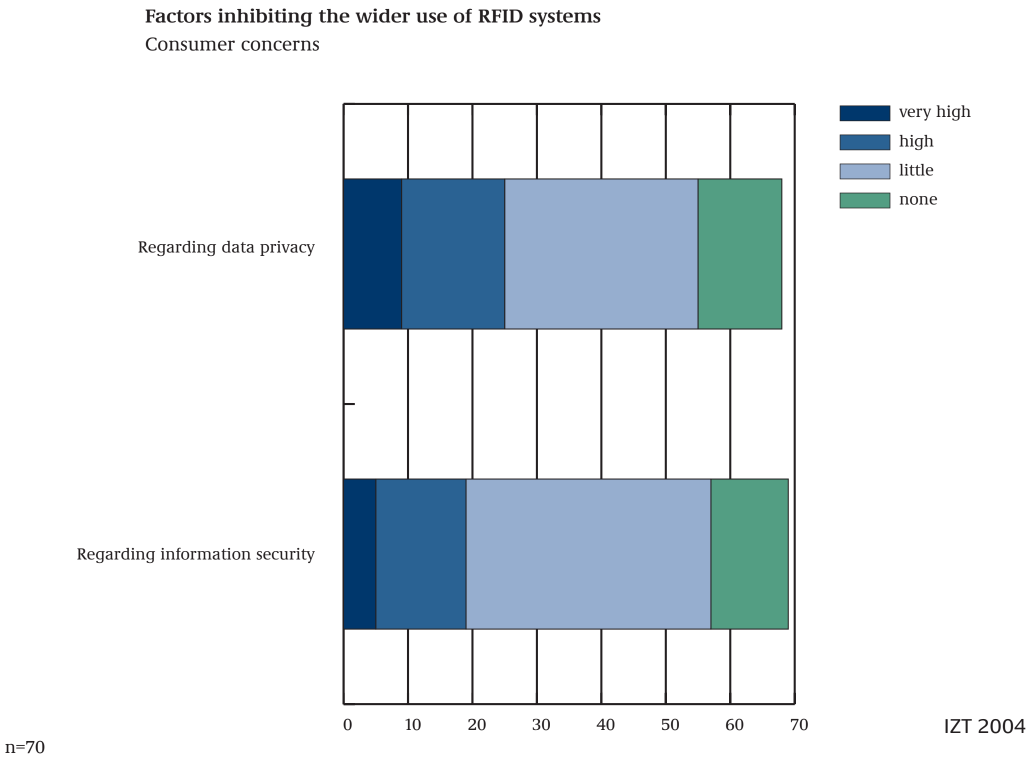


Figure 9-9: Factors inhibiting the wider use of RFID systems –Consumer concerns

Lack of practical knowledge

From an economical point of view, a deficit of practical knowledge is one of the main factors inhibiting the broader use of RFID systems. Thus, poor RFID know-how of companies and the lack of reference solutions were cited by over half of the study's respondents as being a very high or high inhibiting factor (see Figure 9-10.)

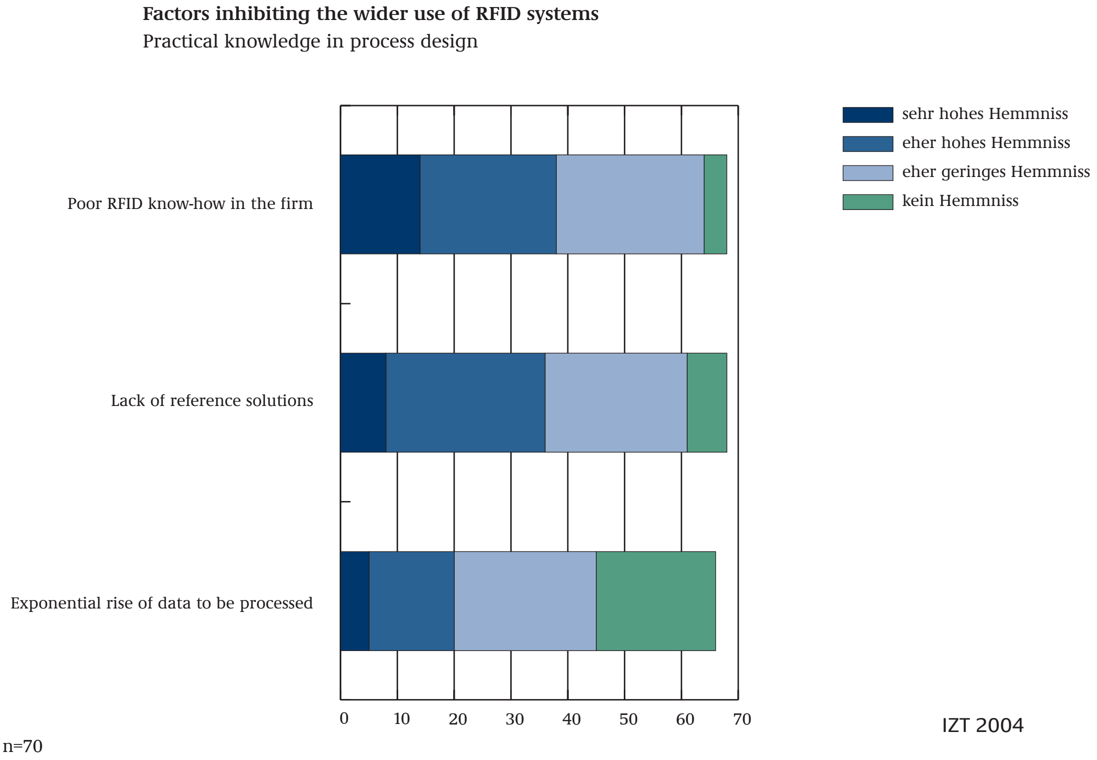


Figure 9-10: Factors inhibiting the wider use of RFID systems –Practical knowledge in process design

10. Development perspectives of RFID technology

10.1 Making the risks visible in the form of fictive cases

10.1.1 Introduction

On the one hand, RFID technology is opening up numerous opportunities for society and business. On the other hand growing risks are connected with broad use of the technology. The economic success of RFID technologies – and that of the companies investing in them – depends inter alia on the extent to which one succeeds in protecting internal data stocks and external communication from data loss and data abuse.

The following fictive cases are intended to make visible possible risks of RFID technology for the time horizon up to 2010 in the selected application contexts of Labelling of Products and Access and Route Control.

They have been put together based on experience in using RFID technology, with a view to showing a spectrum of RFID technologies that is as wide as possible (from low-end to high-end).

The fictive cases are explicitly not to be understood as forecasts. Instead they are intended to help sensitize decision makers for the topic of IT security in the field of RFID innovation, to raise awareness for risks and to motivate the decision makers to analyse and protect information technology systems in companies and organizations in an appropriate way.

10.1.2 Application area Labelling of Products

RFID technology offers great economic potential for identifying products in selected business systems. RFID tags are being uses in more and more objects of daily life. Especially high-value products and ones vulnerable to counterfeiting are being equipped with RFID transponders. Examples include products in the pharmaceutical industry, the automobile industry and the textile and fashion areas. Expansion of the technology will not cover all areas before the Year 2010. The costs of using RFID technology will probably drop moderately; standardization will continue in some areas. RFID technology will not penetrate broad sectors until the Year 2010 as a result of a level of standardization which is still unsatisfactory.

In addition to RFID systems auxiliary applications will continue to expand which are contributing to an expansion of customer-based data stocks. One example of this is the loyalty card which is giving retail companies and large supermarkets comprehensive access to individual customer behavior and which is being accepted by customers for their price incentives.

The continuing spread of RFID technology in the area of identification of products is expanding the possibilities of data collection and processing. Various potential abuses are resulting from this which are hard to monitor due to a lack of transparency. The danger exists that as the labeling of products spreads further, greater correlations will be established between the RFID labels and the customers i.e. users of the products, and stored. This is a topic in the current discussion of data and consumer protection.

Fictive case study no. 1:
Artificial limiting of compatibility and service life

RFID tags have become an integral component of many products in this Year 2010 and cannot be detached from them.

Many devices only accept replacement parts if an authorization code is stored on the RFID. That precaution forces cheap fake replacement parts off the market and increases safety considerably. One example is a reduction in the risk of exploding replacement batteries for mobile phones. The success of this idea has induced other manufacturers as well to use authorization chips in order to differentiate markets better. Large manufacturers of convenience food equip packages with RFID tags bearing regionally different codes, which supply additional information about preparation time and recipes only to microwave ovens of the same region. Packages originating in unauthorized regions (such as Eastern Europe) do not offer this additional function, even if it could be implemented technically.

An even more aggressive intrusion on consumer rights has aroused opposition in parts of the population: shavers, inkjet printers and cameras accept only replacement parts from their respective original manufacturer. One example is washing machines that can only be loaded with pellets which have a proper one-way RFID impressed on them. Foreign detergents are thus not accepted.

Most newly manufactured cars contain an RFID system which automatically monitors the replacement parts (such as tires) for their genuineness and age. These are equipped with RFID tags and some even with sensors. In authorized garages parts that have reached a maximum service life as specified by the manufacturer or whose use licence has expired are recognized and replaced. Only such replacement parts can be installed that have been made by licensed manufacturers. The on-board computer checks and accepts these on the basis of their coded ID. Unless a valid ID is present, the vehicle refuses to function. The manufacturers legitimate their action with safety arguments; but customers cannot verify the action in detail and are forced to trust the manufacturer blindly . One consequence is that RFID tags are dealt on the black market after being taken from accident vehicles whose time limit is not yet expired.

Fictive case study no. 2:
Analysing data traces of objects in court cases

Implementing the Internet of Things has progressed in the Year 2010. This development has made it possible to expand government surveillance as part of criminal proceedings to material objects of everyday life, as used to be possible only in the area of telecommunications back in 2004.

