FIDIS

Future of Identity in the Information Society

Title:	"A Holistic Privacy Framework for RFID Applications"
Author:	WP12
Editors:	Simone Fischer-Hübner (Karlstad University, Sweden) Hans Hedbom (Karlstad University, Sweden)
Reviewers:	Jozef Vyskoc (VaF, Slovakia) Maren Raguse (ICPP, Germany) Mark Gasson (University of Reading, UK)
Identifier:	D12.3
Type:	[Deliverable]
Version:	1.2
Date:	Wednesday, 30 April 2008
Status:	[Final]
Class:	[Public]
File:	fidis_deliverable_D12 3_v1.2.doc

Summary

The objective of this deliverable is to discuss whether it is possible to create a holistic privacy framework for Radio Frequency Identification (RFID) systems given current advances in the area and, if so, what such a framework would look like.

The deliverable gives an overview of privacy problems in relation to RFID from legal, ethical, social and technical standpoints and discusses and presents some of the efforts made to address these problems.

The overall conclusion is that much more research effort and technological development needs to be done before a true holistic framework can be constructed.

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 (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	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 (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	24.04.2007	• Initial release
0.2	16.05.2007	• Comments from Hildebrandt, Köpsell and Anrig added. First draft of solution chapter added
0.3	05.06.2007	• The legal part restructured
0.4	22.06.2007	• Added contributions from Hildebrandt and Meints
0.5	16.08.2007	• Restructured problem section, moved scenarios and moved first part of approach to introduction
0.6	16.08.2007	• Introduction to problem domain and the approach chapter rewritten
0.7	21.08.2007	• Reformulated the RFID basics and moved some parts of technical approaches to privacy friendliness
1.0	25.09.2007	• Final version
1.1	21.04.2008	• Updated version with minor errors and ambiguous statements corrected
1.2	25.04.2008	• Minor correction

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**)**	Hans Hedbom (Karlstad University).
2 (Introduction**)**	Simone Fischer-Hübner and Hans Hedbom (Karlstad University).
3 (RFID technology basics**)**	Stefan Köpsell (Dresden University of Technology) and Hans Hedbom (Karlstad University).
4 (RFID Case Studies and Scenarios**)**	Martin Meints (ICPP)
5 (The Problem Space**)**	Bernhard Anrig, Emmanuel Benoist, David-Olivier Jaquet-Chiffelle (VIP, Berne University of Applied Sciences), Eleni Kosta (ICRI/K.U.Leuven), Stefan Köpsell (Dresden University of Technology), Mireille Hildebrandt (VUB), Martin Meints (ICPP), Hans Hedbom and Simone Fischer-Hübner (Karlstad University).
6 (A Holistic Approach to Privacy-Enhancements**)**	Bernhard Anrig, Emmanuel Benoist, David-Olivier Jaquet-Chiffelle (VIP, Berne University of Applied Sciences), Eleni Kosta (ICRI/K.U.Leuven), Stefan Köpsell (Dresden University of Technology), Mireille Hildebrandt (VUB), Martin Meints (ICPP) , Hans Hedbom and Simone Fischer-Hübner (Karlstad University).
7 (Conclusions**)**	Bernhard Anrig, Emmanuel Benoist, David-Olivier Jaquet-Chiffelle (VIP, Berne University of Applied Sciences), Eleni Kosta (ICRI/K.U.Leuven), Stefan Köpsell (Dresden University of Technology), Mireille Hildebrandt (VUB), Martin Meints (ICPP), Hans Hedbom and Simone Fischer-Hübner (Karlstad University)

Table of Contents

1 Executive Summary

Businesses have always had a need to keep track of their inventory and assets. In the computerised age barcodes and other optically or magnetically readable media have been used to solve this task. However, these solutions have the precondition that they either need line of sight or physical contact in order to be interrogated. In later years, Radio Frequency Identification (RFID) technology has increasingly been used to solve the asset management and tracking problem. RFID technology has the advantage that it can be used without line of sight or physical contact. These properties have also inspired other uses besides asset management and tracking. Thus RFID is used nowadays in, or envisioned to be used in many types of applications for tracking, authenticity verification, matching, process control, access control and automated payment in military, medical, governmental and business applications. There is little doubt that these types of applications have benefited and will benefit from properties of the RFID technology, however, these properties and the possible omnipresence of RFIDs changes the informational landscape in a profound way and brings with it new threats and challenges within the privacy sphere. The fact that RFID technology is still in its infancy and that parts of the technology have strong limitations in both power and computational capabilities makes it very hard to apply well known and understood privacy protection techniques that normally rely heavily on cryptography. RFID also raises a number of ethical and legal issues that stem from this new informational landscape and it is very difficult to foresee the social consequences of a widespread use of the technology.

