FIDIS

Future of Identity in the Information Society

Title:	"D3.7 A Structured Collection on Information and Literature on Technological and Usability Aspects of Radio Frequency Identification (RFID)"
Author:	WP3
Editors:	Martin Meints (ICPP)
Reviewers:	Jozef Vyskoc (VaF) Sandra Steinbrecher (TUD)
Identifier:	D3.7
Type:	[Template]
Version:	1.0
Date:	Monday, 04 June 2007
Status:	[Deliverable]
Class:	[Public]
File:	fidis-wp3-del3.7.literature_RFID.doc

Summary

In this deliverable the physical properties of RFID, types of RFID systems basing on the physical properties and operational aspects of RFID systems are introduced and described. An overview on currently know security threats for RFID systems, countermeasures and related cost aspects is given. This is followed by a brief overview on current areas of application for RFID. To put a light on status quo and trends of development in the private sector in the context of RFID, the results of a study carried out in 2004 and 2005 in Germany are summarised. This is followed by an overview on relevant standards in the context of RFID. This deliverable also includes a bibliography containing relevant literature in the context of RFID. This is published in the bibliographic system at http://www.fidis.net/interactive/rfid-bibliography/

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1.	***Goethe University Frankfurt***	Germany
2.	***Joint Research Centre (JRC)***	Spain
3.	***Vrije Universiteit Brussel***	Belgium
4.	***Unabhängiges Landeszentrum für Datenschutz***	Germany
5.	***Institut Europeen D'Administration Des Affaires (INSEAD)***	France
6.	***University of Reading***	United Kingdom
7.	***Katholieke Universiteit Leuven***	Belgium
8.	***Tilburg University***	Netherlands
9.	***Karlstads University***	Sweden
10.	***Technische Universität Berlin***	Germany
11.	***Technische Universität Dresden***	Germany
12.	***Albert-Ludwig-University Freiburg***	Germany
13.	***Masarykova universita v Brne***	Czech Republic
14.	***VaF Bratislava***	Slovakia
15.	***London School of Economics and Political Science***	United Kingdom
16.	***Budapest University of Technology and Economics (ISTRI)***	Hungary
17.	***IBM Research GmbH***	Switzerland
18.	***Institut de recherche criminelle de la Gendarmerie Nationale***	France
19.	***Netherlands Forensic Institute***	Netherlands
20.	***Virtual Identity and Privacy Research Center***	Switzerland
21.	***Europäisches Microsoft Innovations Center GmbH***	Germany
22.	***Institute of Communication and Computer Systems (ICCS)***	Greece
23.	***AXSionics AG***	Switzerland
24.	***SIRRIX AG Security Technologies***	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	22.08.06	• Initial Draft (Martin Meints, ICPP). Contributions written by Pavel Rotter (IPTS, chapter 3), Martin Meints (ICPP, chapter 4) and Sven Wohlgemuth (ALU-FR, chapter 5) integrated.
0.2	08.10.06	• Introduction (Martin Meints, ICPP) and large parts of chapter 2 (Mark Gasson, Reading University) integrated
0.3	26.10.06	• Revised version of chapter 3 (Pavel Rotter, IPTS) integrated
0.4	25.02.07	• Chapter 2 revised (Mark Gasson)
0.5	12.03.07	• Chapter 6 added (Markus Hansen, ICPP)
0.6	04.04.07	• Integrative editing (Marit Hansen, Martin Meints, ICPP)
0.7	14.05.07	• Remarks from the reviewers and updated versions from the contributors integrated
1.0	14.05.07	• Final Version of the document (V 1.0)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Executive Summary)	Martin Meints (ICPP)
2 (RFID)	Mark Gasson (Reading University)
3 (Security Threats)	Pavel Rotter (IPTS), special review by Simone Fischer-Hübner (KU)
4 (Areas of Application)	Martin Meints (ICPP)
5 (Study: RFID in Germany)	Daniel Gille, Jens Strüker and Sven Wohlgemuth (ALU-FR)
6 (Standards)	Markus Hansen (ICPP)
7 Summary	Martin Meints (ICPP), Mark Gasson (Reading University)
8 (References)	All authors
9 (Bibliography)	Günter Karjoth (IBM-ZRL)
10 (Abbreviations)	All authors

Table of Contents

1 Executive Summary

This document gives an overview on Radio Frequency Identification (RFID). It is the first of currently (October 2006) planned two FIDIS deliverables and one declaration in the context of RFID. D3.7 is the technical background document for the following documents:

- D7.7 “RFID, Profiling and AmI”,
- D3.6 “Study on ID Documents” and
- D12.3 “Holistic Privacy Framework for RFID”.

For this reason certain aspects of RFID such as the use of data generated by RFID systems for profiling purposes and in the context of AmI and privacy aspects of RFID are not part of this deliverable. In addition this deliverable addresses a reader that is interest in technical details of this technology, though by far it can not be comprehensive. A more general introduction can be found in the Wikipedia.[1]

In chapter 2 the physical properties of RFID, types of RFID systems basing on the physical properties and operational aspects of RFID systems are introduced and described. Chapter 3 describes currently known security threats for RFID systems, countermeasures and related cost aspects. Chapter 4 gives a brief overview on current areas of application for RFID. To put a light on status quo and trends of development in the private sector in the context of RFID in chapter 5 the results of a study carried out in 2004 and 2005 are summarised. Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.** describes relevant standards in the context of RFID. This deliverable also includes a bibliography publicly available at http://www.fidis.net/interactive/rfid-bibliography/, see also chapter 9.

[1] See http://en.wikipedia.org/wiki/Radio-frequency_identification

2 Radio Frequency IDentification (RFID)

Since their conception, a plethora of RFID systems have been developed. Their popularity has primarily been driven by cost effective manufacturing techniques which allow for the production of a range of contactless RFID tags at a price which essentially makes them disposable - that is, the cost of the RFID tag is insignificant compared to the cost of the item being tagged, or revenue bought in or saved through tagging. With production costs dropping and new applications being developed, it is estimated[2] that production of these items will grow from some 1.3 billion parts manufactured in 2004 to 33 billion by 2010. However, because manufacturing costs are key to this technology, the majority of the systems developed are based on only a few basic operating procedures.

2.1 Physical properties

In this section, we shall elaborate on some of the key aspects of the RFID system design to highlight some of the important methodological differences between systems. An understanding of these different facets is essential to the appreciation of the fundamental limitations to RFID technologies.

Generally speaking, the variances between RFID systems can be broken down into eight key areas. Although this is not a comprehensive detailing of all potential differences between any two given systems, it does account for the major variants which have a significant bearing on the operating principles of the system.

These eight key areas are:

1. Operation type:
   The basic operation of the RFID system is for the RFID tag to communicate some piece of information back to the reader. However, by what protocol the RFID tag and the reader communicate to each other varies between systems.

2. Data Quantity:
   Although the basic premise is for the RFID tag to transfer information to the reader, the amount of data transferred varies from system to system from only one bit to several bytes.

[2] Research from In-Stat (www.in-stat.com) a provider of actionable research, market analysis and forecasts of advanced communications services, infrastructure, end-user devices and semiconductors.

3. Programmability:
   In some cases, the RFID tag can actually be programmed to run a sequence of instructions. This differs from the very basic tags in the sense that they are hard-wired to perform only one basic function.

4. Data carrier’s operating principle:
   There is a choice of transport methodology by which data can be transferred between the RFID tag and its reader. This aspect has a direct bearing on the range of frequencies which can be utilised, which in turn sets other system limits. Typical implementations use either surface acoustic wave (SAW) or, more usually, inductively coupled (IC) solutions.

5. Sequence:
   The sequence refers to the principles governing the RFID tag’s mode of operation. Essentially, this can either be a complex microprocessor (µP), as is required in programmable tags, or a simpler ‘state-machine’.

6. Power supply:
   This aspect is undoubtedly the driving force behind the design of the majority of RFID systems. Ideally, the RFID tag will not require its own power source, but will be given its power through some contactless means from the reader. However, in cases where this is not practical, such as with higher power microprocessor based tags, a supply internal to the tag is needed.

7. Frequency range:
   The operating frequency of the transport media between the RFID tag and reader is another key design aspect which sets limits on other aspects of the RFID system.

8. Data transfer:
   The data transfer from the RFID tag to the reader will be through some form of manipulation of the data carrier which is directly related to the ‘response frequency’ of the RFID system.

The interdependencies of these important factors and the resulting design methodologies can be derived from Figure 1: A flow diagram representing the major basic combinations of RFID systems

.

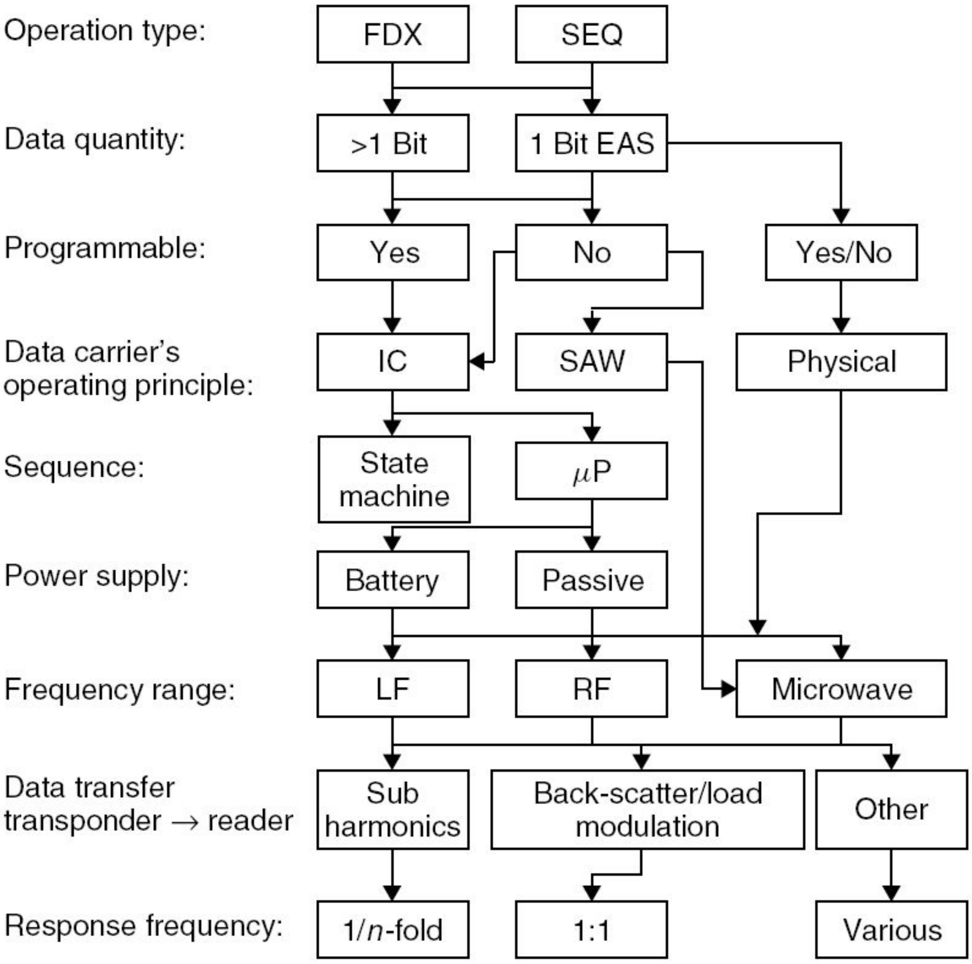

Figure 1: A flow diagram representing the major basic combinations of RFID systems[3]

The design of an RFID system, and thus the operation of its component parts is very much application specific. In most cases there will be fixed requirements which have to be catered for, and typically these will dictate the other aspects of the system. In the next section we will further describe the variations within the key areas of RFID system design.

2.2 Types of RFID systems

The flow diagram in Figure 1: A flow diagram representing the major basic combinations of RFID systems

[3] (Integrated Silicon Design, 1996)

illustrates how some of the aspects of the RFID system are dictated through the choice of others. Conversely, some aspects are independent, and are selected based purely on the RFID system design criteria. Here we shall discuss the factors involved in the decision process of some of the main system aspects.

2.2.1 Frequencies and range

RFID systems can operate over a large range of frequencies (see Figure 2**Fehler! Verweisquelle konnte nicht gefunden werden.**) although the choice of frequency depends on the mode of operation and the application. One of the main factors to consider is the range over which the RFID reader and tag can communicate with each other which is directly effected by the frequency utilised.

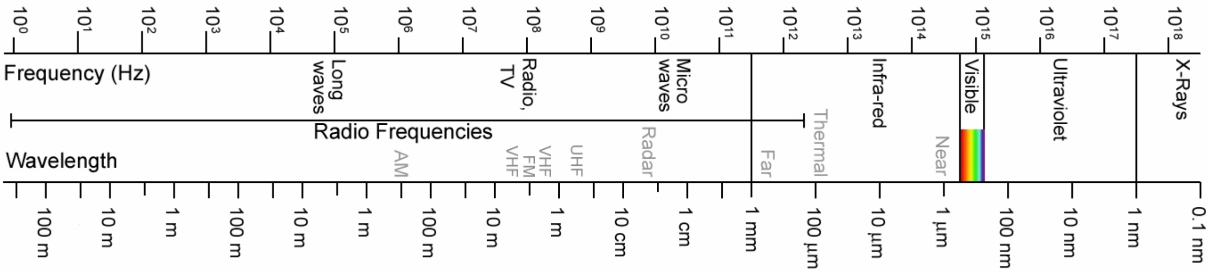

Figure 2: Illustration showing the broad range of frequencies within the electromagnetic spectrum that RFID systems can utilise

RFID transmission frequencies are roughly classified into the three ranges:

- LF (low frequency, 30-300 kHz),
- HF (high frequency)/RF radio frequency (3-30 MHz)
- UHF (ultra high frequency, 300 MHz-3 GHz)/microwave (>3 GHz).

However, the specific *absorption rate* (i.e. how much energy is lost as it passes through an object) of non-conductive substances (and water) is smaller by a factor of 100 000 at 100 kHz than it is at 1 GHz, so practically no energy is lost. The result of this is that systems operating at these frequencies will typically have a greater range. That said, lower frequency systems are noted for their improved object penetration over higher frequency ones.