Although the value of such data collections for criminal proceedings has been questioned repeatedly, the analysis of logfiles has taken on an extent unknown until now. In addition to data from telecommunications now data from RFID systems also have to be stored with person-specific data. As a matter of course, data sets from service stations, toll bridges, etc. are used as part of terrorism defence. Besides that, such data are combined with telecommunication data, thus making it possible for the data traces from material objects (such as goods) to be correlated with those of logical objects (such as Internet connections, credit card numbers).

After various changes to the law have been made, practically all operators of open RFID systems are obliged to store the logfiles of all RFID transactions for a long time and to turn them over to the police when requested to do so.

This situation has brought operators of smaller applications into economic problems, because the costs of data management have risen rapidly in recent years, although the direct costs of data storage have dropped.

The development, establishment and maintenance of police information systems cannot keep up with technical RFID developments despite heavy outlays, display inner incompatibilities and are hardly accessible to any effective monitoring by parliament.

10.1.3 Application Area Access and Route Control

Access and Route Control using RFID systems and storage of data in central databases will be widespread by the Year 2010 both in the public, semi-public and corporate areas. Control will spread all the faster because incompatibilities matter less in closed systems.

Especially large companies opening new locations or expanding their existing IT systems in the area of access will decide in favour of an RFID system. In-house RFID-based access and route control is used not only in the incoming area, but also for other functions (such as time management, for break times, access to safety relevant areas on the premises, optimizing processes and thus determining person-specific data for performance monitoring).

Companies are already using the potential of information and communication technologies (ICT) today to monitor the behavior and performance of their employees – even at subcontractors'. The employees are not always informed that ICT are being used to monitor them.

In leisure areas as well RFID systems establish themselves for access control. Although they can be used for route control, this function does not stand in the main focus of interest. Instead it is the rising acceptance of online shopping on the Internet and mobile phones in the area of ticketing and the advantage that tickets can be replaced if lost that act as enablers.

Thus both for the corporate area and the semi-public area RFID-based access and route control opens up an expanded potential for surveillance. A field of tension develops between efficiency and convenience on the one hand and security and data protection on the other.

Fictive case study no. 1:
Surveillance of soccer fans

Tickets for major sport events in the Year 2010 all contain an RFID chip, which automatically lets visitors into the stadium. For one thing, soccer fans are supposed to be relieved of long waiting times at the gate; secondly, black market dealing in tickets is supposed to be counteracted in this way. A central database ensures that if a ticket is lost, a new one can be issued and the old one deactivated.

Correlating the ticket number to a person is done during pre-event sales, and cannot be altered afterwards. Only the recipients of gift tickets have to identify themselves and present an ID when they first enter the stadium.

The stadium is equipped with readers not only at the entrance, but also at all passageways. This activity has been legitimized in the General Terms of Business beforehand. Personal-reference data are transferred to the event organizer, a private security service and the police. The latter has already set up a personalized database during ticket sales and thus is informed at all times about where such persons are in the stadium who are known to the police from earlier events. Any blocks of fans that become conspicuous are dealt with collectively without necessitating that the police carry out any confrontational and expensive person checks.

Innocent bystanders who happen to be near the reader monitoring the conspicuous blocks also get registered.

Fictive case study no. 2:
Performance and behavior monitoring in companies

German labor law requires permission from a company's works council before any technological devices can be used to monitor workers. [The particular basis for this role of the works council in German law is § 87 Abs. 1 Nr. 6 BetriebsVG]

In the Year 2010 the works council agrees to introduction of an RFID system in order to control access to security-relevant areas. At the same time synergy effects are used and the access control system is connected to the time management system in the company. Other functions such as a pay function in the company cafeteria are also integrated. The data obtained on the employees in these ways are brought together. It becomes possible to prove that a worker failed to perform a duty in his/her work agreement by analyzing these data. The collection and evaluation of employee-related data are being done by the company to monitor performance and behavior in violation of the German co-determination law. On the basis of these data an employee is to be fired. The works council agrees to the firing although the data obtained using the RFID system were used to monitor performance and behavior in violation of the German co-determination law. The data can be used in court because the works council knows how the labor law was intentionally neglected and thus agrees to the use of proof obtained in this way and the firing based on it. The situation is even worse among the self-employed who do not benefit from German labor laws in the same way as salaried and wage personnel. Relationships laid down in employment agreements can be suspended or not extended as a result of performance and behavior monitoring using RFID.

[In the German original the details were: Diese Rechtslage bezieht sich nicht auf „arbeitnehmerähnliche Personen“ – „Kleinst-unternehmen“, „Einpersonenfirmen", Scheinselbstständige bzw. „neue Selbstständige“, die sich nicht selten in hoher Abhängigkeit von einem Auftraggeber befinden. Hier gelten nicht einmal die Regelungen des Mitbestimmungsrechts bzw. des Kündigungsschutzes.]

10.2 Expected developments by 2010

10.2.1 Note

The development perspectives of RFID technology are not marked by technological possibilities alone. In addition to technology and standardization one has to remember also market and price development, information security and data protection along with societal outreach.

In the following the future developments in the areas technology and standardization and market and price development are evaluated from the standpoint of experts in the RFID sector. Afterwards the present state of the public discussion will be described in the context of RFID.

10.2.2 Technology and standardization

A continuation of the recent exponential increase in the performance of information and communication technology is to be expected in the coming ten years. In addition to improvement in the price/benefit ratio the technological components used will become dramatically miniaturized. The miniaturization of microelectronics will probably continue for another ten years without a technology shift. It is an important driver of the Pervasive Computing vision. [Source: HBBB 03] Developments in the RFID sector will also be marked by new technologies. Since the end of 2002 Near Field Communication (NFC) has been under discussion for use in RFID systems, with which Sony and Philips intend to establish a wireless networking standard. NFC technology is based on a combination of contactless identification using RFID and wireless connection technology. NFC uses 13.56 MHz and is expected to facilitate networking per Bluetooth or W-LAN with a range of a few centimeters in which end devices identify themselves automatically and establish a data connection. A pilot application developed by Philips for instance makes it possible to sell tickets per Internet in that an advertising poster equipped with an NFC tag contactlessly and automatically sends an Internet address to a PDA or mobile phone held in front of it. Secure transactions and access control and surveillance in buildings are other applications being discussed [Source: HAMM 04]. Together with Nokia, Sony and Philips have founded the NFC Forum [Source: NFC 04a], in order to promote the spread of NFC technology. The new forum is intended to promote the implementation and standardization of NFC technology and to ensure the compatibility between devices and services. [Source: NFC 04b]

According to the opinions of experts in companies and research establishments working in the RFID sector, essential technological factors currently inhibiting the spread and use of RFID systems will be overcome by the Year 2007 or 2010. These inhibiting factors include the low ranges of readers, problems in multi-access identification and recognition across different frequency bands. The greatest skepticism of the experts surveyed concerned the assumption that the existing problems with recognizing transponders near metals or liquids in certain frequency ranges will not be solved by the Year 2010. (see Figure 10-1)

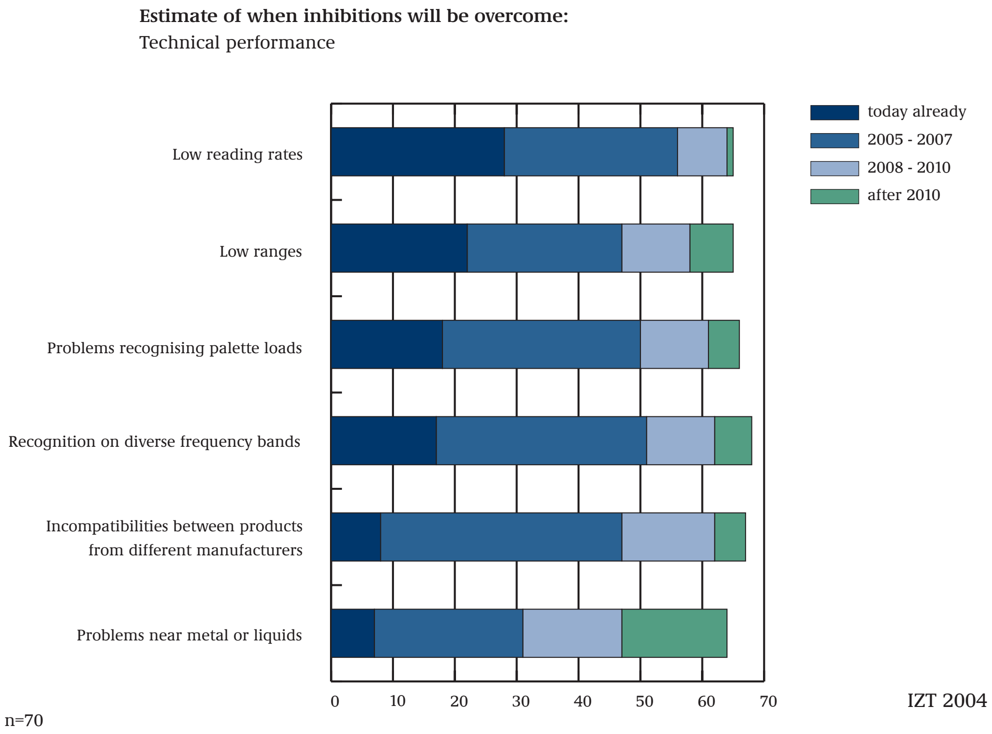


Figure 10-1: Estimate of when inhibitions will be overcome: Technical performance