Commonly an RFID system consists of two parts: an RF- subsystem and a backend system. The RF-subsystem consists of RFID tags containing identification data and related information and RFID readers that interrogate the tags and send the data to the backend system. The backend system contains the components necessary to store, analyse and in other ways make use of the collected data.

This deliverable tries to answer the following research question: *Is it possible to create a holistic privacy framework for RFID systems given current advances in the area and if so what would such a framework look like.* The reason why we choose a holistic approach is that we do not believe that the privacy issues surrounding RFID can be properly addressed and solved without taking legal, technical, ethical, economical and social views into consideration.

In order to try to answer the question, we have first analysed and discussed the possible privacy problems that are associated with the RFID technology and the obstacles for reaching privacy-enhanced solutions. Both fictitious scenarios and real case studies are used as exemplification throughout the chapter. In the discussion we have tried to limit ourselves to RFID specific issues. This means that the discussion is highly centred on the RF-subsystem part, and the backend component is only addressed if the RF-subsystem places different requirements or introduces new privacy problems other than the ones traditionally present in "normal" information processing systems. The conclusion of the problem inventory is that there exist a number of problems and requirements that needs to be addressed. These issues are summarised in a problem list and associated with example scenarios.

In order to see if the problems and requirements can be addressed, different approaches to solutions are discussed. Within this discussion an overview of proposed guidelines for non-technical and technical means are presented and analysed.

The overall conclusions of the deliverable are the following:

- The use of RFID technology in several contexts and its role as a prime Ambient Intelligence enabler raises important data protection and privacy threats.
- The current legal privacy framework partly gives too much room for interpretation and does not always give clear answers with regards to RFID technology. Such issues are currently being addressed by the EU.
- We believe that in order to get a privacy friendly RFID system both the RF-subsystem and the backend system needs to provide privacy protection. Since the backend system presumably is under the control of the data controller while some parts of the RF subsystem is not (notably the RFID tag), it is of utmost importance that the RF-subsystem provides for its own privacy protection.
- Many proposals for Privacy Enhancing Technologies (PETs) for RFID exist - but only a few of them really seem to be feasible. One of the main problems is that low-cost RFID tags by themselves currently cannot offer any solution for strong privacy. Nevertheless, in the short term the mechanisms suitable for a given area of application should be implemented in order to increase the level of privacy the RFID system offers.
- The state-of-the-art at the moment is to have a privacy patchwork for RFID rather than a holistic and integrative approach. A lot more effort in terms of research and development seems to be necessary to finally get a true holistic privacy framework for RFID applications. Among other things, low cost RFID tags with better and stronger cryptographic mechanisms need to be developed, transparency and awareness needs to be raised and the incentives for manufacturers and users of RFID technology to develop more privacy friendly and secure solutions need to be increased.
- And finally, the combination of RFID and profiling, eventually coupled with many other privacy-sensitive means and techniques such as biometrics, may be a major privacy concern, as RFIDs, profiling and biometrics themselves already bear many risks, which are multiplied in combination.

2 Introduction

2.1 Background and Motivation (Setting the Scene)

Radio Frequency Identification (RFID) technology is increasingly used for various applications, including retail applications, transportation, aviation, healthcare, automatic toll collection, security and access control. RFID tags are tiny electronic radio tags that can be embedded in or affixed to objects for the purpose of identifying the object via a radio link. RFID readers can read the unique ID code and any other information stored in RFID tags remotely by sending and receiving a radio frequency signal. In an RFID system, RFID readers are connected to a backend system which processes the data read from tags and can link them to other data stored in backend databases. The use of RFID systems can enhance the efficiency and functionality of such applications, create new services and can provide further benefits and added value for the owner of RFID tagged items (e.g., smart fridges operating in combination with RFID tagged items, or the possibility to include warranty information on tags).

However, besides such benefits and opportunities, RFID technology also poses severe privacy problems. Privacy as an expression of the right of self-determination and human dignity is considered a core value in democratic societies and is recognised either explicitly or implicitly as a fundamental human right by most constitutions of democratic societies. In the era of modern information technology, an early definition of informational privacy was given by Alan Westin: "Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [2]. The German Constitutional Court had also defined privacy in its Census decision as the right to informational self-determination, i.e. individuals must be able to determine for themselves when, how, to what extent and for what purposes information about them is communicated to others.

RFID tags can either directly contain personal data (for instance identity cards will contain identifiable data such as name, birth dates (and in some countries personal number) or biometrics) or include data that could be linked to individuals (for instance individuals who carry or wear tagged items or who have implanted RFID tags). As pointed out in [4], RFID related privacy threats can basically be divided into privacy threats within the reader-tag system and privacy threats at the backend. Privacy threats within the reader-tag system comprise unauthorised reading and manipulation of information and real-time tracking of individuals. RFID readers can potentially secretly scan and track RFID tags that individuals passing by are wearing or carrying, without the concerned individual's knowledge or consent. Consequently, privacy principles implemented by the European Legal privacy Framework, such as transparency, informed consent, or more generally the right of informational self-determination, are at stake. Privacy threats at the backend include profiling and monitoring specific behaviour. Besides, there are security-related threats for the integrity, availability and authenticity of personal data stored on the tag or in the backend system.