RFID systems are also classified by range into:

- Close-coupling (0-1 cm),
- Remote-coupling (0-1 m),
- Long-range (>1 m) systems.

These ranges represent the theoretical maximum that could be achieved, and although clearly an important factor, the achievable range of communication between RFID tag and reader is dependent not only on the frequency utilised, but also a host of other factors. This can be issues such as the positional accuracy of the transponder, the minimum distance between several transponders in practical operation and the speed of the transponder in the interrogation zone of the reader (Finkenzeller, 2003).

2.2.2 Power supply

When considering power supply, we typically only consider the supply for the tag, since the reader is most often either powered from mains supply, or from standard batteries since size is rarely much of an issue.

In the majority of RFID applications it is desirable to have small and low cost tags. Additionally, the tag should have a long expected lifetime, perhaps of many years, with no maintenance required. These factors rather prohibit the use of batteries within the tags since this goes against all of these design criteria. Equally, in different applications, the tag may be required to perform some intensive processing, and thus requires significant power to do this. In these cases, batteries may be the only option.

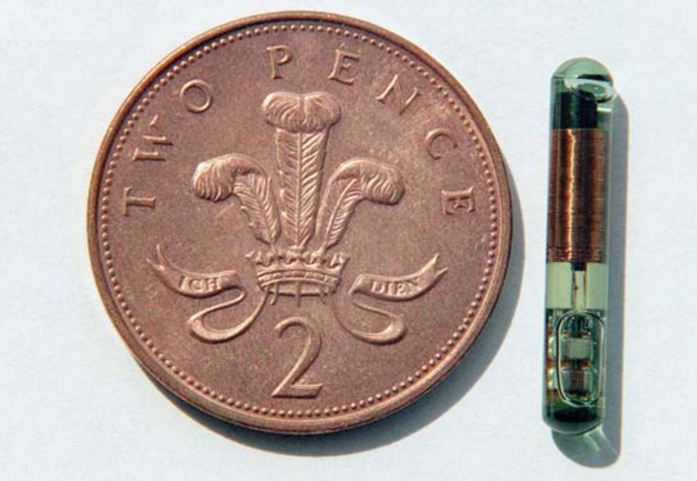

Figure 3: An example of a passive RFID tag, shown next to a UK two pence piece (roughly the size of a two Euro coin) for scale

As such, two variants of RFID tags have evolved. The tag is known as a *passive* transponder if it is unable to function without the reader since the reader supplies power to it. If the tag has its own power supply such as a battery, then it is an *active* transponder. Figure 3 shows an example of a passive tag. It is completely enclosed in glass, and has no serviceable components. Notably, the top section appears as a red-brown colour, and is in fact a tight coil of wire which is an integral part of its power and communication system – essentially acting as an aerial.

RFID systems that utilise frequencies between approximately 100 kHz and 30 MHz operate using inductive coupling, whereas microwave based systems in the frequency range 2.45–5.8 GHz are coupled using electromagnetic fields. However, it should be noted that the ranges achievable at higher frequencies are suitable for data transfer, but not for supplying power from the reader, and as such these typically utilise active devices. Conversely, almost all inductively coupled system utilise passive tags.

2.2.3 Data rate

Typically, the data quantity a tag holds is in the region of a few bytes to a few kilobytes (sometimes referred to as n-bit). However, some tags only operate using 1 bit – that is the reader can only tell if a tag is there or not, and nothing else. This is useful in applications such as shop security (Electronic Article Surveillance (EAS)) where you want an alarm to sound if a tag passes through the door *regardless* of what the tagged item is.

Some n-bit tags are programmable, that is the data that they contain can be changed by the 'reader'. Systems that have this functionality typically use Induction Coupling as their means of communicating between reader and tag, and most IC systems utilise passive tags. Simpler programmable tags contain simple logic (known as a state machine) which can control read/write access or to perform fairly complex sequences as well as holding 'state variables'. More complex varieties use a microprocessor which allows some degree of complex operations to be performed, and is ultimately more flexible than the state machine solution.

2.2.4 Operation type

The operation type of an RFID system is dependant on the application. Essentially, the RFID system can operate based on one of two basic protocols: Full (or half) duplex (FDX / HDX) or sequentially (SEQ).

During FDX / HDX the tag transponder sends its data when the RFID reader is asking for it. In the case of passive tags it is during the communication of the data request that power it is actually supplied, i.e. power is actually drawn from the communication signal itself. The difference between full and half duplex is simply that during full duplex, both the reader and tag and send data at the same time, whereas with half duplex, only one can send data at any one time. In either case, the reader continuously supplies power to the tag.

The SEQ protocol however requires the reader to briefly turn off the supply of power to the tag, during which time the tag sends its data. The reasoning behind the choice of operation type is essentially one of power coupling, that is, the way in which energy is transferred to the tag. Because full duplex systems can send data bi-directionally while power is being supplied to the tag, the tag is continuously using power. This means that the internal circuitry of the tag and its aerial have to be power matched in order to use power optimally. Unfortunately if they are matched, only half the potential source voltage (i.e. supply voltage to the tag) can be achieved, thus there is a trade off between power and voltage matching. This is not the case in SEQ systems, and as such provides distinct power advantages.

2.3 RFID systems

The basic RFID system consists of two main components, the small transponder, more commonly known as a tag, which is attached to the item needing identification and the interrogator, or reader, which in some cases is used to both power the tag and read its data without contact. Note that 'reader' is somewhat of a misnomer as the device in some cases can actually be used to write to the tag to change its data as well as reading from it. The basic components of the RFID system are shown in Figure 4:

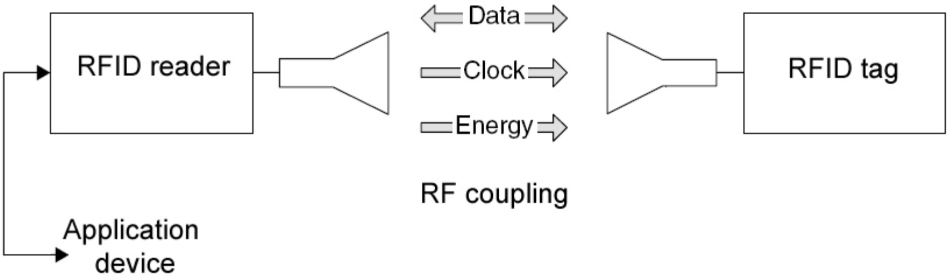

Figure 4: The two main components of the RFID system

The range of RFID implementations available are broad, and are covered in more depth in other FIDIS deliverables.

2.3.1 Tags

RFID tags are essentially radio transponders, i.e. they can receive and transmit using radio waves. Whilst all RFID tags at the basic level are used to store and transmit data, the variations in RFID tags are mainly due to their specific application. The application may dictate that the tag has to be readable over a certain range, and that will in turn dictate the technology just to transmit data and the amount of data it can store. These factors have a further bearing on the form factor (i.e. shape and size) of the tags themselves. Typically the most decisive element of the tag is the aerial – greater reading range will generally require an aerial with a larger surface area. With applications such as smart cards, a large flat area exists which can house a suitable aerial. However, in other applications such as RFID tags used for medical identification, the size is of importance and as such the useable range is limited. In some cases this is a desirable feature which helps in increase the security of the device.

In case readers cannot receive the signals of tags e.g. placed on various products on a palette, repeater tags can be used. These tags simply act as a kind of proxy. They are powered with a battery and are able to receive and resend signals from other tags. Using repeater tags shielding can be circumvented and weak signals of tags in farer distances can be amplified.

2.3.2 Readers

The fundamental role of the reader is to interrogate the tag and retrieve its stored data. In the case of active tags this role is extended to bidirectional communication. Whilst this is a seemingly simple task, the reader actually has to deal with potentially complex streams of data. This is, in part, because at any given times several RFID tags may well be within the polling range of the reader. When this happens the reader must be able to ensure the integrity of the data it is receiving. The functions of the reader are controlled by 'middleware', the software which runs inside the reader. This allows basic error checking, filtering, and low level control over the polling and tag reading. It also forms the interface between the reader module and the backend system. Readers can use one or more antennas.

2.3.3 Backend systems

Valid data received from RFID tags is passed by the middleware to the backend system. The backend system is where data is manipulated and stored, and forms the data resource for the system users. Typically the backend system incorporates some sort of database which allows the linking of the RFID data to other stored information or storing of the tag details themselves. For example, a given bit string RFID tag code is essentially useless as a piece of data in isolation, but if this unique code is associated with a given product or person, then the backend system can be used to cross reference the code and thus reveal the identity of the tagged item. Equally, a backend system may simply record the occurrences of RFID tags in specific locations, and thus tracking of tags becomes possible even if the identity of the tagged item is unknown.

The construction of the backend system is very application specific and can range from one computer which simply logs data, to banks of machines which perform complex analysis on data from thousands of distributed readers. Notably the backend system need not be geographically near to the RFID readers. Typical applications involve real time payment systems for access such as cashless motorway tollbooths. A brief overview on current areas of application of RFID is given in chapter 4.

The generally centralised database structure of backend systems makes them vulnerable from a security perspective. Essentially while reading RFID tags has associated privacy issues, it is widely understood that the easily exploitable data is most likely located in the databases – i.e. personal details, credit card numbers and so on. These issues will be further elaborated in the next chapter.

3 Security threats for RFID systems

3.1 Introduction

When considering the security challenges of RFID in a broader perspective, one has to take into account the infrastructure including a back office where additional information of all tags is stored, and the aspect of convenience in use. A general architecture of RFID systems is depicted in Figure 5:

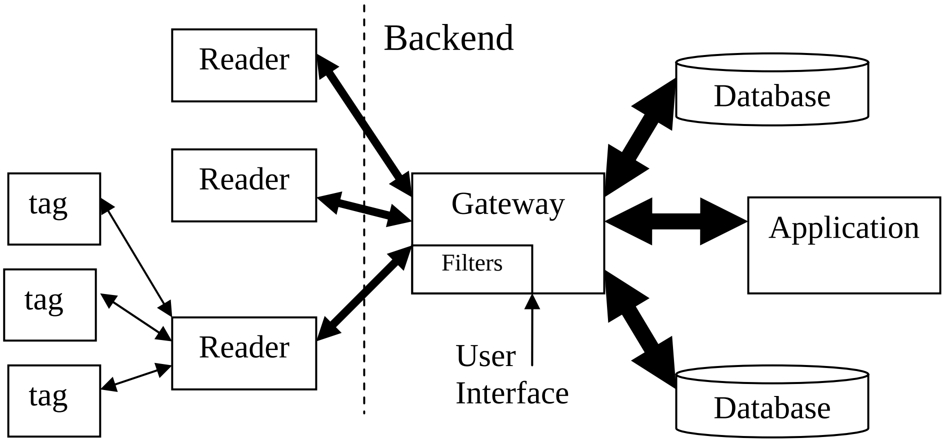

Figure 5: A general RFID architecture

Real-life RFID deployments employ a wide variety of physically distributed RFID readers, access gateways, and databases. The middleware of the gateway receives events from the RFID readers when tags are scanned. These events are passed through a number of filters, which process the events in an application-specific manner (e.g. by filtering irrelevant or faulty data out). When an event has passed through all filters, it is dispatched to the components that have registered an interest in such events. Often, one of these components will store the event in a database, for further processing.

RFID readers are generally connected to the middleware using modular drivers much like Windows uses device drivers to communicate with a graphics card. This allows different readers to be used with the middleware, without having to modify the middleware.

In addition to event-processing, the middleware handles different kinds of user interfaces. A user interface is generally provided for system-management purposes, for example to modify the series of filters through which an event is passed. There will also be user interfaces that allow regular users to access the system and use it. For example, in a supermarket distribution centre, there will be a user interface that provides information on the current stock levels.

The middleware also communicates with other software systems, which implement the application's business logic. To stay with the supermarket example, it is likely that the supermarket RFID system is connected to a stock management system, which orders new stock from suppliers before it runs out.

A good overview on security aspects of RFID and related systems can be found in the "Guidance for Securing RFID Systems" published by the (U.S.) National Institute of Standards and Technology (NIST)[4].

3.2 Commonly discussed security threats for RFID systems

3.2.1 Security threats for the tag

As already explained in chapter 2.3.1 RFID tags can be of different types. Consequently not all of the following threats and corresponding measures can be applied to all types of tags. As most of today's tags are used in supply chain management and follow the EPC standards (see chapter 6.9), threats relevant for these tags are listed in a separate chapter. This does not mean that these threats are not relevant for other types of tags – for example destruction or detaching can be done with all types of tags.

3.2.1.1 Security threats for EPC tags

Deployment of copied tags

Since basic RFID tag is a device which sends ID number when requested, it is relatively easy to build a duplicate of it, especially if an attacker does not have any constraints related to physical size.

Security measures for deployment of copied tags

Security measure to reduce the risks of deployment of falsified tags are the use of authentication protocols (not mandatory in basic EPC tag) in combination with key management procedures and management of issued tag numbers.[5] Also measurements of properties of signal sent by the tag may help to discriminate the proper tag from the fake, but not in case of a high quality falsification.

Related costs

Building falsified tag is not expensive, however requires some basic knowledge and skill. Protocols with tag authentication which can be applied as a measure require more sophisticated tags (and must be also supported by readers), therefore they cannot be applied in lowest cost solutions.

[4] See http://csrc.nist.gov/publications/drafts/800-98/Draft-SP800-98.pdf

[5] See http://www.gs1-germany.de/content/e39/e466/e468/datei//epc_rfid/mip_faelschungssicherheit.pdf

Deactivation

These types of attack render the tag useless through the unauthorized application of delete or kill (Auto-ID 2006) commands. 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.

Security measures for deactivation

Unauthorized application of delete commands or kill commands can be prevented by using an authentication method for the reader (when available).

Related costs

A deactivation by means of a kill command requires a dedicated device and usually a password. When the tag has an authentication method available, the costs of switching it on are low and most expenses would go in the management of tags and readers which have to be loaded with cryptographic keys. This would prevent unauthorized usage of the kill command.

Destruction

Tags could be physically destroyed by chemical or mechanical means, or by using strong electromagnetic fields (like in a microwave oven). Active tags could also be shut down by removing or discharging the battery.