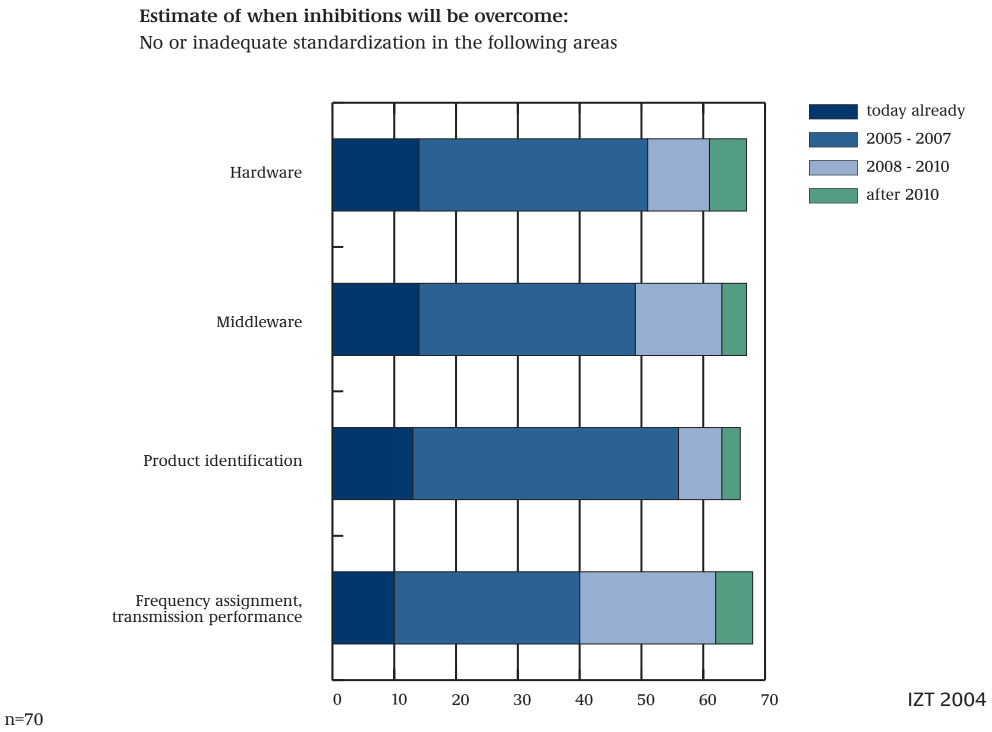


Figure 10-2: Estimate of when inhibitions will be overcome: No or inadequate standardization

10.2.3 Market and price development

The results of our online survey done as part of the present project refer to the Years 2005 to 2010 as a period of overall positive or stable market development for RFID systems in Germany. Thus 43 percent of those surveyed expected a positive development, and 33 percent expected a stable market development (see Figure 10-4). A smaller percentage of those surveyed expected a stagnating market development (3 percent). In the area of the price development of RFID systems as well until the Year 2010 those surveyed were comparatively in agreement: 90 percent of them expected falling prices on the whole (see Figure 10-4). 36 percent of those surveyed expected a rapidly falling price development, whereas 54 percent of those surveyed expected only a slightly falling price development. Due to the importance of costs in investment decisions even a moderate price drop can dampen the further spread of RFID technology considerably.

Estimates as to which application areas RFID systems will continue to expand in are varied. On the long range –- for the years between 2008 und 2010 – more than half of those surveyed in each case assumed that a positive market development will be had in the application areas Surveillance of access, rooms and routes (80 percent), Supply chain: automation, process control and optimization (79 percent), labelling merchandise, objects, animals or persons (73 percent), take-back and multiple-use systems, disposal and recycling (63 percent), and maintenance and repair, recalls (53 percent) (see Figure 10-3).

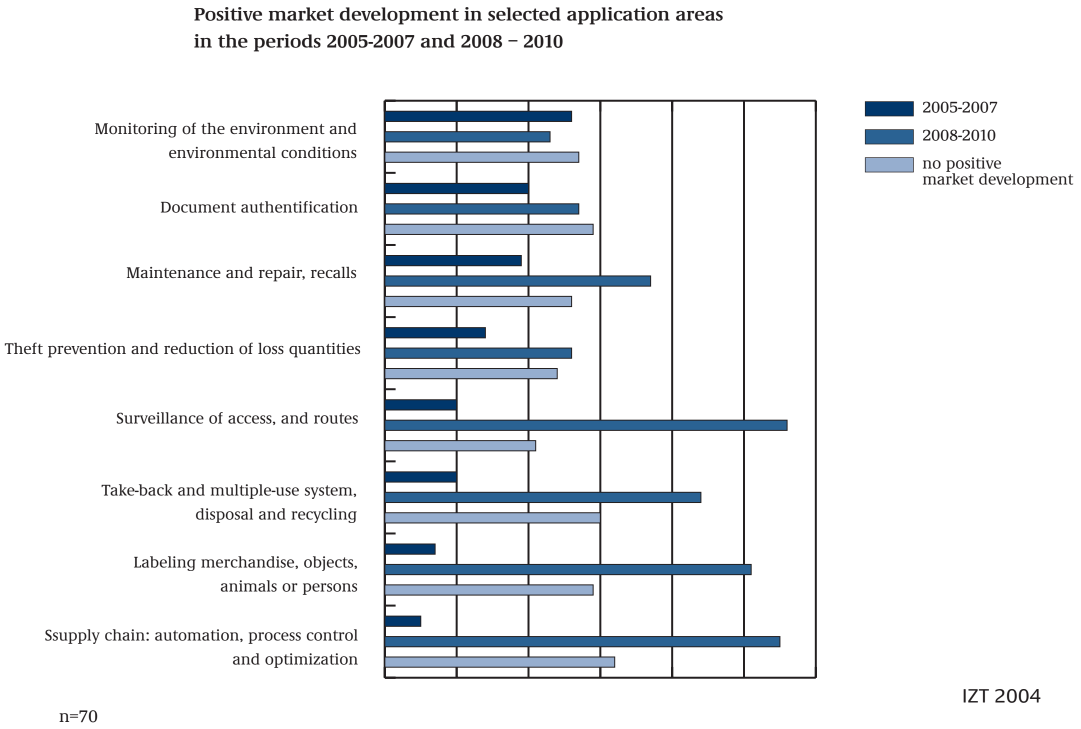


Figure 10-3: Market development of RFID systems in application areas

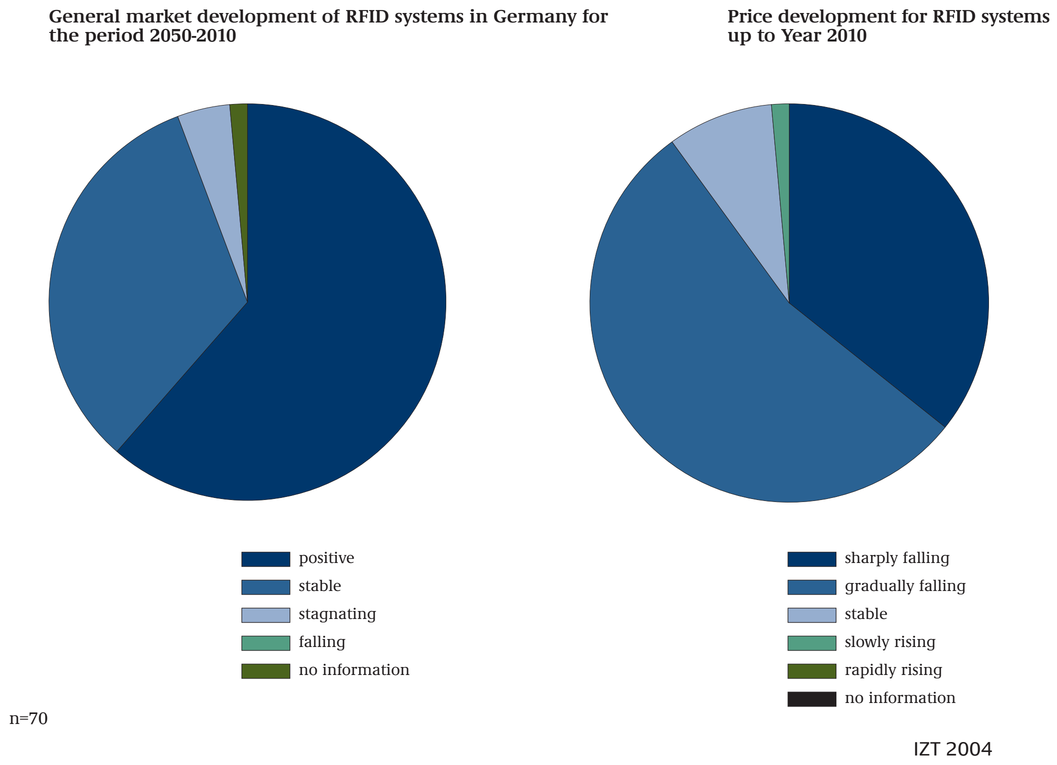


Figure 10-4: **General market development of RFID systems in Germany**

10.2.4 Requirements on information security, data protection and privacy

In comparison to current applications of information and communication technology future applications of Pervasive Computing will be characterized by a great dispersion, spontaneous networking and an increased system complexity connected with the above. At the same time the connections between actions and their consequences will be made less and less transparent by having the functions and services delivered in a networked mode. Therefore the causes of any malfunctions and possible abuses will be more difficult to determine. Future technological systems will become more difficult to manage. The large bandwidth in the technological devices needed for pervasive computing will require more and more individual security solutions (for instance, depending on the device resources being used, on the type of data to be transmitted or the individual use situation). [Source: Lang 04]

As our everyday life becomes more informatized and networked, the dependence on technological background processes rises. It will be a matter of counteracting the increasing unmanageability of technological systems and of increasing the trust of users in RFID technology by making it more transparent.

Thus a radical informatization of our everyday and professional lives with objects that sense part of their environment and communicate with one another also has basic effects on information security and privacy (data protection) in addition to economic potentials.

In the current public discussion of RFID data protection is in the center of interest, whereas concern over information security is playing only a secondary role. Chapters 7.4 and 7.5 on the threats to active and passive parties provide a good impression of the dangers of RFID systems. It becomes apparent there that the threats to information security (input of incorrect data, denial of service attacks) affect primarily the user of RFID systems and thus the active party. These potential threats become real dangers as more and more automatic industrial processes are introduced. Input of incorrect data into

RFID systems and manipulating the correct functioning of RFID systems can have great effects on the orderly continuation of production processes, and thus great business losses.

In the case of the passive party – the customer or employee of an operator of an RFID system – it is primarily the data privacy and location privacy that are threatened by the use of RFID systems. The Web Services WAN Special Interest Group set up by the Auto-ID Center of the Massachusetts Institute of Technology (MIT) suggests that this threat is a real danger, and is working on a prototype for a standard architecture. [Source: Robe 04] This architecture lets as many interested persons as desired have access in real time to data generated by reading RFID labels. RFID systems intrude upon a special aspect of the [German] General Law to One’s Personality – the right to determine information about one’s self – to determine the release and use of one’s personal data oneself. Future technical facilities will let data be collected, processed and used beyond the purpose originally anticipated not only by the state but also by non-public entities such as private-sector companies.

The regulations of current data protection law refer to person-specific data. The term person-specific data also includes data that can be referenced to persons. In an expertise written for the Federal [German] Ministry of the Interior, Messrs Roßnagel, Pfitzmann and Garstka draw the conclusion: In a future world of networked and ever-present data processing there will be an increasing number of cases in which data – such as URLs or other identifiers – are processed for which at the time it is not known whether they refer to certain persons (example: URLs), or which persons they refer to (example: Globally Unique Identifiers - GUID) or with which persons they might be associated in the future (example: RFID-Tags). Even when the data do not yet qualify as person-specific data, the principles of avoiding the personal reference, being necessary and obtained for specific purposes should still be applied due to the the precautionary principle whenever it can be expected that the personal reference will be established or could be established. [Source: RPG 01]

On the basis of RFID systems data can be collected for a rainy day . Then an idea of the context can be generated using a variety of variables which escapes the control of data protection due to the heterogeneity and large number of components involved. Mattern and Römer speak of a paradigm shift: Whereas one used to process data in EDP, now one identifies the physical phenomena themselves automatically, online and in real time, as is becoming possible to a larger extent, making possible a wholly new quality of results. [Source: MaRö 03 and ECPS 02]

On the basis of RFID systems data can be collected for a rainy day . Then an idea of the context can be generated using a variety of variables which escapes the control of data protection due to the heterogeneity and large number of components involved. Mattern and Römer speak of a paradigm shift: Whereas one used to process data in EDP, now one identifies the physical phenomena themselves automatically, online and in real time, as is becoming possible to a larger extent, making possible a wholly new quality of results. [Source: MaRö 03 and ECPS 02]

Against this background the requirement of data economy and the requirement that data be collected only for specified purposes are to be seen as essential criteria for the future preservation of the right to privacy. As RFID technology continues its advance, the question arises as to who can determine or is allowed to determine whether and which information is associated by electronically empowered things. Finally one should also remember that in an informatized world the correct functioning of information technological infrastructure can become a matter of life and death for society and the individual. The advancing miniaturization of technological systems gives one reason to fear that existing legal prohibitions will no longer be monitorable or enforceable as RFID systems advance. Therefore solution strategies must be developed for these cases.

According to the Federal German Data Protection Report there are in principle no objections to the use of RFID systems, as long as their introduction takes place on a legal basis and while observing the data protection regulations: It is legitimate to use the new technical developments. However at the same time technical monitoring systems and a surveillance structure are being established which, once they are in place, could be used for quite different purposes and whose legal and data protection compliant use is ultimately no longer ascertainable. Here again it becomes apparent that the sum of useful and data protection compliant applications on the whole represents a potential threat to the basic right to determine information about one’s self, which is not yet being perceived as such by those affected nor in society’s political discussion [Source: BuDa 01/02]

In order to use the opportunities of RFID and at the same time to keep the threats as small as possible, it will be a matter of implementing the principles of modern data protection laws, data economy and the most rapid possible anonymization or pseudonymization of personal referenced data in RFID systems early in the design process and in market introduction.

10.2.5 Social acceptance

Future developments in the area of pervasive computing and RFID technology have effects on many areas of one’s personal, professional and public life. Therefore one asks about the social acceptance of the new technologies. One prerequisite of assessing the opportunities and risks of pervasive computing and RFID technology in such a way that is objective and can be understood by the individual is that society be given open, objective and comprehensive information.

The media are very important for public and individual perception and communication of technology-related opportunities and risks. The have not only the role of information suppliers, but also a central function as information collectors and reinforcers. It is the resonance in the mass media that gives social acceptance to a potential opportunity and social and political hotness to a potential risk. [Source: Büll 03]

The media have begun to pay more attention to RFID systems in recent years. Specialized media – depending also on how important RFID is to the particular sector – have been reporting on it quite intensively. Even in the press aimed at a wider public, a number of reports with quite critical or even negative headlines have been published (for example, RFID - The Inquisitive Chip in your Yoghurt Cup and Satan’s Work or the Next Step into a Digital World?). Since the possible effect of RFID systems are particularly comprehensive in the retail sector, privacy thoughts and data protection aspects are playing an increasingly important role in the media deliberations. An empirical analysis of the media has not been done, but could provide information about how the information and communication about the opportunities and risks of RFID technology has been dealt with in the mass media and relevant specialized media. Therefore it cannot be determined with any certainty whether in the media reporting and in public communication certain subtopics and problems in the context of RFID systems have been classified either as important or as unimportant.

The question as to how enthusiastically and fast social groups have opened themselves to RFID technology or how slowly or indifferently they will react to future developments is difficult to estimate. In the debate about the opportunities and risks of RFID technology two opposing positions are crystallizing:

whereas on the one hand the opportunities are seen which result from use of RFID, on the other hand it is the risks, threats and limitations that are seen.

From the point of view of consumers the potential utility of RFID systems for them is to get greater security and more convenience in everyday situations. From this standpoint, one can expect a lot of social acceptance of RFID systems to result. This is confirmed by the fact that there are already products that enjoy social acceptance and demand (loyalty cards, RFID-based ski passes). Apparently the utility that consumers get in such cases is more important than is the fear of intrusions into one’s private sphere. Existing research findings point in this direction that applications based on information and communication technologies are only accepted when they offer a considerable added value. Therefore the question of balancing opportunities and risks is at the center of social discussion and acceptance for each individual RFID application.

The population today uses and accepts many technologies and applications that related to RFID in the areas of advertising and market and opinion research to produce comprehensive customer profiles on the basis of new procedures. More and more customer data are being collected and evaluated. Methods of data mining are being used. Incentive systems of businesses induce consumers to regularly deliver more and more data. According to an analysis done by Emnid, for example, loyalty cards are have become the most important card in the pockets of a large percentage of the German population, ranking right after their health insurance and ec bank cards. In March of 2002 more that half of all Germans had at least one loyalty card; in Great Britain it was even more than 86 percent in 2003. [Source: Scha 04] Many consumers are apparently willing to reveal their buying behavior for discounts of less than one percent of the merchandise value and to have it analysed for purposes of market research and for making them special individualized offers. [Source: Lang 04]

On the other hand, RFID systems in the context of pervasive computing have to be regarded as a bundle of innovations that will bring fundamentally new things and surprising applications. However it is still basically an open question as to which social needs and inhibitions will exist in the future. One has to remember that the number of doubting voices is increasing in some parts of the population which see data protection and privacy in danger if RFID is to advance further. Consumer organizations have called to boycott companies that are using or promoting RFID technology. Marc Langheinrich writes: RFID tags or smart labels have mobilized fears in the population, as no other technology of ubiquitous computing ever has, of living in a surveillance state in the near future. [Source: Lang 04]

Since in a modern, differentiated society a variety of different sized interest groups exists, some of which are in competition with one another, it will be important for future developments to reflect the pluralism of these opinions in an appropriate ratio in the field of RFID. One should create more transparency in the discussion of RFID in the individual groups of actors. That would be a central step toward making the discussion more objective, and social opinion formation could be improved by more objectivity.

11. Abbreviations

AIM:	Association for Automatic Identification and Mobility"
BSI:	Bundesamt für Sicherheit in der Informationstechnik
CRC:	Cyclic Redundancy Check
DRAM:	Dynamic Random Access Memory
EAS:	Electronic Articel Surveillance
EEPROM:	Electrically Erasable Programmable Read Only Memory
EMPA:	Eidgenössische Materialprüfungs- und Forschungsanstalt
EPC:	Electronic Product Code
EPROM:	Erasable Programmable Read Only Memory
EU:	European Union
FoeBuD:	Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs
FRAM:	Ferroelectric Random Access emory
GHz:	Gigahertz
GUID:	Globally Unique Identifier
HF:	High Frequency
ICT:	Information and Communication Technology
IP:	Internet Protocol
ISO:	International Organization for Standardization
IZT:	Institut für Zukunftsstudien und Technologiebewertung
kHz:	Kilohertz
LF:	Low Frequency
MHz:	Megahertz
NFC:	Near Field Communication
OCR:	Optical Character Recognition
ONS:	Object Name Service
PLM:	Product Lifecycle Management
PML:	Procedural Markup Language
RAM :	Random Access Memory
RFID:	Radio Frequency Identification
ROM:	Read Only Memory
SRAM:	Static Random Access Memory
TA-SWISS:	Zentrum für Technologiefolgen-Abschätzung beim Schweizerischen Wissenschafts- und Technologierat
UHF:	Ultra High Frequency
USA:	United States of America
VIBE!AT:	Verein für Internet-Benutzer Österreichs
W-LAN:	Wireless LAN
XML:	Extensible Markup Language