Security measures for destruction

A countermeasure for destruction of the tag would be a close mechanical connection between the tag and the tagged item to make it difficult to destroy the tag without damaging the item. To prevent discharging the battery of an active tag one could implement a sleep mode in the tag.

Related cost

To physically deactivate a tag is easy by means of chemicals or exposure to an electromagnetic field, or to destroy the antenna. To prevent physical deactivation one could introduce a tight mechanical bond between the tag and the tagged item to ensure that removing the tag will also damage the product.

Detaching the tag

A tag is separated physically from the tagged item and may subsequently be associated with a different item, in the same way that price tags are "switched". Since RFID systems are completely dependent on the unambiguous identification of the tagged items by the transponders, this type of attack poses a fundamental security problem, even though it may appear trivial at first sight.

Security measures for detaching the tag

A countermeasure for detaching the tag from the tagged item would be a tight mechanical bond between the tag and the tagged item to ensure that removing the tag will also damage the product. In case of active tags, an alarm function is conceivable: a sensor determines that the tag has been manipulated and transmits the alarm to a reader as soon as it comes within range. For high value items an option would be to manually check whether the tag is attached to the correct item.

Related costs

In general a tag can be easily detached from the tagged item, unless some mechanical bond is placed between the tag and the tagged item. Alarm functions in which tag manipulation is detected by a sensor are only available in more expensive active tags.

3.2.1.2 Security threats for other types of RFID tags

Falsification of contents and/or tag ID

Data can be falsified by unauthorized write access to the tag. This type of attack is suitable for targeted deception only if, when the attack is carried out, the ID (serial number) and any other security information that might exist (e.g. keys) remain unchanged. This way the reader continues to recognize the identity of the tag correctly. This kind of attack is possible only in the case of RFID systems which, in addition to ID and security information, store other information on the tag.

The attacker obtains the ID and any security information of a tag and uses these to deceive a reader into accepting the identity of this particular tag. This method of attack can be carried out using a device that is capable of emulating any kind of tag or by producing a new tag as a duplicate of the old one (cloning). This kind of attack results in several tags with the same identity being in circulation.

Security measures to prevent unauthorized modification of tag data (contents and ID)

An obvious security measure to prevent modification of tag data is to use read-only tags for which unauthorized modification is intrinsically impossible. Another effective measure, also recommended for reasons of data management, is to shift all data except the ID to the backend. Some types of tags dispose of an authentication method (like the ISO 9798 standard), through which the reader can be authenticated by the tag such that only authorized readers can modify the tag's contents. In addition the data stored on the tag can be signed electronically.

Related costs

To perform an unauthorized modification of data in case of re-writable tags, the attacker would have to acquire a reader that is capable of writing on the tag. Due to the short range involved the possibility of this attack is limited. The longer the range of the reader, the more expensive the attack would be.

In general, a read-only tag is less expensive than a re-writable tag, so in case the application allows, a replacement by read-only tags would be a fine countermeasure. When the tag has an authentication method available, the costs of switching it on are low, most expenses would go in the management of tags and readers which have to be loaded with cryptographic keys. To shift all data on the tag to the backend requires a new infrastructure (in the backend and for provisioning of the tags and readers) which brings high initial costs, but will fade out later.

Unauthorised read access

If there is no authentication mechanism, the data placed on the tag can be read by an unauthorized reader, often from much bigger distance than foreseen for standard communication. For example data from e-passport, where standard 14443 is used have standard range 10 cm but it can be extended to 50 cm or even several meters.

Security measures for unauthorised data access

A simple, effective and low-cost security measure against unauthorised data access is shielding, i.e. wrapping the tag in metal foil or by placing it in an aluminium-coated bag. Shielding is a good solution for e.g. identity documents but for some applications is not appropriate because it does not allow for full automation of the process. More advanced solution is authentication of reader: the tag sends data to the reader only after checking its electronic signature.

Related costs

Unauthorized access to the tag can be obtained by relatively low cost, if no measures are applied. Reading data from shielded tags is practically impossible. Spoofing strong authentication procedure (challenge-response) can be done by reverse engineering of legitimate reader but is quite difficult and expensive.

A cost of shielding is low while appropriate authentication procedure cannot be done with a low-cost tag.

3.2.2 Security threats for the air interface

Eavesdropping

The communication between reader and transponder via the air interface can be monitored by intercepting and decoding the radio signals. This is one of the most specific threats to RFID systems. The eavesdropped information could for example be used to collect privacy sensitive information about a person.

Security measures for eavesdropping

An effective measure to reduce the effect of eavesdropping is to shift all data to the backend. However shifting data (e.g. biometrics) to a central database may bring some new privacy concerns and raises new security issues related to database protection.

More advanced tags have a module to encrypt the communication with the reader which also prevents eavesdropping. Another measure would be to design the RFID system such that tags are used with a small range which is just sufficient for the legitimate readers (and thereby shutting out a class of unauthorised readers).

Related costs

To perform eavesdropping, the attacker would have to acquire a suitable reader. Due to the short range involved the possibility of this attack is limited, however it can be performed from much greater distance than standard range of communication. On the other hand when attacker wants to eavesdrop communication from distance significantly greater than standard range, cost of attack increases.

A cheap and effective way to prevent eavesdropping is to use some kind of shielding of the tag, although this would have to be performed for every tag. When the tag has an encryption method available, the costs of switching it on are low; most expenses would go in the management of tags and readers which have to be loaded with cryptographic keys. To shift all data on the tag to the backend requires a new infrastructure (in the backend and for provisioning of the tags and readers) which brings high initial costs, but will fade out later.

Blocking

So-called blocker tags simulate to the reader the presence of any number of tags, thereby blocking the reader. A blocker tag must be configured for the respective anti-collision protocol that is used and for some protocols blocking is not possible. It is worth noting that blocker tag can be also a tool for protecting privacy (Juels, Rivest, Szydlo 2003) which does not allow the reader to read specific tags.

Security measures for blocking

Appropriate law regulations could be helpful (however obviously some attackers do not follow rules). Blocking can be prevented by using specific protocols.

Related costs

A blocker tag is relatively cheap and can prevent a reader from working properly, although they only work for specific anti-collision procedures. Price of using protocol which does not allow for blocking depends on implementation.

Jamming

Jamming means a deliberate attempt to disturb the air interface between reader and tag and thereby attacking the integrity or the availability of the communication. This could be achieved by powerful transmitters at a large distance, but also through more passive means such as shielding. As the air interface is not very robust, even simple passive measures can be very effective.

Security measures for jamming

It is possible to detect jamming transmitters by performing random measurements or by using permanently installed field detectors.

Related costs

A jamming transmitter has to be powerful enough to jam the tag-reader interface, and it requires some technical experience. The further the range, the more expensive the transmitter.

A field detector to detect possible jamming transmitters is a dedicated device, and measurements are performed by skilled engineers.

Relay attack

A relay attack (Kfir, Wool 2005) for contactless cards is similar to the well known man-in-the-middle attack. A device is placed in between the reader and the tag such that all communication between reader and tag goes through this device, while both tag and reader think they are communicating directly to each other. Smartly modifying this communication could for example in payment systems lead to charging the wrong electronic wallet (a smart card with an RFID tag). To make this attack more practical one could increase the distance between the legitimate card and the victim's card by splitting the device into two components, one communicating with the reader, and one with the victim's card. The communication between these two components could be implemented by any kind of fast wireless technology.

Security measures for relay attacks

One way to guard against relay attacks is to shield the tag when it's not used e.g. by putting the tagged card in a Faraday like cage (Kfir, Wool 2005). Another way is to require an additional action by the user (push a button, type in a PIN code or other authentication procedures) to activate the tagged card, although this solution eliminates some of the convenience of the contactless system. In addition the communication between tag and reader can be encrypted properly.

Related costs

To perform a relay attack requires a special device to intercept and modify the radio signal, and especially the communication between the two main components would be sophisticated.

To place the smart card in a Faraday save holder is relatively easy to do. An extra action by the user before activating the smart card and encryption require a more sophisticated card and/or reader.

3.2.3 Security threats for the reader

Falsifying reader ID

In a secure RFID system the reader must authenticate to the tag. If an attacker wants to read the data with his own reader, this reader must fake the "identity" of an authorized reader. Depending on the security measures in place, such an attack can be "very easy" to "practically impossible" to carry out. The reader might need access to the backend in order, for example, to retrieve keys that are stored there.

Security measures for falsifying the reader ID

To prevent readers to falsify their ID and obtain unauthorized access to a tag, an authentication method (when available at the tag) can be used to authenticate the reader towards the tag (ISO 1999). In authentication method called Basic Access Control, mandatory for European e-passports, the reader is authenticated to the tag based on key calculated from optical field, scanned directly from the passport. Therefore in order to retrieve data from passport, an attacker needs to know content of optical field. On the other hand, if the attacker once can see the optical field, he can get access to the data any time. Extended Access Control, applied for some e-passports, is more advanced authentication algorithm, based on asymmetric cryptography. In other words, a kind of digital signature is required from the reader to start communication.

Related costs

If no authentication method is deployed, falsification of reader ID is not difficult and can be done with relatively low cost. Authentication requires implementation both on the side of readers and tags, so it cannot be deployed in lowest cost solutions but average cost tags have often authentication method available, then the costs of switching it on are low and most expenses would go in the management of tags and readers which have to be loaded with cryptographic keys.

In the case of systems with authentication, in order to falsify the reader ID an attacker would have to obtain the secret key. The difficulty and costs for obtaining such a key depends on the implementation.

3.2.4 Security threats for the whole system

Malware

When considering the broader RFID architecture of Figure 5, new security risks and countermeasures come to mind: one could foresee an attack at the back office through information stored at the tag, which was recently shown in (DCSA 2006). Basically there are three types of RFID malware (Rieback 2006), which are mentioned in increasing complexity of implementation:

1. RFID exploits:
   Just like other software, RFID systems are vulnerable to buffer overflows, code insertion and SQL injection.
2. RFID worms:
   A worm is basically an RFID exploit that downloads and executes remote malware. A worm could propagate through the network or through tags.
3. RFID viruses:
   An RFID virus starts with malicious content of a tag. When the tag is read out, this initiates a malicious SQL query which would disturb a database in the back office. This type of attack already has been demonstrated (Juels 2006).

Measures for malware

To avoid such attacks, the compliance of the content of tags with respect to the corresponding standards should be checked by the reader, and regular security measures such as checks and filtering against signature databases should be taken to protect the gateway. In addition patches for the database should be installed, if available.

Threats to gateway interface

In case of insufficient access control the user interface to the gateway could be misused by unauthorised people to attack the integrity of the filters and to misguide the product management system.

Measures for threats to gateway interface

To prevent such an attack the user interface should be provided with a sufficient authentication mechanism such that only authorised users are able to access the gateway. Another measure would be to place the gateway and the user interface in a physically protected room such that only authorised employees that have access to this room can access the user interface.

Threats to drivers

The drivers that are used by RFID readers to communicate with the middleware could be corrupted. This could be done by either modifying the driver of a legitimate reader, or by replacing the legitimate reader with a fake reader that has a corrupted driver. A corrupted driver could be used to attack and misguide the gateway.

Measures to threats to drivers

A possible solution to this problem is to use only signed drivers, i.e. each legitimate driver should be digitally signed by manufacturers or trusted third parties such that the gateway can check that communicating readers contain a legitimate driver.

Threats to back office and measures

Systems at the back office could be subject to attack. These kinds of attacks (and their countermeasures) are known as attacks (and countermeasures) for regular IT systems and therefore not specific RFID related attacks.

Threats to communication reader ↔ gateway

The communication between reader and gateway could be eavesdropped or modified.

Measures to threats to communication reader ↔ gateway

Since an RFID reader is a more sophisticated device than a tag, some kind of encryption mechanism should be available to encrypt the communication between reader and gateway. Note that transfer of data between reader and gateway is similar to transfer of any other kind of data through the network (the connection can be wireless of wired) so threats and countermeasures are from technical point of view similar to existing in other kinds of networks.

3.3 Conclusions

Given commonly discussed security threats for an RFID system, and the available security measures against these threats, we can evaluate their implementation on RFID. This means incorporating (a qualitative estimate of) the costs of each security measure and on the other hand (a qualitative estimate of) the costs of performing a specific attack (BSI 2004). The comparison of these two types of costs will give insight into the current vulnerabilities of RFID systems.

The summary of this evaluation is shown Table 1. The qualitative estimates of the costs are explained in the following sections, followed by a separate section of conclusions.

Object	**Threat**	**Cost of performing threat**	**Cost of countermeasures**
EPC Tag	Deployment of falsified tag	Medium to high	Medium
	Deactivation	Low to medium	Medium
	Destruction	Low to medium	Low to medium
	Detaching the tag	Low	Low to medium
Tag-general	Falsification of content and/or tag ID	Medium to high	Medium
	Unauthorized read access	Medium to high	Low to medium
Air interface	Eavesdropping	High	Medium
	Blocking	Low	Low
	Jamming	Medium to high	Medium to high
	Relay attack	High	Low to medium
Reader	Falsifying reader ID	Medium to high	Medium

Table 1: Summary of security evaluation

From a financial point of view, the most alarming risk would be the risk that has low costs for performing the threat and high costs for taking countermeasures. By only analysing Table 1, this would be the risks of deactivating or detaching the tag because these are fairly easy to perform and countermeasures are more involved. Although much attention in the media is paid to eavesdropping on the air interface because of the privacy consequences of the consumer, from a security cost point of view indeed the vulnerability of the tag itself is an often overlooked aspect. Since tags are easily removed or destroyed, and countermeasures are costly, this can be seen as the weakest point of an RFID system.

At first sight it seems that a redesign of tags might be needed to overcome these risks. However, some important considerations have to be taken in mind:

- These are the results of a general threat analysis and rough cost estimation. No conclusions can be drawn with respect to specific applications or scenarios. Each application or scenario would require its own more detailed and specific security analysis. The (seriousness of the) consequences of removing or destroying RFID tags depend on the application. Depending on the business case of the application, even a Common Criteria accreditation process might be worthwhile.