12. Bibliography

[Source: ACG 04:]
ACG IDENTIFICATION TECHNOLOGIES GMBH, http://www.acg.de, Abruf vom 02.07.2004

[Source: AdHö 04:]
AUF DEM HÖVEL, J.: Smarte Chips für die Warenwelt. In: Morgenwelt – Magazin für Wissenschaft und Kultur vom 4.06.2004, http://www.morgenwelt.de/418.html, Abruf vom 12.07.2004

[Source: aid 04:]
AID INFODIENST, VERBRAUCHER- SCHUTZ, ERNÄHRUNG, LANDWIRTSCHAFT E. V.: Neue Kennzeichnungsvorschriften für Schafe und Ziegen, http://www.aid.de/downloads/ER_Kennzeichnungsvorschriften.pdf, Abruf vom 15.07.2004

[Source: AOLm 04:]
AOL MEMBER BEREICH: Lachs-Rennen in Schweden. http://members.aol.com/vhsf/lachrenn.htm, Abruf vom 04.08.2004

[Source: ArKo 04:]
ARBEITSKREIS KONTAKTLOSE CHIPKARTENSYSTEME FÜR ELECTRONIC TICKETING E. V. (KONTIKI): Feldversuche E-Ticketing im ÖPV, http://www.kontiki.net/deutsch/index_dt.html, Abruf vom 09.08.2004

[Source: ATKe 04:]
A.T. KEARNEY: RFID spart dem deutschen Einzelhandel sechs Milliarden Euro pro Jahr. Nutzen für Händler – Kosten für Hersteller, Pressemitteilung vom 08. März 2004, http://www.atkearney.de/content/veroeffentlichungen/pressemitteilungen_ detail.php/id/49046, Abruf vom 14.7.2004

[Source: Auto 02 :]
AUTO-ID CENTER: 860 MHz – 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification. Auto-ID Center /EPCglobal, Cambridge, MA, USA. verfügbar unter: www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf. (16.07.2004)

[Source: Auto 03:]
AUTO-ID CENTER: 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification. Auto-ID Center/EPCglobal, Cambridge, MA, USA. verfügbar unter: www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf. (16.07.2004)

[Source: Auto 03b:]
AUTO-ID CENTER (2003) Technical Report: 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Recommended Standards, Version 1.0.0, http://archive.epcglobalinc.org/publishedresearch/mit-autoid-tr011.pdf, Abruf vom 09.09.2004

[Source: Baum 04:]
BAUMER IDENT: Branchenlösungen Automobilindustrie. http://www.baumerident.com/deutsch/4_branchen/automobil.htm, Abruf vom 15.07.2004

[Source: BCLM 03:]
BOHN, J., COROAMA, V., LANGHEINRICH, M., MATTERN, F. und ROHS, M.: Allgegenwart und Verschwinden des Computers – Leben in einer Welt smarter Alltagsdinge. In: GRÖTKER, RALF (Herausgeber): Privat! Kontrollierte Freiheit in einer vernetzten Welt. Heise-Verlag, 2003. http://www.inf.ethz.ch/vs/publ/papers/allvercom.pdf, Abruf vom 19.08.2004

[Source: Biob 04:]
BIOBOARD.DE. DAS FORUM FÜR BIOLOGIE: Kostenlose Hilfen für Biologie. http://.www.bioboard.de, Abruf vom 03.07.2004

[Source: Booz 04:]
BOOZ ALLEN HAMILTON in Kooperation mit der UNIVERSITÄT ST. GALLEN: RFID-

Technologie: Neuer Innovationsmotor für Logistik und Industrie?, http://www.boozallen.de/content/downloads/5h_rfid.pdf, Abruf vom 19.07.2004

[Source: Borc 04a:]
BORCHERS, D.: Reisepass mit Transponder. In: Heise Online vom 19.03.2004, http://www.heise.de/newsticker/meldung/45780, Abruf vom 18.07.2004

[Source: BORC 04b:]
BORCHERS, D: Holland testet Biometrie im Pass. In: Heise Online vom 02.07.2004. http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48809, Abruf vom 18.07.2004

[Source: BSI 03:]
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI in Kooperation mit der TECHNISCHEN UNIVERSITÄT MÜNCHEN UND DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN: Kommunikations- und Informationstechnik 2010+3 – Neue Trends und Entwicklungen in Technologie, Anwendungen und Sicherheit. Secu Media Verlag: Ingelheim.

[Source: Buch 04:]
BUCHHOLZ, T.: RFID-Technologie zur Identifizierung von Hunden. In: Logistik Inside vom 19.2.2004, http://www.logistikinside.de/sixcms4/sixcms/detail.php/69876/de_news, Abruf vom 06.07.2004

[Source: BuDa 01/02:]
BUNDESBEAUFTRAGTER FÜR DEN DATENSCHUTZ: Tätigkeitsbericht 2001 und 2002 des Bundesbeauftragten für den Datenschutz. 19. Tätigkeitsbericht. Über: Bundesdaten-schutzbericht: http://www.bfd.bund.de/information/19tb0102.pdf, Abruf vom 11.06.2004

[Source: Büll 03:]
BÜLLINGEN, F.: Elektrosmog durch Mobilfunk? Akzeptanz und Risiko im Licht der öffentlichen Debatte. In: Aus Politik und Zeitgeschichte (B 42/2003), http://www.bpb.de/publikationen/9EP0Y6,1,0,Elektrosmog_durch_Mobilfunk.

html, Abruf vom 22.08.2004

[Source: CCG 03:]
CENTRALE FÜR COORGANISATION GMBH (CCG) (HRSG.): „RFID – Optimierung der Value Chain – Einsatzbereiche, Nutzenpotenziale und Herausforderungen“, Managementinformation Mai 2003

[Source: CMBC 03:]
CLEMENTS, B., MAGHIROS, I., BESLAY L., CENTENO, C., PUNIE, Y., RODRÍGUEZ, C., MASERA, M.: Security and privacy for the citizen in the Post-September 11 digital age: A prospective overview. Über: http://www.jrc.es/home/ publications/publication.cfm?pub=1118, Abruf vom 12.05.2004

[Source: Com 04a:]
Wal-Mart treibt RFID-Nutzung voran. In: Computerwoche vom 19.05.2004: http://www.computerwoche.de/index.cfm?pageid=254&artid=61149, Abruf vom 2.07.2004

[Source: Com 04b:]
Metro eröffnet RFID-Zentrum. In: Computerwoche vom 08.07.2004:, http://www.computerwoche.de/index.cfm?pageid=254&artid=62890, Abruf vom 13.7.2004

[Source: Comp 04c:]
Schinken an Zentrale: „Bin reif“. In: Computerwoche Online: CW-EXTRA Nr. 01 vom 15.02.2002 Seite 12-13, http://www1.computerwoche.de/heftarchiv/ 2002/20020215/a80106467.html, Abruf vom 04.07.2004

[Source: ComW 04:]
Preismanipulation bei RFID-Transpondern. In: Computerwelt, http://www.computer welt.at/detailArticle.asp?a=84374&n=4, Abruf vom 12.08.2004

[Source: DrLi 04:]
DRÄGER & LIENERT: TagIt Informationsmanagement. http://dlinfo.de/tagit.htm, Abruf vom 12.07.2004

[Source: EC 95:]
EUROPEAN COMMISSION: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, November 1995.

[Source: ECIN 04:]
ECIN: Fußball-WM 2006 baut auf RFID. In: Ecin.de, http://www.ecin.de/news/2004/ 01/16/06623/, Abruf vom 05.08.2004-08-09

[Source: ECPS 02:]
ESTRIN, D., CEILLER, D., PISTER, K. UND SUKHATME, G.: Connecting the Physical World with Pervasive Networks. IEEE Pervasive Computing, 1 (1): 59-69.

[Source: ECR 04:]
EFFICIENT CONSUMER RESPONSE INITIATIVE DEUTSCHLAND ÖSTERREICH UND SCHWEIZ (ECR D-A-CH): Rückverfolgbarkeit von Lebensmittel und Warenrückruf. http://www.ecr.de/ecr/award/e21/e24/e307, Abruf vom 20.07.2004

[Source: Enge 03:]
Engelhardt, Torsten: Der Hamburger Hafen. In: GEO 11/2003.

[Source: EPC 04:]
EPCGLOBAL INC.: http://www.epcglobalinc.org, Abruf vom 19.07.2004

[Source: EPCG 04:]
CCG-Expertenrunde „RFID/EPC“ nimmt Arbeit auf, In: EPCGlobal vom Juni 2004, http://www.epcglobal.de/ccg/Inhalt/e56/e131, Abruf vom 19.07.2004

[Source: Euro 03:]
EUROPÄISCHE KOMMISSION: Überwachung aller Nutztiere in Europa durch elektronische Markierung, In: Innovationsreport 2003, Forum für Wissenschaft, Industrie und Wirtschaft, http://www.innovationsreport.de/html/berichte/agrar_forstwissenschaften/ bericht-18194.html, Abruf vom 14.07.2004

[Source: Euro 04:]
EURO I.D. IDENTIFIKATIONSSYSTEME, RF-IDENTIFIKATION: Für eine runde Lösung mit System, Anwendungen in der Transponder-technologie, http://www.euroid.com, Abruf vom 02.07.2004

[Source: FiKe 04:]
FINKE, T., KELTER, H.: Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. BSI, http://www.bsi.de/fachthem/ rfid/Abh_RFID.pdf, Abruf vom 12.10.2004

[Source: Fink 02:]
FINKENZELLER, K.: RFID-Handbuch. Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. 3. aktualisierte und erweiterte Auflage, Hanser Fachbuchverlag, Oktober 2002, Wien. http://www.rfid-handbook.de

[Source: FiRo:]
FISHKIN, K.P. UND ROY, S.: Enhancing RFID Privacy via Antenna Energy Analysis. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, MA, USA.