- The costs are not the only point of view. Also user convenience, user's acceptance, interoperability, etc. are important factors to take into account. This would require a case by case analysis.
- The RFID system is usually part of a larger IT system which includes the back-office. Since the security chain is as weak as the weakest link, we have to consider the entire IT system.

The next chapter gives an overview on common areas of application for RFID.

4 Areas of application

In this chapter a number of typical applications for RFID are listed and briefly described from a technical perspective. This overview is meant to show the variety of applications of RFID, it is not comprehensive.

4.1 Access management

Access control for buildings or lockers is a largely accepted application using RFID. Typically for this purpose so called proximity cards containing a passive RFID tag from various manufacturers[6] are used. In many cases the RFID signal of proximity cards seems to be not encrypted ore secured by other measures. Cloning of proximity cards thus seems to be possible easily (Garfinkel, Rosenberg 2006: 291).

Other systems e.g., remote door openers for cars or vehicle immobilisers use active and passive RFID tags. Today the transmitted signals are typically encrypted, though encryption in some cases has obvious weaknesses (Bono et al. 2005).[7]

4.2 Tracking of goods and RFID in retail

Passive RFID tags are increasingly used for tracking goods. Integrated solutions for supply chain management (SCM) are available. In many cases in this context the Electronic Product Code (EPC) is used to tag palettes or items. Examples are:

- Tracking of goods in retail; in this context also smart shelves to locate and automatically order goods are used. In additional after sales services such as easier access to service without the original receipt of purchase basing on RFID are offered to the customers (see for example the Metro Case, Hildebrandt, Meints 2006: 21). RFID tags also can be used for theft prevention (Garfinkel, Rosenberg 2006: 384).
- Tracking of goods with the need for increased quality and security measures during the lifecycle, for example pharmaceuticals (see for example Garfinkel, Rosenberg 2006: 201). Management of perishable goods (such as milk) and recalls of faulty goods can be improved.
- Tracking of books in libraries (see for example Garfinkel, Rosenberg 2006: 229)
- Tagging of equipment and medicine in the healthcare sector (e.g. hospitals) to prevent theft and error in medication (see for example Garfinkel, Rosenberg 2006: 211)

[6] For example Bewator cards, see http://www.bewator.com/ or the Indala FlexPass, see http://www.indala.com/advantages.php?adv_id=4

[7] See for example http://www.rfidanalysis.org/

4.3 Tracking of persons and animals

In addition to goods persons and livestock can be tracked. For this purpose typically passive RFID tags are used. They can be attached to persons (for example new born babies in the hospital to endure that they stay matched to their mothers) or implanted into persons and animals (for example the VeriChip[8]).

In the context of persons the VeriChip also can be used additional purposes such as authentication, for example access control[8] or payment[9].

In the context of animals additional purposes are control / management e.g. of the feeding, or tracking of the movement of animals (Garfinkel, Rosenberg 2006: 245).

4.4 Toll collection and contactless payment

Active RFID tags in the USA are widely used for payment. Well documented examples are the Intelligent Highway Vehicle Systems (IHVS, Garfinkel, Rosenberg 2006: 360) for toll tracking and the SpeedPass system for payment run by ExxonMobile. According to Forester Research in U.S. the number of issued RFID payment tags had already reached 22 Mio households in 2003.[10]

In the SpeedPass system an encrypted identifier actively transmitted by the RFID tag is linked to a credit card. Via this credit card financial transactions take place. The encryption used in the SpeedPass system is the same as for some types of vehicle immobilisers and shows the same weaknesses.[7]

4.5 Machine readable travel documents

Basing on the Document 9303 by the ICAO (ICAO 2004) RFID microcontrollers are used in the European passport (also called ePass) to store personal data including biometrics. The use of RFID in machine readable travel documents (MRTDs) such as the ePass was described and analysed by Meints and Hansen (2006). Currently many countries such as France (Meints, Hansen 2006) and Germany (Engel 2006) plan to use RFID in combination with biometrics for national ID cards as well. Currently an improved access control for data on RFID tags, the so called extended access control (EAC) is in the specification process. Draft versions of these specifications are available at the German Federal Office for Information Security (BSI).[11]

[8] See http://www.verichipcorp.com/

[9] The use of the VeriChip for payment was called VeriPay, see http://www.atsnn.com/story/43890.html and http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=38038

[10] See http://www.forrester.com/ER/Research/Brief/Excerpt/0,1317,16708,00.html

[11] See http://www.bsi.de/fachthem/epass/eac.htm

4.6 Other applications

4.6.1 Smart dust

Since 1997 at the Berkley University Pister et al. carried out research with the target to develop self-contained, millimetre-scale sensing and wireless communication devices (so called motes) for massively distributed sensor networks. A number of wireless connected motes are called SmartDust. The working group suggested many different areas of use for SmartDust, many of the with a military or secret service background.[12] State-of-the-art in SmartDust related research, development and application recently was summarised by Steel (2005).

4.6.2 Location Based Services

RFID also can be used to mark a certain location. Location based services (LBS) basing on RFID typically use fixed passive tags to denote the location and mobile readers. RFID based LBS are used e.g. for educational purposes (Hildebrandt, Meints 2006, c.f. chapter 3.3) or fully autonomous warehouses, where RFID tags are fixed at the shelves and the readers are attached to vehicles moving the goods around.[13]

In the context of the football world championship 2006 in Germany also LBS using mobile RFID tags, fixed readers and mobile phones have been suggested (Strobl, Roth 2006: 91). These services have not been implemented so far.

[12] See http://www-bsac.eecs.berkeley.edu/archive/users/warneke-brett/SmartDust/index.html

[13] See for example http://www.directionsmag.com/press.releases/index.php?duty=Show&id=7702&trv=1

5 Study: RFID in Germany

5.1 Survey: methodology and standard values

The Institute of Computer Science and Social Studies of the Albert-Ludwig University Freiburg has been carried out an on-line survey from November 2004 to February 2005 regarding the economic use of RFID in German companies. This study is part of the series "Electronic Commerce Enquête" (ECE) focussing on the development of information and communication technology and its economic use (IC 2005). The objective of this on-line study is to give as far as possible an overview of first applications, planning and estimation of German enterprises already using RFID or where RFID is significant for their business. These enterprises are of the branches retail, processing business, logistics as well as other services and suppliers for RFID components and solutions. The questionnaire has been addressed to decision-maker of the highest hierarchy level. 68 out of 438 addressed enterprises have answered the questionnaire. The survey was carried out electronically. The statistical values have been calculated based on the number of answers for each question. Identifiable data regarding a person or an enterprise have not been collected. The distribution of the 68 enterprises regarding the branches is shown in **Fehler! Verweisquelle konnte nicht gefunden werden.**.

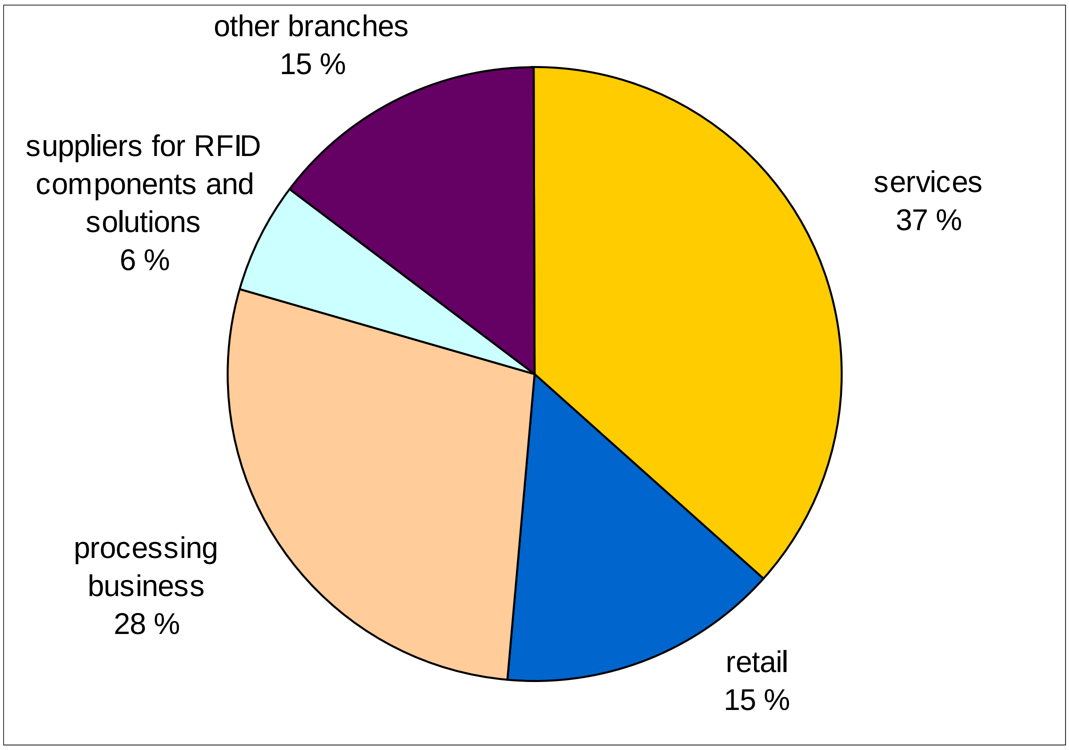

Figure 6: Distribution of enterprises belonging to a specific branch

In order to classify these 68 enterprises, the numbers of permanent employees and the annual turnover in millions of Euro have been collected. The determination of small and medium enterprises (SME), which represent 98% of all enterprises in the European Union (EU), has taken place according to the Official Journal of the European Union L123 (EU 2004). Regarding this method, 40% of the consulted enterprises are identifies as SME. This value is less than the average in the EU. The explanation is that only those enterprises are addressed which have already reached a specific progress in the use or testing of RFID. In addition to advertisements on web sides, e-mail newsletter and in journal by branches, enterprises listed in the Hoppenstedt database for SME[14] has been addresses individually. The relative big share of large-scale enterprise stems from the fact that large-scale enterprises are able to test a technology with sufficient funds at the beginning of its economic use while SME adapt an established and matured technology with a delay. This corresponds with the experiences gained by the introduction of other information and communication technology, e.g. the Internet (Sackmann, Strüker 2005).

5.2 Status quo and chances of using RFID

5.2.1 Current and future distribution of RFID

It is not surprising that 45% of 65 enterprises have already implemented a RFID application or are testing their RFID application, since the examined sample is focussed on industry which uses RFID very probably and it is not representative for all German enterprises. The further structuring of these enterprises is more expressive: 62% plan to expand the use of RFID and 14% test this technology in pilot projects. No enterprise will stop using RFID. This result is more surprising, since the participants are addressed via various and different channels (covering letter, web sides, e-mail newsletter of journals, references to the survey in journals, etc.) so that one cannot assume a distortion in favour of enterprises using successfully RFID.

Besides this fact, 23% of the respondents plan to use RFID in the next two years. Only 32% of them reject the question of using RFID for business applications. The use of RFID is in general suitable for 71% of these enterprises. This fact is more meaningful, if their long-term planning is taken into account. 13 out of these 15 enterprises (87%) plan to implement RFID applications at the latest in ten years, although they have no medium-term planning for it. Only 29% of the enterprises who gave a negative answer to this question or 9% of all enterprises estimate the use of RFID as “in general not suitable” for them.

Considering the branches of the 44 enterprises already using, testing or planning RFID applications, the branches services, in particular logistics and processing business put the main stress of using RFID. Regarding their planning, the branches consumer goods industry and logistics service providers will strengthen this trends, as shown in Table 1.

Retail (basis 10)	
Automobile trade, maintenance of automobiles	2

[14] http://www.hoppenstedt.de/

Retail procurement and wholesale (without automobiles)	4
Retail (without automobiles and filling stations)	4
Services (basis 25)	
Traffic, traffic agency	4
Logistics	5
Data processing and databases	6
Service providers especially for enterprises	9
Other services	1
Processing business (basis 19)	
Processing of consumer goods	13
Other processing business	6

Table 2: Distribution of those branches already planning and using RFID technology

Regarding the size of those 29 enterprises using and testing RFID, 82% of them are large-scale enterprises. But, if one looks at the planning status and at the minor role of SME in this sample, one can assume that they catch up: 8 planning large-scale enterprises stand facing 7 SME.

5.2.2 Scale of investment

35 enterprises have responded the question concerning the scale of investment. Quantifying the investments for RFID applications as part of the whole budget for information and communication technology (IT), only 7.1% of investments for IT are spent in the average for RFID (relative standard error: 24.3 %; median: 1%). Regarding only those 19 enterprises who have already invested in RFID, the average part of their investments is 13.1% (relative standard error: 18.8 %; median: 10%). The corresponding value of the representative study for Germany “ECE 2005” (Sackmann, Strüker 2005) is 6.9% (relative standard error: 17.8 %; median: 5%). This makes it clear that the investments in RFID applications are at the time of this RFID survey reserved.

However, one can assume a clear expansion of the investments. On the base of 59 enterprises, 85% state that they plan to increase (61%) or strongly increase (24%) their investments in RFID applications. Only 15% of the decision makers assess the development in the next two years as remain. No enterprise assumes a decrease of such investments.

5.2.3 What are the targets of an RFID application?

Besides the application of RFID, the concrete targets that enterprises pursue with the use of the technology were also established. The main focus of attention of enterprises already using RFID in the field of **logistics and stock keeping,** or are testing or planning to use it within the next two years, is the high degree of importance of the optimization of company-internal logistic processes (18 out of 21 “(relatively) high degree of importance”) and the offer of new, extended or improved services for customers (17 out of 20 “(relatively) high degree of importance”). As can be inferred from **Fehler! Verweisquelle konnte nicht gefunden werden.**, a relatively high degree of importance is attached to most of the targets questioned. Furthermore, it becomes clear that the “killer application” stocktaking previously identified as well as the high requirement for more frequent inventories may on no account be regarded as an end in itself. On the contrary, RFID-supported stocktaking must be interpreted as an “enabler” for advanced process optimizations. The optimization of logistic processes and the avoidance of out-of-stock situations are consequently rated higher in importance by the respondents than the pure price reduction of the inventory.

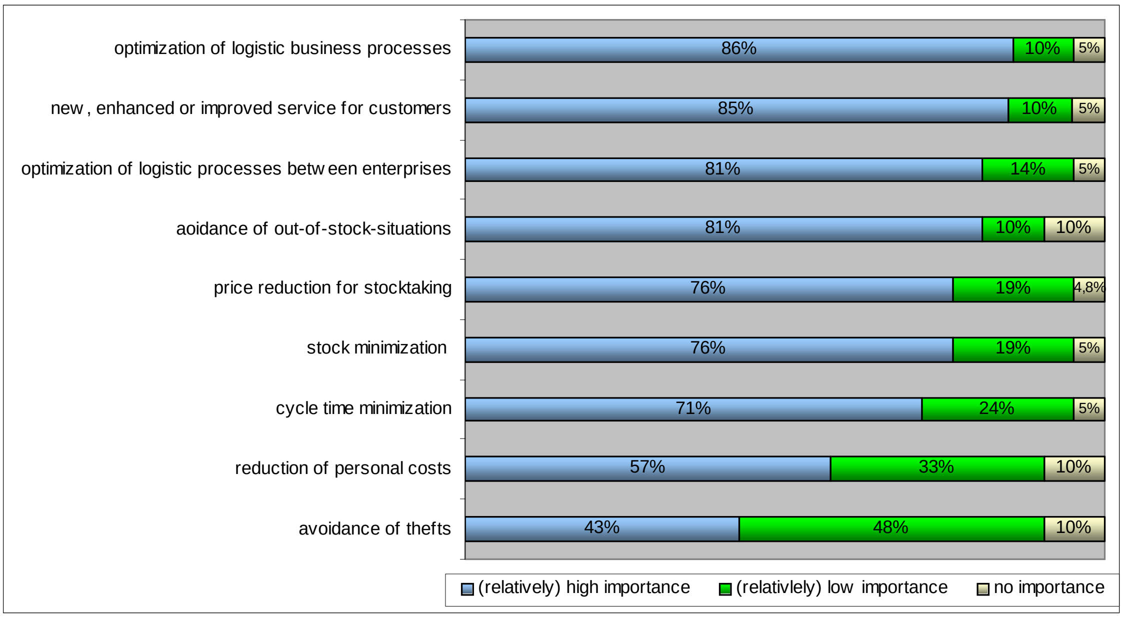

Figure 7: Targets of enterprises using, testing or planning to use RFID

In relation to the other targets, however, slightly less importance is attached to the lowering of personnel costs and the avoidance of theft.

In the course of the introduction of RFID technology, various hypotheses regarding the **opportunities** of this step were drawn up, which are to be evaluated with regard to their significance. Accordingly, enterprises see the biggest opportunity in a reduction of stock keeping due to the possibility of being able to react in good time to fluctuations in demand through the employment of RFID. 46% (basis 50) attach a (relatively) high degree of importance to this potential. In contrast to this cost reducing potential, the possibility of increasing turnover with RFID is more soberly assessed. The corresponding proportion of enterprises that promise themselves higher turnover due to increased sales of their customers merely amounts to 32% (basis 47).

In contrast to logistics, other **targets** stand in the foreground for RFID employment in **stores**. A strong focusing on the customer can be primarily detected here. For 20 out of 24 of the respondent enterprises, the increase in customer satisfaction has a (relatively) high degree of importance. A (relatively) high degree of importance is also attached to the offer of new, extended or improved services for customers and the increase in sales by 17 enterprises in each case (both: basis 23). Of somewhat lesser importance, however, are the targets of avoidance of theft (14 out of 25 attach a "(relatively) high degree of importance" to this and the increase that customers will buy the same goods again (10 out of 23). A further segmentation of the replies according to enterprises that, on the one hand, already use RFID in stores, are testing or planning this and enterprises for which, on the other hand, this use is basically suited was dispensed with due to the low number of cases.

In addition to the targets of the use of RFID, the original **reasons for an investment** in the technology that were decisive were also ascertained. A strong customer-orientation is again to be observed: 20 out of 24 enterprises attach a (relatively) high degree of importance to the expansion of services for customers. In addition, for 16 out of 22 firms, the realization of a competitive advantage is of (relatively) high importance. The fact that this potential advantage over rivals will not last long according to the assessment of the respondents can be illustrated by the evaluation of the sustainability of competitiveness: This investment reason is to be rated almost equivalent with 14 out of 21 enterprises that certified it with a (relatively) high degree of importance. At least some of the enterprises questioned therefore estimate that competitive advantages can be realized merely for a short time with the employment of RFID. According to the assessment, the technology will soon be so widespread that it can only be a matter for companies when making investment decisions not to lose contact with competitors. The initiative of suppliers and customers, on the other hand, presents a rather insignificant reason for introducing the technology. Only 8 out of 23 enterprises regard this factor as crucial for the investment decision of their enterprise.

5.2.4 What are the technical and economic risks of an RFID application?

The **risks** of an introduction of RFID are comparatively moderately evaluated. 47% ("(relatively) high degree of importance"; basis 49) anticipate an increasing retail market power due to the increasing availability of detailed purchasing information with RFID. The proportion of enterprises that fear finance problems with the introduction of RFID systems is similarly high (45%: basis 51). Other risks are rated significantly lower in importance however. Hence 35% (basis 49) of the enterprises attach a (relatively) high degree of importance to the danger of customer protests due to a restriction of the right to informational self-determination with the introduction of RFID. The respective proportions of further potential dangers turn out even less. For 27% of the enterprises (basis 49), the reduction in the order volumes of customers due to an RFID-related reduction in wastage together with respective turnover losses is a potential problem with a (relatively) high degree of importance. Financial problems with continuous RFID expenditure, e.g. for transponders, are feared by 26% of the respondents (basis 50). The increase in transport costs due to more frequent (just-in-time) orders of the customers (14%; basis 49) is ultimately practically ruled out as potential problem.

5.3 Hurdles and application problems

5.3.1 What are the biggest hurdles for an RFID investment?

In addition to the potentials of RFID technology, the problems that can arise with the introduction and use of the technology occupy a central position in the public discussion. Besides technical and financial problems, there is primarily the fear of consumers that the employment of RFID is linked with a restriction of their privacy. Within the scope of the study in hand, these problems were ascertained in the form of hurdles that have to be overcome when investing in RFID technology. A total of 14 hurdles could be evaluated according to their importance by the enterprises. Of particular interest is – besides the separate evaluation of individual hurdles – the analysis of the evaluations in relation to one another. This relative significance of the various obstacles is apparent in **Fehler! Verweisquelle konnte nicht gefunden werden.**.

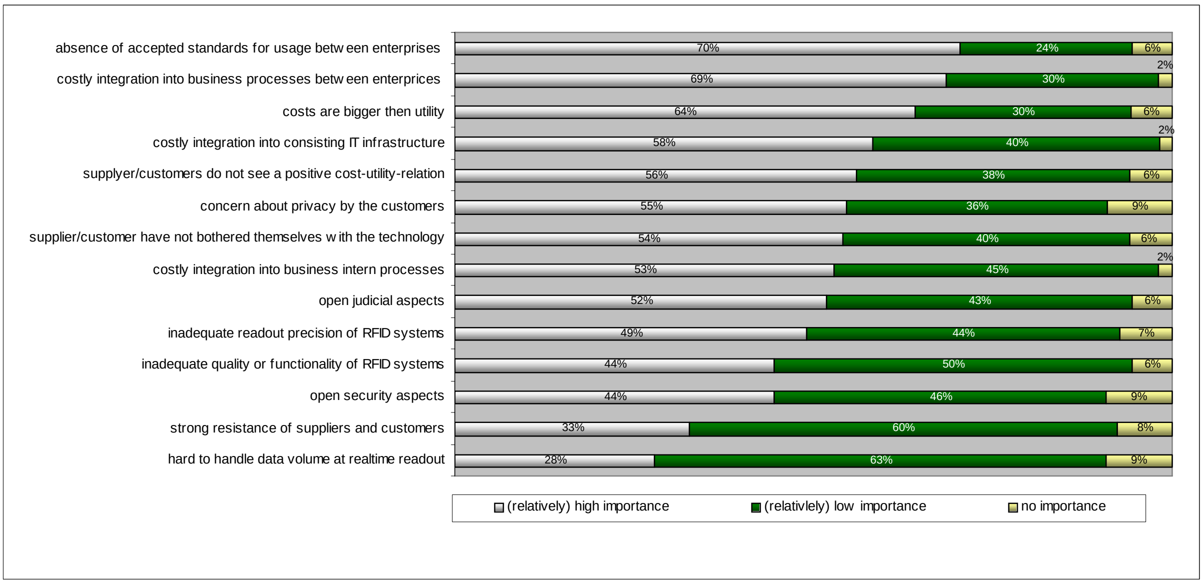

Figure 8: Hurdles regarding the investment in RFID technology (base 55-50)

Main hurdles

Standardization issues and integration of RFID technology into existing process and IT architectures are primarily regarded as **main hurdles**. 70% of the respondents (basis 54) attach a (relatively) high degree of importance to the lack of an accepted standard for inter-enterprise use as investment hurdle. The same applies for the complex integration of the technology into inter-enterprise business processes and the existing IT infrastructure of the enterprises. Furthermore, an unfavourable cost-utility relationship of RFID technology – from both the point of view of the respondent enterprises as well as from the perspective of the suppliers and customers – and data protection concerns of the customers are rated as significant hurdles. These findings are largely consistent with current prognoses and practice reports. Above all, the problem of data protection and the danger that the costs of the technology could exceed the utility for individual actors (e.g. manufacturers of low-value consumer goods) are frequently quoted. Moreover, it can be assumed that the main hurdles so far – standardization issues and integration– will decrease in significance with the introduction of the EPCglobal Gen 2 standards.

Further hurdles of relatively high significance

The point that cooperation partners have not yet grappled with RFID technology can be placed **midway** on the priority list of investment hurdles, just as the complex integration of the technology into company-internal business processes. The same applies for open legal aspects that arise from the introduction of RFID technology. It should be noted, however, that a (relatively) high degree of importance is attached to all of the previously presented hurdles by more than half of the respondent enterprises. The fact that German enterprises are uninformed with regards to RFID technology is particularly highlighted in numerous studies. The study of the marketing research company “Lünendonk und Technoconsult” results that 800 out of 1000 German decision makers do not know the meaning of the term RFID (Quack 2005).

Trend towards relatively insignificant hurdles

Hurdles that address the technical aspects of RFID systems are perceived to a comparatively **low degree.** Both the inadequate readout precision and the quality/functionality of the RFID systems and the drastic increase in the data volume to be handled for the readout of RFID transponders in real time are estimated to be a hurdle of (relatively) high significance by a minority of the enterprises questioned. This result gives rise to the conclusion that the technical problems with the introduction RFID systems, undoubtedly still existent (see section 3.4), are rated as “teething troubles”. Their cure is thus merely a question of time and, for this reason, is of secondary priority for the enterprises.

Strong resistance by suppliers and customers is decisive for enterprises, to a similarly low degree, when deciding about a potential investment in RFID technology. A possible explanatory approach for this is provided by the fact that RFID has so far mainly be used in enterprise-internal applications and therefore the majority of the enterprises have not yet been confronted with the problem of having to motivate cooperation partners to an adaptation of the technology.

Finally, open security issues are attached a (relatively) high degree of importance by 44% of the respondents (basis 54). This hurdle therefore belongs to the last but two positions in relation to the other established hurdles in order of priority. In view of the mainly high degree of significance that is attached to this hurdle in surveys with regard to the operational Internet application, this positioning is surprising. For example, the respondents of the “ECE 2005” study, representative for Germany, rated open security issues for both the networking with other enterprises as well as external access by personnel to business information systems as the most significant hurdle. This hurdle also always occupies a position in the top half for the offer and supply of services via Internet (Sackmann, Strüker 2005). The possible explanatory approach that the slightly less degree of significance of open security issues in the RFID context is due to the present dominance of company-internal RFID applications, cannot be sustained for the present: Both the enterprises that use RFID solely for internal processes (basis 24) and the (still) outnumbered group of inter-enterprise users (basis 18) unanimously rate the significance of open security issues at exactly 50 percent as “(relatively) high”. There can therefore be no difference made between these two groups with regard to the significance of security issues. This result indicates that other explanations for the low evaluation of open security issues for the application of RFID technology must be found.

5.3.2 Are the costs for RFID transponders too high?

One of the most important hurdles with regard to an RFID investment, whose significance is rated as "(relatively) high" by 64% of the respondents (basis 53), is the danger that the costs of an RFID application could exceed its utility. The analysis of the payment reserves of enterprises for active and passive transponders and the evaluation of the relative significance of individual items in the (planned or already realized) RFID investment volumes should therefore provide deeper insight with regard to the costs that are incurred for enterprises with the introduction of RFID technology.

The market for **active RFID transponders** is characterized by a great diversity of models with different functionalities and correspondingly varying prices. In contrast to this, the **payment reserves** of the 37 respondent enterprises are relatively homogenously distributed. 15 enterprises (41%) are therefore prepared to pay a maximum of 1 € for active transponders. Added to this are a further 16 firms for the sum of up to maximum 5 €, so that with 84% the great majority of all the enterprises are not prepared to pay more than 5 € for active transponders. Only 6 enterprises (16%) estimate their payment reserves at between 5 and 50 €.

The price range for **passive transponders** is considerably more limited compared to this. With 17 out of 45 respondent enterprises (38%), the relative majority of the enterprises are only prepared to pay between 1 and 10 cents per chip. A further 16 enterprises account for the next highest category (11-20 cents), so that with 74% the majority of the respondents are not prepared to pay more than 20 cents for a passive transponder (see also Table 13). In view of this concentration of payment reserves, the price reductions of the large chip manufacturers constitute a first step towards a broader acceptance and application of the technology.

1 – 10 cent	17	38%
11 – 20 cent	16	36%
21 – 30 cent	3	7%
31 – 40 cent	1	2%
41 – 50 cent	4	9%
> 50 cent	4	9%

Table 3: Payment reserve for passive RFID transponder (basis 45)

To determine the **relative significance of the transponder costs** in proportion to other items of the entire RFID investment volume, a priority sequence of the proportions of the six most important elements was ascertained from the RFID budget. Besides the transponder costs, these elements comprise the acquisition costs for reader devices, other hardware (e.g. additional computers) and software as well as integration costs into existing information systems and conversion costs of previous company-internal and inter-company business processes. Due to the low case number of 17, the significance of the responses is, however, very limited.