[Source: Flei 01:]
FLEISCH, E.: Was bringt die nächste Technologiewelle? Wenn Dinge denken lernen... http://www.m-lab.ch/pubs/ Akzente_01efl.pdf, Abruf vom 11.07.2004

[Source: Flei 04:]
Die Ohrmarke bekommt elektronische Konkurrenz. In: fleischwirtschaft.de vom 03.02.2004,

http://www.fleischwirtschaft.de/dokumentation/onlinearchiv/pages/show.prl?params=keyword%3DITeK%26all%3D%26type%3D1%26laufzeit%3D0&id=4454&currPage=1, Abruf vom 10.07.2004

[Source: Fleis 04:]
FLEISCH, .E.; HALLER, S.; STRASSNER, M.: Regal ruft Palette. In: SAP Info vom 16.12.2002. http://www.sap.info/public/de/article.php4/Article-49043df892f123d88/de, Abruf vom 04.08.2004

[Source: FoeB 04:]
VEREIN ZUR FÖRDERUNG DES ÖFFENTLICHEN BEWEGTEN UND UNBEWEGTEN DATENVERKEHRS E. V. (FOEBUD): Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, http://www.foebud.org/rfid/positionspapier#1, Abruf vom 12.08.2004

[Source: FrSt 04:]
FREY, H. und STURM, P. (Universität Trier): UBICOMP Episode 14. http://www.syssoft.uni-trier.de/systemsoftware/Download/Sommersemester_2004/Vorlesungen/Ubiquitous_Computing/14%20RFID.pdf

[Source: FSL 04:]
FLOERKEMEIER, C., SCHNEIDER, R., LANGHEINRICH, M.: Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols. 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), Tokyo, Japan, November 2004 http://www.vs.inf.ethz.ch/publ/papers/floerkem2004-rfidprivacy.pdf Abruf vom 09.09.2004

[Source: FSL 04:]
FLOERKEMEIER, C.; SCHNEIDER, R. und LANGHEINRICH, M. (2004): Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols, Institute for Pervasive Computing ETH Zurich, Switzerland, http://www.inf.ethz.ch/~langhein/articles/

[Source: GCIB 03:]
GLOBAL COMMERCE INITIATIVE/IBM: Global Commerce Initiative EPC Roadmap Executive Brief, Published in association with IBM November 2003

[Source: GInO 04:]
GERMANY.INDYMEDIA.ORG vom 24.05.2004: Wer wann mit wem..., http://germany. indymedia.org/2004/05/84254.shtml, Abruf vom 12.08.2004

[Source: Gole 04:]
GOLEM.DE vom 29.03.2004: Transponder macht Handy zum Türschlüssel oder zur Geldbörse. Siemens zeigt Einsatz von Transponder in Mobiltelefonen, http://www.golem.de/0403/30559.html, Abruf vom 04.07.2004

[Source: HaHa 04:]
Der Hamburger Hafen bleibt auch 2004 auf Rekordkurs. In: DIE WELT Online vom 10. Juni 2004, http://www.welt.de/data/2004/06/10/289082.html, Abruf vom 26.08.2004

[Source: HAMM 04:]
HAMMERSCHMIT, C.: CeBIT: Nokia, Philips und Sony forcieren neuen Kommunikations-standard. In: EETIMES.de vom 18. März 2004, http://www.eetimes.de/story/OEG20040318S0010, Abruf vom 26.08.2004.

[Source: Hand 03:]
Funkchips sichern Ware gegen Diebstahl. In: HANDELSBLATT vom 19. August 2003, http://www.handelsblatt.com/pshb/fn/relhbi/

sfn/buildhbi/cn/GoArt!200104,203116,654244/SH/0/depot/0/, Abruf vom 08.07.2004

[Source: Hand 04:]
Biometrie fürs Schlachtvieh – Gesetzlich geforderte Überwachung. In: Handelsblatt, Freitag, 11. Juni 2004, 13:32 Uhr, http://www.handelsblatt.com/pshb/fn/relhbi/sfn/buildhbi/cn/GoArt!200104,204819,746496/SH/0/depot/0/, 17.06.2004, Abruf vom 28.07.2004

[Source: HBBB 03:]
HILTY, L., BEHRENDT, S., BINSWANGER, M., BRUININK, A., ERDMANN, L.Z, FRÖHLICH, J., KÖHLER, A., KUSTER, N., SOM, C. und WÜRTENBERGER, F.: Das Vorsorgeprinzip in der Informationsgesellschaft Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. Eine Studie der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA) und des IZT – Institut für Zukunftsstudien und Technologiebewertung im Auftrag des Zentrums für Technologiefolgen-Abschätzung beim Schweizerischen Wissenschafts- und Technologierat (TA-SWISS) von August 2003 (TA 46/2003), http://www.ta-swiss.ch/www.remain/projects_archive/information_society/pervasive_d.htm, Abruf vom 16.08.2004.

[Source: Heis 03:]
Gillette will von Bespitzelung durch RFID-Tags nichts wissen. In: Heise Online vom 15.08.2003, http://www.heise.de/newsticker/meldung/39458

[Source: Heis 04a:]
Funketiketten für japanische Schulkinder. In: Heise Online vom 11.07.2004, http://www.heise.de/newsticker/meldung/49004, Abruf vom 23.07.2004

[Source: Heis 04b:]
RFID-Umfrage – Fußball-WM 2006 soll den Durchbruch bringen. In: Heise Online vom 21.04.2004, http://www.heise.de/newsticker/meldung/print/46724, Abruf vom 05.08.2004

[Source: Heis 04c:]
Fußball-WM 2006: Nur mit RFID ins Stadion. In: Heise Online vom 15.01.2004, http://www.heise.de/newsticker/meldung/ 43645, Abruf vom 26.06.2004

[Source: Heis 04d:]
Münchner Grüne wollen City-Maut mit RFID-Technologie. In: Heise Online vom 23.05.2004 http://www.heise.de/newsticker/meldung/47583, Abruf vom 26.08.2004

[Source: HeMü 04:]
HENRICI, D. und MÜLLER, P. (2004): Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In: Ferscha A., Mattern F.: Pervasive Computing (Proceedings of PERVASIVE 2004, Second International Conference on Pervasive Computing). Springer-Verlag, LNCS 3001: 219-224

[Source: Hill 03a:]
HILLENBRAND, T.: Wissen ist Verbrauchermacht. In: Spiegel Online vom 3. September 2003, http://www.spiegel.de/wirtschaft/0,1518,262761,00.html, Abruf vom 12.07.2004

[Source: Hill 03b:]
HILLENBRAND, T.: Zeigefreudige Models, hilfsbereite Mülltonnen. In: Spiegel Online vom 3. September 2003, http://www.spiegel.de/wirtschaft/0,1518,262758,00. html, Abruf vom 12.07.2004

[Source: Hilt 04:]
HILTY, LORENZ: Verselbständigt sich der Computer? Pervasive Computing könnte den Menschen schrittweise entmündigen. Electrosuisse Bulletin SEV/AES, 9/2004

[Source: HMM 04:]
HENRICI, D., MÜLLER J. und MÜLLER P. (in press): Sicherheit und Privatsphäre in RFID-Systemen. AG Integrierte Kommunikations-systeme, Technische Universität Kaiserslautern, 18. DFN-Arbeitstagung über Kommunikationsnetze, Springer, Lecture Notes in Informatics. 1.-4. Juni 2004, Düsseldorf

[Source: Höni 03:]
HÖNICKE, INA: Probleme und Problemchen mit RFID. In: ZDNet. http://www.zdnet.de/itmanager/tech/0,39023442,2137403,00.htm, Abruf vom 27.08.2004

[Source: ICAO 04a:]
INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO): PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Technical Report, published by authority of the Secretary General, http://www.icao.int/mrtd/Home/Index.cfm, Abruf vom 10.09.2004

[Source: ICAO 04b:]
INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO): Development of a logical data stucture – LDS. For optional Capacity Expansion Technologies, Revision -1.7, published by authority of the Secretary General
http://www.icao.int/mrtd/download/documents/LDStechnical%20report%202004.pdf, Abruf vom 10.09.2004

[Source: Idel 98:]
IDEL, A.: Krankheitsresistenzen bei landwirtschaftlich genutzten Tieren. In: Nutztierhaltung 4/1998. http://www.ign-nutztierhaltung.ch/NTH/PDF1998/nutz_498.pdf, Abruf vom 10.07.2004

[Source: Iden 04:]
IDENTEC SOLUTIONS: Volkswagen Processes Pre-delivery Automobiles with RFID. http://www.identecsolutions.com/pdf/IDENTEC%20SOLUTIONS_Volkswagen%20Case%20Study_2003.pdf, Abruf vom 24.07.2004

[Source: IDTE 04:]
IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. May 20, 2004. URL: http://www.idtechex.com/products/en/ article.asp?articleid=7&topicid=79.