5.3.3 Is there a threat of lacking customer acceptance?

Possible data protection concerns of customers with an increased use of RFID transponders at article-level continue to be rated in their significance as "(relatively) high" by the majority. This is due, amongst others, to the technically easy to perform option for enterprises, authorities and private persons, of collecting unauthorized personal data with a wide distribution of RFID transponders and to aggregate this in the form of profiles. The real or at least feared loss of privacy by the consumers resulting from this can have an affect on enterprises using RFID in the form of turnover losses owing to a boycott for example.

According to the estimation of the enterprises questioned, data of a different quality and further data about business partners (e.g. for the improvement of the cooperation) is primarily stored (see Figure 4) with the use of RFID and the resultant **modified data situation.** These assertions apply for 72% (basis 47) and 69% (basis 48) of the respondents. Furthermore, with 59% the majority of the respondents (basis 49) are of the opinion that the use of RFID technology necessitates a tightening of data protection declarations. Further assertions felt by the majority as applicable imply an elaborate protection of personal data against loss, theft or misuse and an increasing amount of stored data about end customers. Conversely, a minority of the enterprises believe that with the use of RFID, data is stored longer than before (42% "(relatively) applies"; basis 48). Moreover, it is virtually ruled out (10% "(relatively) applies"; basis 48) that with RFID even a slackening of previous data protection declarations has become necessary.

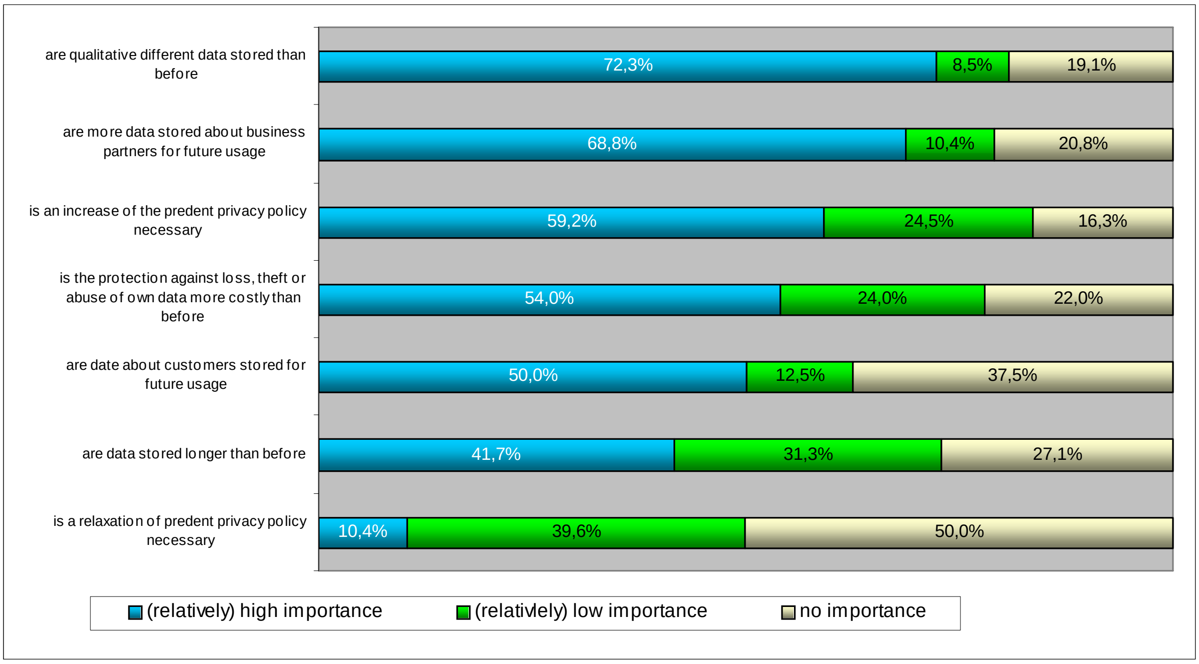

Figure 9: Estimation of several statements regarding data protection: "By using RFID technology …" (basis 50-47)

This modified data situation can also generate a series of **problems** for enterprises, of which inadequate security has the highest significance (58% "(relatively) high significance"; basis 48) for the respondents **after successful introduction of the technology**. This result is particularly interesting in view of the low significance attached to open security issues as investment hurdles, therefore as problem before the introduction of the technology (see section 3.4). Further cooperation-related problems, e.g. information retention, information misuse and unobservability of misconduct of the transaction partner are rated as less serious by the majority. The same applies for the loss of control over personal data, which is felt to be a (relatively) significant problem by only 39% of the enterprises (basis 49).

5.3.4 Is the problem of inadequate readout precision overestimated?

Although the significance of hurdles concerning the functionality of RFID systems is to be regarded as relatively low, problems concerning the **readout precision of RFID transponders** are known from numerous practice reports. Owing to the multitude of environments in which wireless technology can be used and particularly for the use of passive transponders that do not have any power supply of their own for sending their information, variations with regard to the readout precision are virtually unavoidable.

The presence of liquids and metals which hinder wireless transmission presents by far the most significant problem with regard to readout precision for the respondent enterprises. 17 enterprises are or were confronted with this problem (basis 18), of which only 2 enterprises had solved the problem at the point in time of the survey. The high margin of error with the readout of moving transponders presents a problem for 11 out of 16 enterprises, which was solved in 4 cases. A too small a range of readability is criticized by 13 firms (basis 18), could however be remedied in 7 cases. Only a minority of the enterprises encounter further problems, such as the damage of transponders through dampness or temperature fluctuations.

With regard to the required **period for increasing the readout precision to an acceptable level**, it is to be noted that no adjustment was necessary in only one out of 17 cases. Most of the enterprises still succeeded in solving their readout problems relatively quickly. 6 enterprises could increase the precision of their RFID systems within a month to an acceptable level, 6 others within the first six months of use or trial use. 3 firms required between 6 and 12 months, whereas only one enterprise did not solve the problems regarding readout precision even after a year. These figures substantiate the impression that technical problems when introducing RFID technology are of course virtually unavoidable, but can be relatively quickly solved by enterprises (teething troubles) and are therefore relatively lowly assessed in their relative significance compared with other hurdles.

5.4 Summary

The most important results of this survey are as follows:

1. **The "killer application" inventory shows big market potentials:** Automatized stocktaking in logistics and stock-keeping is the most deployed application of RFID. 22% of the respondents make use of RFID for this purpose. Furthermore, 60% of the

respondents want to conduct an inventory more often, if the inventory becomes definitely cheaper by using RFID.

2. **Insufficient accurateness of reading RFID transponders is only a "children's disease":** The collection of RFID transponders in operative areas, e.g. close to metal, is often considered as an essential problem. In fact, 70% of the interviewed RFID pioneer enterprises were able to solve their reading problems in less than half a year.
3. **Limited willingness to pay:** More than 70% of the respondents are not up to pay more than 20 Cent per passive transponder.
4. **Cutting-edge enterprises enlarge their activities:** 60% of the respondents already using RFID plan to enlarge their corresponding activities. None of them wants to stop its RFID activities.
5. **Dominance of inter-company RFID applications:** So far, most of RFID applications are used within an enterprise. Identification of stillages and shipping casks by passive UHF transponders is the main task.
6. **Standardization and integration are the most important hurdles**: Facets of standardization and integration of RFID technology in current process and information system architectures are seen as the most important hurdles for its use. Data protection concerns of customers and a unfavourable cost-profit relation is also seen problematic.
7. **Postulation for intensification of data protection statements:** Since of a possible denial of RFID technology by customers, 60% of the respondents consider an intensification of data protection statements necessary.
8. **Security has (yet) no relevance:** Security concerns in the context of RFID are not seen as a hurdle for investment in RFID.

6 Norms and standards concerning Radio Frequency Identification[15]

6.1 ISO 11784, 11785, and 14223/1[16]

ISO 11784 and ISO 11785 are international norms for contactless identification of animals and agricultural equipment using low frequency (134.2 kHz) RFID transponders. ISO 11784 specifies the structure of the identification code while ISO 11785 specifies the characteristics of the transmission protocols between transponder and reader. ISO 14223/1 is an extension of ISO 11784 and ISO 11785.

A 15 digit (3 digit country code in conformance with ISO 3166, 12 digit national ID code) number is specified in ISO 11784 that is supposed to be a globally unique identifier for a period of thirty years.[17] A physical form for the transponders is not defined to allow for use-case specific customisation.

The code structure is as follows:

Bit #	Encoded Information
1 Flag:	Animal (1), Non-Animal (0)
2-15	Field reserved for future use
16	Flag: Data Block existent (1), Data Block non-existent (0)
17-26	Country Code (ISO 3166 numeric-3)
27-64	National Identification Code

Data transmission takes between 15 (full duplex reading) and 50 (half duplex reading) ms.

ISO 11784/11785 transponders face criticism as the uniqueness of codes can not be guaranteed, minimum performance requirements are not stipulated, and patents impact implementations of the standards.[18]

ISO 14223/1 is based on ISO 11784/11785 and consists of three parts:

- Part 1:
  Radio Frequency Identification of Animals, Advanced Transponders – Air Interface
- Part 2:
  Radio Frequency Identification of Animals, Advanced Transponders – Code and Command Structure
- Part 3:
  Radio Frequency Identification of Animals, Advanced Transponders – Applications

[15] For a detailed overview of the ISO norms, c.f. Klaus Finkenzeller: RFID-Handbuch, 4. Auflage, August 2006.

[16] ISO norms can be purchased and downloaded from http://webstore.ansi.org/

[17] Pieter Hogewerf, Kees van 't Klooster: ISO 11784/11785 a Brief Historical Overview, http://www.wsava.org/MicrochipComm2.htm

[18] RFID News: ISO 11784/85 "Standard" with Blemish, http://www.rfidnews.com/iso_11784.html

ISO 14223/1 transponders contain the same ID code as ISO 11784/11785 ones, but in addition possess a larger memory and management functions for it. Transponders and readers are downwards compatible to ISO 11784/11785, i.e. ISO 14223/1 transponders answer their ID code to an ISO 11784/11785 reader, and ISO 11784/11785 transponders can be read by ISO 14223/1 readers.

To access the additional memory and functions of an ISO 14223/1 transponder, bit 16 is flagged to 1, data block existent. A system with an ISO 14223/1 reader can make use if the advanced features of the transponder.

6.2 ISO 10536

ISO 10536 is an international norm for contactless identification smartcards with a communication range of up to 2 cm (close coupling).

The standard series ISO 10536 consists of four parts. It is an international norm for contactless integrated circuit(s) cards with a communication range of up to 2 centimetres used for identification purposes. After initialisation (reset), ISO 10536 cards start communication with 9600 bit/s and can then be switched to higher data transfer rates.

The four parts of ISO 10536 describe

- the physical characteristics (part 1),
- the dimensions and locations of coupling areas (part 2),
- the electronic signals and reset procedures (part 3), and
- the answer to reset and transmission protocols (part 4).

Due to the small communication range and comparatively high production costs in reference to contact smartcards, ISO 10536 card systems have very small market presence.

6.3 ISO 14443

ISO 14443 is an international norm for contactless identification smartcards with a communication range of up to 20 cm (proximity or remote coupling).

The standard series ISO 14443 consists of four parts and related amendments.[19] It is an international norm for contactless integrated circuit(s) cards with a communication range of 10 to 20 centimetres (proximity cards) used for identification purposes. A data transfer rate of up to 424 kBit/s can be established, the frequency used is 13.56 MHz.

The four parts of ISO 14443 describe

- the physical characteristics (part 1),
- the radio frequency power and signal interface (part 2),
- the initialization and anti-collision (part 3), and
- the transmission protocol (part 4).

[19] http://wg8.de/sd1.html

ISO 14443 uses the terms PICC (proximity integrated circuit(s) card) for the contactless cards and PCD (proximity coupling device) for the readers. It describes two types of cards, type A and type B. The main differences between these two types regard signal modulation methods,[20] coding schemes, and protocol initialization procedures.

ISO 14443 chips are used in a variety of products. E.g. one kind of Philips' MIFARE cards or Machine Readable Travel Documents (MRTD) according to ICAO document 9303[21] is based on ISO 14443.

While the norm defines communication ranges between 10 and 20 centimetres, experiments showed that the communication between chip an reader can be eavesdropped at higher distances up to several metres.[22] Such eavesdropping has already been used to show that the cryptographic key used to protect the communication between chip and reader in case of Dutch MRTDs could be broken in approximately three hours.[23]

6.4 ISO 15693

ISO 15693 is an international norm for contactless identification smartcards with a communication range of up to 100 cm (vicinity or long range coupling).

ISO 15693 consists of three parts. It is an international norm for contactless integrated circuit(s) cards with a communication range of up to 100 centimetres (vicinity integrated circuit cards, VICC) used for identification purposes. A data transfer rate of to 1.65 kBit/s can be established, the frequency used is 13.56 MHz.

The three parts of ISO 15693 describe

- the physical characteristics (part 1),
- the air interface and initialisation (part 2), and
- the anti-collision and transmission protocol (part 3).

6.5 ISO 10373

ISO 10373 is an international norm defining test methods for cards containing data such as smart cards or magnetic strip cards. It consists of seven parts as follows:

- General (part 1),
- Magnetic Strip Technologies (part 2),
- Integrated Circuit Cards (part 3),
- Contactless Integrated Circuit Cards, Close Coupling / ISO 10536 (part 4),

[20] c.f. http://www.rfid-handbook.de/german/chipkarten.html#ISO14443

[21] c.f. http://www.icao.int/mrtd/Home/Index.cfm

[22] Thomas Finke, Harald Kelter: Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, http://www.bsi.bund.de/fachthem/rfid/Abh_RFID.pdf

[23] Harko Robroch, ePassport Privacy Attack, http://www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf

- Optical Memory Cards (part 5),
- Contactless Integrated Circuit Cards, Proximity Coupling / ISO 14443 (part 6), and
- Contactless Integrated Circuit Cards, Vicinity Coupling / ISO 15693 (part 7).