[Source: IEEE 04:]
IEEE: P1363.2: Standard Specifications for Password-Based Public-Key Cryptographic Techniques, version D16, July; verfügbar unter: http://grouper.ieee.org/groups/1363/passwdPK/draft.html (16.07.2004)

[Source: Infi 02:]
INFINEON: Short Product Information: Security & Chip Card Ics my-d products for contactless systems my-s vicinity SRF 55V10P July 2002
http://www.infineon.com/cmc_upload/documents/029/172/SPI_SRF55V10P_0702.pdf

[Source: Inno 04a:]
Innovationsreport – Forum für Wissenschaft, Industrie und Wirtschaft: Michelin bringt funkende Reifen, http://www.innovations-report.de/html/berichte/innovative_produkte/bericht-15756.html, Abruf vom 10.07.2004

[Source: Inst o.J.:]
INSTITUTE FOR THE PROTECTION AND SECURITY OF THE CITIZEN: IDEA Project – Identification Electronique des Animaux, Final Report,
http://idea.jrc.it/pages%20idea/index%20of%20final%20report.htm, Abruf vom 04.08.2004

[Source: Isch 04:]
ISCHEBECK, B.: Objekte an der Funkleine. In: Funkschau 13/2004, S. 31 - 33

[Source: ISK 03:]
ISK – ISERLOHNER KUNSTSTOFF-TECHNOLOGIE GMBH: Verbundprojekt: Werkzeugidentifikation und -Management, http://www.isk-design.de/pdf/prospekte/transponder_flyer.pdf, Abruf vom 05.08.2004

[Source: JRS 03:]
JUELS, A., RIVEST, R.L. und SZYDLO, M.: The Blocker Tag: Selective Blocking of RFID-Tags for Consumer Privacy. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/

[Source: Katz 04:]
KATZENFREUNDE NORDEUTSCHLAND E. V.: Mikrochip: Sichere Identifizierung Ihres Tieres – ein Leben lang. http://www.kfndev.de/informatives_mikrochip. html, Abruf vom 04.08.2004

[Source: Klaß 04:]
KLAß, C.: Einkaufsbetrug mit RFID-Umprogrammierung. In: Networld, 29.07.2004
http://www.golem.de/0407/32666.html

[Source: Krem 04:]
KREMPL, S.: Das Internet der Dinge. In: Computerworld 5/2004, http://viadrina.euv-frankfurt-o.de/~sk/Pub/rfid-cw04.html, Abruf vom 02.07.2004

[Source: Kric oJ:]
KRICK, O.: Identsystem OIS-U: RFID Solution for Deutsche Post, http://www.identecsolutions.com/pdf/IDENTEC%20SOLUTIONS_Deutsche%20Post%20Case%20Study_2003.pdf, Abruf vom 25.08.2004

[Source: Land 01:]
LANDT, JEREMY: Shrouds of Time – The history of RFID. An AIM (The Association for Automatic Identification and Data Capture Technologies) Publication, http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf, Abruf vom 09.08.2004

[Source: Land 04:]
LANDKREIS BAMBERG: Restmülltonne mit Identsystem – Abfalltrennung wird künftig belohnt, http://www.landkreis-bamberg.de/index.phtml?start=1sowie http://www.markt-heiligenstadt.de/verwaltung/umwelt/abfallkonzept/restmuelltonne.shtml, Abruf vom 10.07.2004

[Source: Lang 04:]
LANGHEINRICH, M.: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. Über http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf [Source: 13.08.2004:]

[Source: LePh 04:]
LE PHAN MICHÈLE LA: RFID – Große Wirkung kleiner Chips. In: comtec 03/2004 http://www.swisscom-comtec.ch/pdf/comtec032004130.pdf, Abruf vom 05.08.2004

[Source: LLS 00:]
LAW, C., LEE, K. und SIU, K.Y.: Efficient Memoryless Protocol for Tag Identification. Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications. Boston, MA, USA. 75-84, verfügbar unter: http://portal.acm.org/citation.cfm?id=345865&dl=ACM&coll=portal (16.07.2004)

[Source: Malo 04:]
MALONE, M.: Case in Point. High Volume File Management Made Efficient with RFID Technology. http://multimedia.mmm.com/mws/mediawebserver.dyn?qqqqqq&8iBEqKUrq1UrqqqORGaQQQQQ5-, Abruf vom 21.07.2004

[Source: Mark o.J.:]
o.V. Druckkontrolle gegen Autorolle. In: Informations- und Beratungsplattform www.MarkteinstiegUSA.de, http://www.markteinstiegusa.de/Reifendruck-Kontrollsysteme.521.0.html, Abruf vom 08.09.2004

[Source: MaRö 03:]
MATTERN, F. UND RÖMER, K.: Drahtlose Sensornetze. In: Informatik-Spektrum, Vol. 26 No. 3, S. 191-194.

[Source: MASS 04:]
MASSEX SYSTEMHAUS: x-trade und RFID in der Kühlkette, http://www.maxess.de/index.php?id=113&backPID=25&L=0&tt_news=7, Abruf vom 05.08.2004

[Source: Matt 02:]
MATTERN, F.: Der Trend zur Vernetzung aller Dinge – Pervasive Computing und die Zukunft des Internets. In: Neue Kommunikationsanwendungen in modernen Netzen, Seiten 9-13. ITG-Fachtagung, Februar 2002. http://www.inf.ethz.ch/vs/publ/papers/VernetzungAllerDinge.pdf, Abruf vom 19.08.2004

[Source: MBZK 04:]
Ministerie van Binnenlands Zaken en Konin-krijksrelaties: Praktijkproef biometrie in reisdocumenten start 1 september in zes gemeenten. Pressemitteilung vom 27.05.2004,http://www.minbzk.nl/persoonsgegevens_en/in_het_kort/persberichten/praktijkproef, Abruf vom 18.10.2004

[Source: McKa 03:]
MCCUE, A. und KAUFMANN, J.: Sun eröffnet RFID-Testcenter in Europa. In: ZDNet vom

08.12.2003, http://www.zdnet.de/news/business/0,39023142,39118100,00.htm), Abruf vom 12.07.2004

[Source: Mose 04:]
MOSER, P.: Praxisbeispiel aus der Automobilindustrie zeigt Einsparpotentiale der RFID-Technologie. In: Logistik für Unternehmen vom 08.04.2004,
http://www.mylogistics.net/de/news/themen/key/news104382/jsp, Abruf vom 07.07.2004

[Source: Mylo 04:]
Mylogistics.net – Logistik für Unternehmen: Fraunhofer-Gesellschaft gründet RFID-Test-Labor in Magdeburg, http://www.mylogistics.net/de/news/themen/key/news146902/jsp, Abruf vom 14.7.2004

[Source: NFC 04a:]
NFC Forum, http://www.nfc-forum.org/, Abruf vom 25.07.2004

[Source: NFC 04b:]
Nokia, Philips and Sony establish the Near Field Communication (NFC) Forum. Forum will drive industry uptake of intuitive NFC technology that enables touch-based interaction with electronic devices. Presseerklärung von Nokia, Philips und Sony, 18.03.04,
http://www.nfcforum.org/pdfs/NFC_Forum_Announcement.PDF, Abruf vom 23.08.2004

[Source: Noga 00:]
NOGALA, D. F: Der Frosch im heißen Wasser – Die Trivialisierung von Über-wachung in der informatisierten Gesellschaft des 21. Jahrhunderts. In: TELEPOLIS,
http://www.heise.de/tp/deutsch/inhalt/co/8988/1.html, Abruf vom 18.08.2004

[Source: OECD 80:]
OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Document C(80)58(Final), October 1, 1980

[Source: ORF 04a:]
Ein RFID-Rechner aus Pappkarton. In: ORF FutureZone vom 05.03.2004,
http://futurezone.orf.at/futurezone.orf?read=detail&id=219132&tmp=7798, Abruf vom 20.07.2004

[Source: ORF 04b:]
RFID-Armbänder für Patientendaten. In: ORF FutureZone vom 27.07.2004,
http://futurezone.orf.at/futurezone.orf?read=detail&id=240826&channel=1, Abruf vom 30.07.2004

[Source: OSK 03:]
OHKUBO, M., SUZUKI, K. und KINOSHITA, S.: Cryptographic Approach to „Privacy-Friendly“ Tags. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, MA, USA.

[Source: Phil 01:]
Product News From Philips Semiconductors: Philips Semiconductors launches SmartMX, a versatile, highly secure 8051-based family of smart card microcontrollers, tailored to current and future market requirements. Pressemitteilung vom 23. Oktober 2001,
http://www.semiconductors.philips.com/news/content/file_758.html, siehe auch ergänzend
http://www.semiconductors.philips.com/news/publications/content/file_927.html, Abruf vom 14.09.2004

[Source: Phil 04:]
PHILLIPS AUSTRIA: it Philips RFID Know-how gegen Tierseuchen in Europa,
http://www.philips.at/InformationCenter/NO/FArticleSummary.asp?lNodeId=1253&channel=1253&channelId=N1253A3254, Abruf vom 09.08.2004

[Source: Pößn 04:]
PÖßNECK, L.: Fußball-WM: Golden Goal für RFID? Die Fans wollen ein Fußballfest, die Industrie eine IT-Mustermesse. In: Silicon.de,
http://www.silicon.de/cpo/hgrmobile/detail.php?nr=14566&directory=hgr-mobile, Abruf vom 05.08.2004

[Source: Pres 03:]
PRESS RELEASES: Tierseuchenbekämpfung: Byrne begrüßt die Verabschiedung von

Kennzeichnungsvorschriften für Schafe und Ziegen durch den Rat, Reference: IP/03/1761, Brüssel, den 17.12.2003, http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/03/1761&format=HTML&aged=0&language=DE&guiLanguage=en#file.tmp_Ref_1, Abruf vom 03.08.2004

[Source: Prog 04:]
PROGRESS SOFTWARE O. V.: RFID-Integration – Brückenschlag vom Transponder zur Unternehmensanwendung, http://www.progress.com/worldwide/de/docs/rfid_whitepaper_de_gif.pdf, Abruf vom 24.07.2004

[Source: Quac 04:]
QUACK, K.: Transponder meldet: „Wartung ausgeführt“. In: Computerwoche Online, http://www.computerwoche.de/index.cfm?pageid=256&artid=52033, Abruf vom 12.07.2004

[Source: RaEf 02:]
RANKL, W.; EFFING, W.: Handbuch der Chip-karten. Aufbau – Funktionsweise – Einsatz von Smart Cards. 2., überarbeitete und aktualisierte Auflage. München und Wien.