6.6 ISO 18000

The ISO 18000 “RFID for Item Management: Air Interface” series of standards currently contains seven parts and spans most of the frequency bands used in RFID.

- Generic Parameter for Air Interface Communication, for Globally Accepted Frequencies (part 1),
- Parameters for Air Interface Communication below 135 kHz (part 2),
- Parameters for Air Interface Communication at 13.56 MHz (part 3),
- Parameters for Air Interface Communication at 2.45 GHz (part 4),
- Parameters for Air Interface Communication at 5.8 GHz (part 5, withdrawn),
- Parameters for Air Interface Communication at 860 to 960 MHz (part 6),
- Parameters for Air Interface Communication at 433 MHz (part 7).

ISO 18000-7 covers active tags used in asset monitoring and location.

For an eighth part, ISO 18000-8, iP-X[24] has been proposed to ISO but is also currently being discussed for integration into ISO 18000-6.

The scope of ISO 18000-1 is to describe the reference architecture for radio frequency identification for item management and to establish the parameters that shall be determined in any standardised air interface definition in the ISO 18000 series. The subsequent parts of this standard provide the frequency specific values and value ranges from which compliance to (or non-compliance with) this standard can be established.

6.7 ISO 15961, 15962, and 15963

ISO 15961, 15962, and 15963 are international norms for RFID-based item management that define data content structures.

ISO 15961 focuses on the interface between the application and the data protocol processor, and includes the specification of the transfer syntax and definition of application commands and responses. It allows data and commands to be specified in a standardised way, independent of the particular air interface of ISO 18000.[25]

ISO 15962 focuses on encoding the transfer syntax, as defined in ISO 15961 according to the application commands defined in that international standard. The encoding is in a logical

[24] c.f. http://www.rfidjournal.com/article/articleview/2595/

[25] http://engineers.ihs.com/document/abstract/SSSJGBAAAAAAAAAA

memory as a software analogue of the physical memory of the RF tag being addressed by the interrogator.[26]

ISO 15963 describes numbering systems that are available for the identification of RF tags. A unique ID is required as part of the write operation to RFID tags. The unique ID guarantees that the information written to a tag is unambiguously written to the correct data carrier (tag). A unique ID is also required in read situations where the contents of the tag are tied to a specific item and that item needs to be unambiguously identified.[27]

6.8 ISO 10374

ISO 10374 is an international norm for automated identification of containers using active RFID transponders containing a 128 bit data set. ISO 10374 transponders work at 850 to 950 MHz and 2.4 to 2.5 GHz frequency ranges.

6.9 Electronic Product Code (EPC)

EPC allows for unique identification and tracking of tagged objects via internet.

EPCglobal Inc. is a non-profit organisation founded by GS1 (former EAN – European Article Numbering International) and UCC (Uniform Code Council), the two main barcode issuing associations.

EPC, the Electronic Product Code standardised by EPCglobal, is intended to replace EAN or UPC (Universal Product Code) numbers when RFID tags replace barcodes as identifiers on products.

EPC is a set of coding schemes for RFID tags, originally developed by MIT Auto-ID Center. EPC numbers start with a header identifying the encoding scheme used, which according to EPC Version 1.3[28] can be one of the following:

- General Identifier (GID), GID-96,
- Serialized version of the GS1 Global Trade Item Number (GTIN), SGTIN-96, SGTIN-198,
- GS1 Serial Shipping Container Code (SSCC), SSCC-96,
- GS1 Global Location Number (GLN), SGLN-96, SGLN-195,
- GS1 Global Returnable Asset Identifier (GRAI), GRAI-96, GRAI-170,
- GS1 Global Individual Asset Identifier (GIAI), GIAI-96, GIAI-202,
- DoD Construct, DoD-96.

The EPCglobal architecture allows the use of a variety of authentication technologies across its defined interfaces. It is expected, however, that the X.509 authentication framework will be widely employed within the EPCglobal network.[29]

[26] http://engineers.ihs.com/document/abstract/UUSJGBAAAAAAAAAA

[27] http://engineers.ihs.com/document/abstract/WLWBGBAAAAAAAAAA

[28] http://www.epcglobalinc.org/standards_technology/Ratified%20Spec%20March%208%202006.pdf

When an EPC number is read, the reading device can identify the object via internet by accessing the Object Name Service[30] within the EPCglobal network[31]. The EPCglobal Networks aims at exchanging data in real time to allow tracking of products.

EPC uses Object Name Service (technically based on DNS) to allow for unique identification of tagged objects (as opposed to identification of object class with barcodes).

6.10 ISO 69873

ISO 69873 is an international norm for tagging tools and clamping devices using RFID transponders.

[29] http://www.epcglobalinc.org/standards_technology/ratifiedStandards.html

[30] http://www.epcglobalinc.org/standards_technology/EPCglobal_Object_Naming_Service_ONS_v112-2005.pdf

[31] http://www.epcglobalinc.org/about/EPCglobal_Network.pdf

7 Summary

This deliverable introduces Radio Frequency Identification (RFID) from a technical perspective, targeting interested laymen who already have a basic knowledge of RFID. This deliverable is part of a number of FIDIS studies and is to be seen as a platform deliverable which mainly summarises and partly analyses the basics of the technology, areas of application, general threats, economic aspects and most relevant standards for RFID in the context of identity and identity management.

A summary of the details described in this deliverable is of limited use, especially as relevant conclusions are drawn in other FIDIS studies. As such, rather than distilling this collection of knowledge, below we present the relationship between the different FIDIS studies planned so far which this document is designed to underpin:

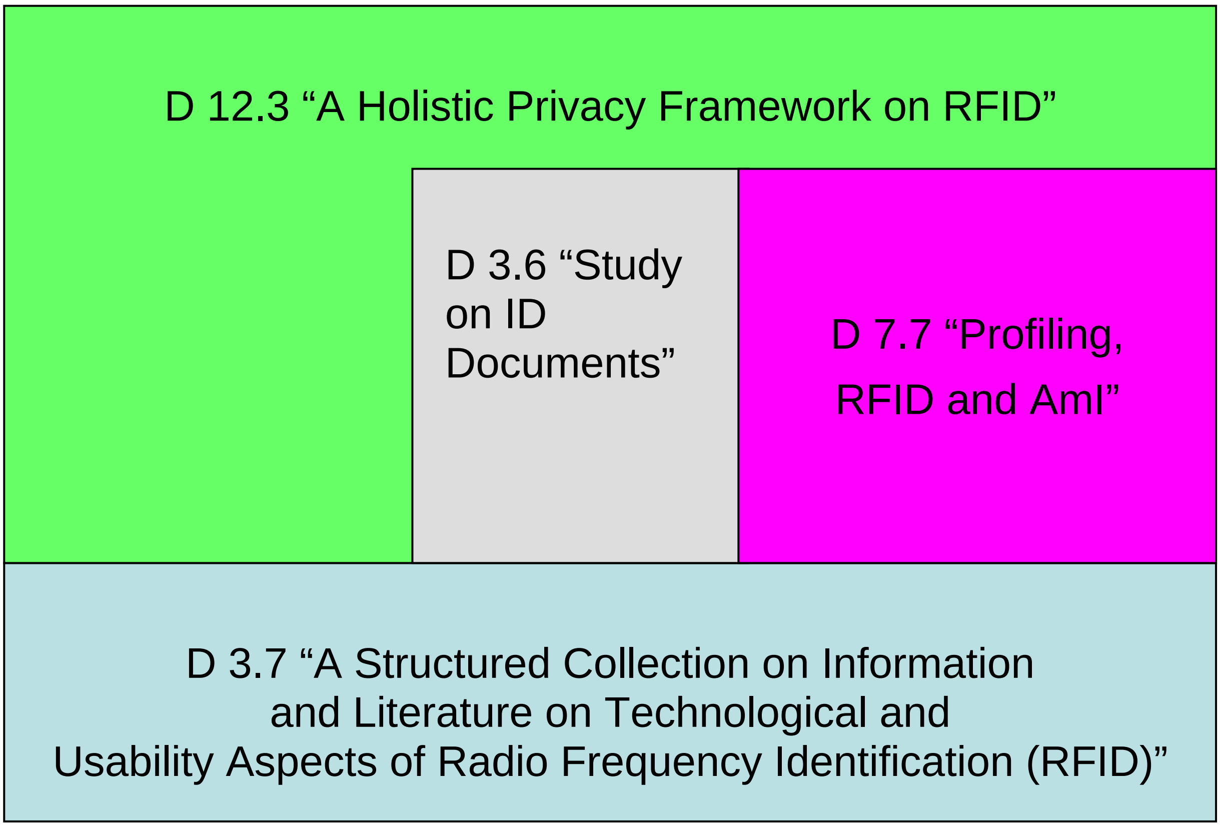
D 12.3 “A Holistic Privacy Framework on RFID”
D 3.6 “Study on ID Documents”
D 7.7 “Profiling, RFID and AmI”
D 3.7 “A Structured Collection on Information and Literature on Technological and Usability Aspects of Radio Frequency Identification (RFID)”

Figure 10: Relationship between FIDIS studies planned so far in the context of RFID

Clearly in addition to being a resource for the subsequent FIDIS work, this document is also of value to laymen beyond this work since it fills a gap between basic introductions to be found e.g. in Wikipedia, and scientific literature such as Finkenzeller’s “Handbook on RFID” (Finkenzeller 2006).

8 References

AIM Global, Why RFID chips can't infect cats – or computers, March 20, 2006, http://www.usingrfid.com/news/read.asp?lc=c62028cx673zn&version=printable

Auto-ID Center, '860MHz–930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification', Candidate Recommendation, Version 1.0.1, Technical Report. See http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf.

Department of Computer Science, Vrije Universiteit Amsterdam, *RFID Viruses and Worms*, Amsterdam, March 2006. See http://www.rfidvirus.org/,.

German Federal Office for Information Security (BSI), *Security Aspects and Prospective Applications of RFID Systems*, Bonn, October 2004.

Engel, C., 'Auf dem Weg zum elektronischen Personalausweis', *Datenschutz und Datensicherheit* 4/2006, pp. 207-210, Wiesbaden 2006.

Finkenzeller, K., *RFID-Handbuch*, 4th edition, München, August 2006.

Finke, T., Kelter, H., *Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems*, http://www.bsi.bund.de/fachthem/rfid/Abh_RFID.pdf

Garfinkel, S., Rosenberg, B., *RFID, Applications, Security and Privacy*. Addison Wesley, Boston 2006.

Hildebrandt, M., Meints (eds.), M., *FIDIS deliverable D7.7: RFID, Profiling and AmI*, Frankfurt a.M. 2006. Available via http://www.fidis.net/fidis-del/period-3-20062007/#c1095

Hogewerf, P., van 't Klooster, K., *ISO 11784/11785 a Brief Historical Overview*, http://www.wsava.org/MicrochipComm2.htm

Institute of Computer Science and Social Studies (IC), Department of Telematics, Albert-Ludwig University Freiburg, Germany: *Electronic Commerce Enquête*, http://www.telematik.uni-freiburg.de/ece.php, 2005 (last accessed at August 8th, 2006).

International Civil Aviation Organization (ICAO), 'Document 9303' and 'Standards for ePassports', Montreal 2004. Available via http://www.icao.int/mrtd/Home/Index.cfm

ISO/IEC standard 9798-2. *Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms*, 1999.

Juels, A., Rivest, R., Szydlo, M., 'The blocker tag: selective blocking of RFID tags for consumer privacy', *CCS'03*, October 2003, Washington.

Juels, A., 'RFID Security and Privacy: a Research Survey', IEEE Journal on Selected Areas in Communication 24, No. 2, pp. 381- 394, 2006. Available via http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf

Kfir, Z., Wool, A., 'Picking virtual pockets using relay attacks on contactless smartcard systems.', *Cryptology ePrint Archive*, Report, Tel Aviv University 2005.

Meints, M., Hansen, M. (eds.), *FIDIS deliverable D3.6: Study on ID Documents*, Frankfurt a.M. 2006. Available via http://www.fidis.net/fidis-del/period-2-20052006/#c1338

Official Journal of the European Union (EU): *Legislation*, L 123, Vol. 47, April 27th, 2004, see http://europa.eu.int/eur-lex/en/archive/2004/l_12320040427en.html (last accessed at August 8th, 2006).

Quack, K.: 'Zwei-Klassen-Gesellschaft bei RFID', *Computerwoche.de*, 16.06.2005, http://www.computerwoche.de/index.cfm?pageid=306&type=detail&artif=76851&category=353

Rieback, M., *Tag-borne attacks against RFID middleware*, Presentation in SAFE-NL workshop, 8 June 2006, Delft, The Netherlands.

Robroch, H., *ePassport Privacy Attack*, http://www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf

Sackmann, S., Strüker, J.: *Electronic Commerce Enquete 2005 - 10 Jahre Electronic Commerce: Eine stille Revolution in deutschen Unternehmen*. Institut für Informatik und Gesellschaft, Telematik, Freiburg i.Br., Germany, 2005.

Steel, D., 'Smart Dust', *University of Houston ISRC Technology Report*, Houston, March 2005. Available at http://www.uhisrc.com/FTB/Smart%20Dust/Smart%20Dust.pdf (accessed on 22nd of August 2006)

Strobl, J., Roth, C., (Eds.), *GIS und Sicherheitsmanagement*, pp. 91-100, Wiechmann, Heidelberg, 2006. Available at http://ifgi.uni-muenster.de/~raubal/Publications/RevBookSections/Tomberge&Raubal_Navigation%20mit%20RFID_AGIT_final.pdf

9 Bibliography

A collection on current articles dealing with security and privacy aspects of RFID is given in this chapter. It also is available in the FIDIS Online Bibliographic System via http://www.fidis.net/interactive/rfid-bibliography/.

[AF05] Manfred Aigner and Martin Feldhofer. Secure symmetric authentication for rfid tags. In Telecommunication and Mobile Computing – TCMC 2005, Graz, Austria, March 2005.

[AO05a] Gildas Avoine and Philippe Oechslin. RFID Traceability: A multilayer problem. In Financial Cryptography – FC'05, in Lecture Notes in Computer Science, pages 125-140, Springer-Verlag, Berlin Germany, 2005.