[Source: RFID 03:]
RFID Journal (2003) Class 1, G2, EPC Tags Ready by Q4, http://www.rfidjournal.com/article/articleview/714/1/1, Abruf vom 09.09.2004

[Source: RF-ID 04:]
RFID-ID.com: 869MHz RF-ID Tags Read Only and Programable, http://www.rf-id.com/rfidit.html, Abruf vom 26.08.2004

[Source: Richt 02:]
RICHTLINIE 2002/58/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

[Source: Robe 04:]
ROBERTI, MARK: Standardizing EPC Data-Sharing. In: RFID Journal, http://www.rfidjournal.com/article/articleview/ 878/1/1/, Abruf vom 20.04.2004

[Source: Roth 03:]
ROTHE, M.: Big Brother im Panopticon? Überwachung aus liberaler und autonomiekritischer Sicht. In: TELEPOLIS, http://www.heise.de/tp/deutsch/inhalt/co/12842/1.html, Abruf vom 09.08.2004

[Source: RPG 01:]
ROßNAGEL, A.; PFITZMANN, A.; GARSTKA, H.: Modernisierung des Datenschutzrechts. Berlin: Bundesministerium des Innern, 2001

[Source: SAP 04:]
SAP: SAP-Lösungen mit RFID finden steigende Verbreitung. http://www.sap.com/austria/company/presse/texte_2004/press39_04_07.asp, Abruf vom 31.07.2004

[Source: Scha 04:]
SCHAAR, P.: „Smart Chips: Kleine Brüder oder große Chance? Datenschutz und Verbraucherschutz vor neuen Herausforderungen“. Referat des Bundesbeauftragten für den Datenschutz auf der Veranstaltung der Heinrich-Böll-Stiftung in Kooperation mit dem Netzwerk Neue Medien e. V. am 05. April 2004 in Berlin, http://www.bfd.bund.de/aktuelles/akt20040513.pdf, Abruf vom 19.08.2004

[Source: Schl 03:]
SCHLÜTER, A.: Integrationshandbuch Microsoft-Netzwerk. Windows Server 2000/2003, Active Directory, Exchange Server, Windows XP und Office XP/2003 im Einsatz. Bonn, S. 841 ff. Hier zitiert nach http://www.wintotal.de/Artikel/Internetarbeit/internetarbeit.php [Source: 13.08.04:]

[Source: Schu 00:]
SCHUERMANN, J.: Information technology – Radio frequency identification (RFID) and the world of radio regulations. In: ISO Bulletin May 2000, S. 4. http://www.iso.org/iso/en/commcentre/pdf/
Radio0005.pdf

[Source: Schu 04a:]
SCHULZKI-HADDOUTI, C.: Elektronischer Pass – „Biometrische Reisepässe“ mit RFID-Transpondern in der Einführungsphase. In: c't 9/2004, S. 52: Biometrie, http://www.heise.de/ct/04/09/052/default.shtml, Abruf vom 18.07.2004

[Source: Schu 04b:]
SCHULZKI-HADDOUTI, C.: Neue Reisepässe: Mit Sicherheit teuer, In: Online Magazin Sicherheit heute, http://www.sicherheitheute.de/index.php?cccpage=readtechnik&set_z_artikel=8, Abruf vom 12.07.2004

[Source: SEC 04a:]
SEC-WORLS.NET: Erste Auto-Nummernschilder mit RFID-Technologie, http://www.sec-world.net/news/66876-erste-autonummernschilder-mit-rfidtechnologie.html, Abruf vom 16.08.2004

[Source: SEC 04b:]
SEC-WORLS.NET: Infineon – Gesprächige Chipkarten, http://www.sec-world.net/news/66688-infineon-gespraechige-chipkarten.html, Abruf vom 16.08.2004

[Source: Sili 04:]
Silicon.de vom 06.04.2004: RFID – Die Technik macht Missbrauch leicht möglich, http://www.silicon.de/cpo/hgrmobile/detail.php?nr=14036, Abruf vom 05.08.2004

[Source: Sili 04:]
Silicon.de vom 25.05.2004: Postunternehmen starten RFID-Mega-Test. http://www.silicon.de/cpo/news-mobile/ detail.php?nr=14739&directory=news-mobile, Abruf vom 12.07.2004

[Source: Sinn 04:]
SINN, D.: Auf RFID ist die IT schlecht vorbereitet, In: Computerwoche Online, http://www.computerwoche.de/index.cfm?pageid=256&artid=58094&main_id=58094&category=25&currpage=1&type=detail&kw=, Abruf vom 8.07.2004

[Source: Sore 04:]
SOREON RESEARCH: Überholspur: RFID-Markt Handel in Europa 2004-2008.Pressemitteilung: 11.05.2004 – Soreon Research
http://www.pressrelations.de/index.cfm?start_url=http%3A//www.pressrelations.de/search/release.cfm%3Fr%3D155879%26style%3D, Abruf vom 14.7.2004

[Source: SSSR oJ:]
STEPHEN A. WEIS, SANJAY E. SARMA, RONALD L. RIVESTAND DANIEL W. ENGELS: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems

[Source: Stan 04:]
PHILIPS SEMICONDUCTORS: Mehr Mitarbeiter, neue Kontaktlos-Technologie. In: Der Standard vom 10. Juni 2004, http://derstandard.at/?url=/?id=1684583, Abruf vom 10.08.2004

[Source: StFl 04:]
STRASSNER, M. und FLEISCH, E.: Ubiquitous Computing in der Flugzeugwartung. http://www.m-lab.ch/pubs/Strassner_Lampe_Fleisch_MultiK2004.pdf, Abruf vom 31.07.2004

[Source: TAB 03:]
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG BEIM DEUTSCHEN BUNDESTAG: „Biometrie und Ausweisdokumente“ Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zusammenfassung des TAB-Arbeitsberichtes Nr. 93, http://www.tab.fzk.de/de/projekt/zusammenfassung/ab93.htm, Abruf vom 12.05.2004

[Source: tecc 04:]
techchannel.de vom 02.07.2004: Delta Air Lines verfolgt Gepäck mit RFID, http://www.tecchannel.de/news/hardware/16170/, Abruf vom 04.07.2004

[Source: Texa 04:]
Elektronische Tiererkennung. In: Texas Trading Rinderhaltung 2003 / 2004, http://www.texas-trading.de/pdf/elektronische_tiererkennung_03-04.pdf, Abruf vom 27.07.04

[Source: Verdi 04:]
Presseinformation des Bundesvorstands ver.di Vereinte Dienstleistungsgesellschaft vom 07. Juli 2004: Bespitzelung von Beschäftigten nimmt zu. Über http://www.onlinerechte-fuerbeschaeftigte.de /service/press_releases/040624155116 [Source: 13.08.04:]

[Source: Vere 04:]
Nutztieridentifikation durch Retina-Scanning – Optibrand stellt neue Lösung für Identifi-kation und Nachverfolgung von Nutztieren vor. In: Veredelungsproduktion – das Info-portal für Landwirte. http://www.veredelungsproduktion.de/pages/de/grundlagen/cpd/836.html, Abruf vom 28.07.2004.

[Source: Vibe 04:]
VEREIN FÜR INTERNET-BENUTZER ÖSTERREICHS (VIBE!AT) ÖSTERREICHS: Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, http://www.vibe.at/verein/, Abruf vom 12.08.2004

[Source: Vinc 03:]
VINCENZ, M.: Möglichkeiten und Grenzen heutiger Transpondertechnologien in der Logistik. Idealisierter Wunschtraum versus bezahlbare Realität. VDI Bericht Nr. 1744 zum 12ten Deutschen Materialflusskongress, März 2003, verfügbar unter: http://www.iqpaper.com/pdf/M%F6glichkeiten %20und%20Grenzen%20heutiger%20Transpondertechnologien.pdf, o. S.

[Source: Vit 04:]
VEREINIGTE INFORMATIONSSYSTEME TIERHALTUNG W. V. (VIT): ITeK-Rind, http://www.vit.de/ITeK-Rind.html#Section946, Abruf vom 04.08.2004

[Source: Vogt 02:]
VOGT, H.: Efficient Object Identification With Passive RFID Tags. In: Mattern F., Nagshineh M.: Proceedings of the First International Conference on Pervasive Computing (Pervasive 2002). Springer-Verlag, LNCS 2414, 98-113

[Source: Ward 04:]
WARD, DIANE MARIE: 5-Cent Tag Unlikely in 4 Years. In: RFID Journal, http://www.rfidjournal.com/article/articleview/1098/1/1/, Abruf vom 15.09.2004

[Source: Weis 03:]
WEIS, S.A.: Security and Privacy in Radio-Frequency Identification Devices. Masters Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, verfügbar unter: http://theory.lcs.mit.edu/~sweis (16.07.2004)

[Source: WSRE 03:]
WEIS, S.A., SARMA, S.E., RIVEST, R.L. und ENGELS, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. First International Conference on Security in Pervasive Computing, Boppard, März 2003. Springer-Verlag, LNCS 2802: 201-212

[Source: ZDNe 04:]
o.V.: RFID-Zentrum von Infineon präsentiert industrielle Lösungen. Flächendeckender Einsatz von RFID-Chips. In: ZDNet.de, http://www.zdnet.de/itmanager/tech/ 0,39023442,391216812,00.htm, Abruf vom 09.08.2004

[Source: ZEBR 03:]
ZEBRA TECHNOLOGIES CORP.: RFID – The Next Generation of AIDC Application white paper (2003) Im Internet u. a. unter http://www.rsiidtech.com/brochures/Zebra%20RFID%20White%20paper.pdf.

[Source: Zeid 03:]
ZEIDLER, M.: RFID – Der Schnüffelchip im Joghurtbecher. In: Monitor vom 08.01.2004, http://www.wdr.de/tv/monitor/pdf/040108f_rfid.pdf, Abruf vom 12.08.2004