[AO05b] Gildas Avoine and Philippe Oechslin. A scalable and provably secure hash based RFID protocol. In The 2nd IEEE International Workshop on Pervasive Computing and Communication Security – PerSec 2005 (To appear), Kauai Island, Hawaii, USA, March 2005. IEEE, IEEE Computer Society Press.

[ART05] ARTICLE 29 Data Protection Working Party. Working document on data protection issues related to RFID technology. EU 10107/05/EN WP 105, January 2005. europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf.

[Avo05] Gildas Avoine. Adversarial model for radio frequency identification. Cryptology ePrint Archive, Report 2005/049, 2005. http://eprint.iacr.org/.

[Boo04] Book Industry Study Group. BISG Policy Statement. www.bisg.org/docs/BISG_Policy_002.pdf, September 2004.

[Bri04] Jerry Brito. Relax, don't do it: Why RFID privacy concerns are exaggerated and legislation is premature. UCLA Journal of Law and Technology, 8(2), Fall 2004. www.lawtechjournal.com/articles/2004/05_041220_brito.pdf.

[Cav04] Ann Cavoukian. Tag, you're it: Privacy implications of radio frequency identification (RFID) technology. www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=15007, February 2004.

[CM03] Vinod Chachra and Daniel McPherson. Personal privacy and use of RFID technology in libraries. White Paper, VTLS Inc., www.vtls.com/documents/privacy.pdf, October 2003.

[CW00] A. Cerino and W.P. Walsh. Research and application of radio frequency identification (RFID) technology to enhance aviation security. In National Aerospace and Electronics Conference NAECON 2000, pages 127–135, 2000.

[EHD04] Stephan Engberg, Morten Harning, and Christian Damsgaard Jensen. Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience. In The Second Annual Conference on Privacy, Security and Trust – PST, New Brunswick, Canada, October 2004.

[FDW04] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In Marc Joye and Jean-Jacques Quisquater, editors, 6th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2004, number 3156 in Lecture Notes in Computer Science, pages 357–370. Springer-Verlag, Berlin Germany, 2004.

[FJJ02] N. Frykholm, A. Juels, and M. Jakobsson. Jeu de paume: A security suite for handheld devices. Manuscript, 2002.

[FJPR04] Kenneth P. Fishkin, Bing Jiang, Matthai Philipose, and Sumit Roy. I sense a disturbance in the force: Unobtrusive detection of interactions with rfid-tagged objects. In Nigel Davies, Elizabeth Mynatt, and Itiro Siio, editors, 6th International Conference on Ubiquitous Computing (UbiComp 2004), number 3205 in Lecture Notes in Computer Science, pages 268–282. Springer-Verlag, Berlin Germany, 2004.

[FL04] Christian Floerkemeier and Matthias Lampe. Issues with RFID usage in ubiquitous computing applications. In Pervasive Computing, volume 3001 of Lecture Notes in Computer Science, pages 188–193. Springer-Verlag, Berlin Germany, 2004.

[FRJ04] Kenneth P. Fishkin, Sumit Roy, and Bing Jiang. Some methods for privacy in RFID communication. In 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), number 3313 in Lecture Notes in Computer Science, pages 42–53. Springer-Verlag, Berlin Germany, 2004. Also published as IRS-TR-04-010, Jun. 1, 2004.

[FSL04] Christian Floerkemeier, Roland Schneider, and Marc Langheinrich. Scanning with a purpose – supporting the fair information principles in RFID protocols. In Lecture Notes in Computer Science 35898 (2005), pages 214-231. Springer-Verlag, Berlin Germany 2005.

[FT05] Christian Floerkemeier and Frederic Thiesse. EPC technology. In D. Hutter and M. Ullmann, editors, Second International Conference on Security in Pervasive Computing (SPC 2005), number 3450 in Lecture Notes in Computer Science, pages 117–118. Springer-Verlag, Berlin Germany, 2005.

[Fus04] Roberta A. Fusaro. None of our business? Harvard Business Review, 82(12), pages 33–38, December 2004.

[Gar02] Simson Garfinkel. An RFID bill of rights. MIT Technology Review, page 35, October 2002.

[GHM+04] Nathan Good, John Han, Elizabeth Miles, David Molnar, Deirdre Mulligan, Laura Quilter, Jennifer Urban, and David Wagner. Radio frequency identification and privacy with information goods. In Workshop on Privacy in the Electronic Society – WPES (To appear), Lecture Notes in Computer Science, Washington, DC, USA, October 2004. Springer-Verlag.

[GJJS04] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. In T. Okamoto, editor, RSA Conference Cryptographers' Track '04, 2004.

[GKS04] Gunnar Gaubatz, Jens-Peter Kaps, and Berk Sunar. Public key cryptography in sensor networks – revisited. In Claude Castelluccia, Hannes Hartenstein, and Christof Paar et al., editors, First European Workshop on Security in Ad-hoc and Sensor Networks (ESAS 2004), number 3313 in Lecture Notes in Computer Science, pages 2–18. Springer-Verlag, Berlin Germany, 2004.

[GL04] Marc Girault and David Lefranc. Public key authentication with one (online) single addition. In Marc Joye and Jean-Jacques Quisquater, editors, Cryptographic Hardware and Embedded Systems (CHES 2004), number 3156 in Lecture Notes in Computer Science, pages 413–427. Springer-Verlag, Berlin Germany, 2004.

[GXW+04] Xingxin (Grace) Gao, Zhe (Alex) Xiang, Hao Wang, Jun Shen, Jian Huang, and Song Song. An approach to security and privacy of RFID system for supply chain. In IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), pages 164–168. IEEE Computer Society, 2004.

[Hjo04] Thomas Hjorth. Supporting privacy in RFID systems (master thesis), December 2004.

[HM04] Dirk Henrici and Paul M¨uller. Tackling security and privacy issues in radio frequency identification devices. In Pervasive Computing, volume 3001 of Lecture Notes in Computer Science, pages 219–224. Springer-Verlag, Berlin Germany, 2004.

[JB04] Ari Juels and John Brainard. Soft blocking: Flexible blocker tags on the cheap. In ACM Workshop on Privacy in the Electronic Society (WPES), pages 1–7. ACM Press, 2004.

[JLR00] S. Janson, T. Luczak, and A. Rucinski. Random Graphs. Wiley-Interscience Series of Discrete Mathematics and Optimization. Wiley, 2000.

[JMW05] Ari Juels, David Molnar, and David Wagner. Security and privacy issues in e-passports. Cryptology ePrint Archive, Report 2005/095, http://eprint.iacr.org/, 2005.

[JP03] A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. In R. Wright, editor, Financial Cryptography, number 2742 in Lecture Notes in Computer Science, pages 103–121. Springer-Verlag, Berlin Germany, 2003.

[JRS03] Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In 10th ACM Conference on Computer and Communication Security, pages 103–111. ACM Press, 2003.

[Jue04a] A. Juels. "Yoking-Proofs" for RFID Tags. In R. Sandhu and R. Thomas, editors, Workshop on Pervasive Computing and Communications Security (PerSec'04), pages 138–143. IEEE Press, 2004.

[Jue04b] Ari Juels. Minimalist cryptography for low-cost RFID tags (extended abstract). In C. Blundo and S. Cimato, editors, The Fourth International Conference on Security in Communication Networks – SCN 2004, number 3352 in Lecture

Notes in Computer Science, pages 149–164. Springer-Verlag, Berlin Germany, 2004.

[Jue04c] Ari Juels. Strengthening EPC tags against cloning. Manuscript, October 2004.

[KOH+05] Shingo Kinoshita, Miyako Ohkubo, Fumitaka Hoshino, Gembu Morohashi, Osamu Shionoiri, and Atsushi Kanai. Privacy enhanced active rfid tag. In International Workshop on Exploiting Context Histories in Smart Environments – ECHISE'05, Munich, Germany, May 2005.

[KP04] Heiko Knospe and Hartmut Pohl. RFID security. Information Security Technical Report, 9(4), pages 9–50, November–December 2004.

[Loe03] Larry Loeb. RFID: Menace to society or just plain dumb? — what's really wrong with radio frequency identification tags. IBM DeveloperWorks http://www-106.ibm.com/ developerworks/wireless/library/wi-roam16.html, November 2003.

[Luc04] D. Luckett. The supply chain. BT Technology Journal, 22(3), pages 50–55, July 2004.

[McA03] Alastair McArthur. Integrating RFID into library systems – myths and realities. In World Library and Information Congress: 69th IFLA General Conference and Council, 2003.

[McG04] Meg McGinity. RFID: Is this game of tag fair play? Communications of the ACM, 47(1), pages 15–18, 2004.

[MT04] Eiji Murakami and Takao Terano. Fairy Wing: Distributed Information Service with RFID Tags. In Computer Helping People with Special Needs (ICCHP 2004), number 3012 in Lecture Notes in Computer Science, pages 174–189. Springer-Verlag, Berlin Germany, 2004.

[MW04] D. Molnar and D. Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In 11th ACM Conference on Computer and Communications Security (CCS), pages 210–219. ACM Press, 2004.

[Oll95] M.M. Ollivier. RFID – a new solution technology for security problems. European Convention on Security and Detection, May 1995.

[OSK03] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. A cryptographic approach to "privacy-friendly" tags. RFID Privacy Workshop, 2003.

[REC04a] Damith Ranasinghe, Daniel Engels, and Peter Cole. Low-cost RFID systems: Confronting security and privacy. Auto-ID Labs Research Workshop, Zurich, Switzerland, September 2004.

[REC04b] Damith Ranasinghe, Daniel Engels, and Peter Cole. Security and privacy: Modest proposals for low-cost RFID systems. Auto-ID Labs Research Workshop, Zurich, Switzerland, September 2004.

[RKK05] Challenge-response based rfid authentication protocol for distributed database environment. In Security in Pervasive Computing, number 3450 in Lecture Notes in Computer Science, pages 70–84, 2005.

[SB04] A. Soppera and T. Burbridge. Maintaining privacy in pervasive computing – enabling acceptance of sensor-based services. BT Technology Journal, 22(3), pages 106–118, July 2004.

[SBE01] Sanjay E. Sarma, D. Brook, and Daniel W. Engels. Radio frequency identification and the electronic product code. Micro, 21(6), pages 50–54, 2001.

[Sch03] Esther Schindler. Location, location, location. ACM netWorker, 7(2), pages 11–14, 2003.

[SF03] Frank Siegemund and Christan Flörkemeier. Interaction in pervasive computing settings using bluetooth-enabled active tags and passive rfid technology together with mobile phones. In IEEE International Conference on Pervasive Computing and Communications (PerCom 2003), pages 378-387, 2003.

[SRS04] J unichiro Saito, Jae-Cheol Ryou, and Kouichi Sakura. Enhancing Privacy of Universal Re-encryption Scheme for RFID Tags. In Laurence T. Yang, Minyi Guo, and et al. Guang R. Gao, editors, Embedded and Ubiquitous Computing (EUC 2004), number 3207 in Lecture Notes in Computer Science, pages 879–890. Springer-Verlag, Berlin Germany, 2004.

[SS05] Junichiro Saito and Kouichi Sakurai. Grouping proof for RFID Tags. In 19th International Conference on Advanced Information Networking and Applications (AINA’05), volume 2, pages 621–624. IEEE Press, 2005.

[SWE02] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. RFID systems and security and privacy implications. In B.S. Kaliski Jr, C.K. Koc , and C. Paar, editors, 4th International Workshop on Cryptographic Hardware and Embedded System (CHES 2002), number 2523 in Lecture Notes in Computer Science, pages 454–469. Springer-Verlag, Berlin Germany, 2002.

[SWE03] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. Radio-frequency identification: Risks and challenges. RSA CryptoBytes, 6(1), pages 2–9, 2003.

[TUI+01] K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh. An ultra small individual recognition security chip. Micro, 21(6), pages 43–49, Nov/Dec 2001.

[VB03] I. Vajda and L. Buttyán. Lightweight authentication protocols for low-cost RFID tags. In 2nd Workshop on Security in Ubiquitous Computing, pages ?–?, 2003. In conjunction with Ubicomp 2003.

[Wan04] Roy Want. RFID: A key to automating everything. Scientific American, pages 46–55, January 2004.

[Wei03] Aaron Weiss. Me and my shadow. ACM netWorker, 7(3):24–30, 2003.

[WSRE03] S.A. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In First International Conference on Security in Pervasive Computing, number 2802 in Lecture Notes in Computer Science, pages 201–212. Springer-Verlag, Berlin Germany, 2003.

10 Abbreviations and Glossary

EPC- electronic product code

ICAO – International Civil Aviation Organization

IHVS - Intelligent Highway Vehicle Systems

ISO – International Standardization Organization

MRTD – machine readable travel documents

PET – privacy enhancing technology

RFID – radio frequency identification

SCM – supply chain management

electronic product code (EPC) - a code electronically recorded on an RFID tag [wikipedia April 2006]

PETs – are defined as "a coherent system of ICT measures that protects privacy [...] by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system." (Borking 1996, translation taken from Borking, Raab 2001).

RFID-system - may consist of several components: tags, tag readers, edge servers, middleware, and application software. The purpose of an RFID system is to enable data to be transmitted by a mobile device, called a tag, which is read by an RFID reader and processed according to the needs of a particular application. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, date of purchase, etc. [wikpedia April 2006]

RFID-tag - a small object that can be attached to or incorporated into a product, animal, or person. RFID tags contain silicon chips and antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver [wikipedia April 2006]

reader – see transceiver

sensor - a physical device or biological organ that detects, or *senses*, a signal or physical condition and chemical compounds; an electronic sensor is a type of transducer [wikipedia April 2006]

transceiver - a device that has a transmitter and a receiver which are combined [wikipedia April 2006]

transducer - a device, usually electrical or electronic, that converts one type of energy to another for the purpose of measurement or information transfer. Most transducers are either sensors or actuators [wikipedia April 2006]

transponder - a receiver-transmitter that will generate a reply signal upon proper electronic interrogation. [wikipedia April 2006]

ubiquitous computing - the method of enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user [Mark Weiser 1993, available at: www.ubiq.com/hypertext/weiser/UbiCACM.html]

11 Indices

11.1 Index of Figures

11.2 Index of Tables