The Art. 29 Working Party [12] and privacy and consumer organisations, such as CASPIAN [6] and EPIC [7] have voiced privacy concerns and discussed high-level privacy guidelines/requirements for RFIDs. Several trials and plans for using RFID in supply chain applications were confronted with protests by consumers, who felt that their privacy was at risk.

RFID related privacy problems cannot solely be addressed by legal and/or technical measures but require a holistic approach. For instance, RFID applications, such as RFID implants, even though they are legally compliant might raise ethical questions that need to be addressed as well. Besides, social aspects of user acceptance and trust also need to be taken into account. Hence, for elaborating privacy-enhancements for RFID application, first the privacy problems need to be analysed from technological, legal, ethical and social science perspectives. Such approaches to privacy-enhancements need then to comprise technical, legal, social and ethical measures that are technically feasible, enforce legal privacy principles, be regarded as ethical, are socially acceptable and trustworthy by end users and other concerned individuals.

In this deliverable, we will take a holistic approach to analyse problems and possible privacy-enhancements for RFID applications. Our analysis will be illustrated by a set of application scenarios which were partly already used in the FIDIS Deliverable 7.7 'RFID, Profiling and AmI'.

2.2 Related work

In recent years, several studies on privacy and security aspects of RFID systems have been conducted. Many of them, such as for instance the report on risks and opportunities of applying RFID systems ("Risiken und Chancen des Einsates von RFID Systemen") from 2004 [8], have focussed solely on technical security and privacy aspects and have not taken a holistic approach.

In 2006 a book called RFID Applications, Security, and Privacy edited by Simon Garfinkel and Beth Rosenberg was published [39]. The book is in essence a collection of articles written by a number of researchers, developers and privacy activists. The purpose of the book is to give a good overview of RFID applications, its underlying technology and the public policy debate, something which we believe it is doing quite well. This goal makes the book take somewhat of a holistic approach. However, it does not try to create or explore the possibilities of creating a framework or to bring the different viewpoints together in a holistic document.

In spring 2007 The National Institute of Standards and Technology (NIST) published Guidelines for Securing Radio Frequency Identification (RFID) systems [5]. In chapter 6 privacy considerations are discussed. This discussion is mainly centred on the US legal landscape and RFID considerations are specifically discussed in connection with OECD principles and Federal CIO Council Privacy Control Families (FCCPCF). The approach is not holistic but rather takes a security approach with a business perspective. The problems in the legal and ethical landscape are not analysed and discussed, except for the fact that some considerations mention the fact that it could be hard to comply with some of the principles in OECD and FCCPCF. Furthermore, the customer perspective is, in our view, poorly treated.

Recently, TNO and DG JRC – IPTs published an extensive study on "RFID Technologies: emerging Issues, Challenges and Policy Options" [4], which investigates RFID technologies and their socio-economic implications. It looked at technical, market, societal and legal issues in order to identify barriers and opportunities. Strengths, weaknesses, threats and opportunities, are also identified through the analysis of specific application areas. Although the study has thus another focus than our framework, it also includes a chapter on "Privacy Aspects of RFID", which is however, in contrast to our framework, discussing legal, social and technical privacy aspects as well as legal, self-regulatory and technical strategies to cope

with privacy threats in less details. Besides, it does not address specifically ethical privacy aspects.

Within the FIDIS project[4], deliverable 3.6 discusses RFID and biometrics and deliverable 7.7 discusses the effects of Ambient Intelligence systems with a focus on RFID. However, in contrast to this document, those deliverables are only analysing impacts but are not elaborating a holistic privacy framework including approaches to privacy-enhancements or discuss possible solution approaches in focused areas. The related findings of D7.7 and their consequences are presented in Chapter 5.2.4

2.3 Document Structure

The remainder of this document is structured into the following chapters:

Chapter 3 (RFID basics) will provide a brief introduction to RFID technology.

Chapter 4 (Scenarios) will present a set of seven application scenarios which should help to illustrate diverse privacy problems and the need for privacy-friendly solutions.

Chapter 5 (Problem Space) will discuss legal, ethical, socio-economic and technical security-related aspects of privacy problems that arise with RFID applications, which are illustrated by the scenarios of chapter 4.

Chapter 6 (A Holistic Approach to Privacy-Enhancements) will discuss approaches for more privacy-friendly RFID applications comprising legal, social ethical and technical means.

Chapter 7 (Conclusions) will summarise the main results and conclusions of this document.

[4] http://www.fidis.net

3 RFID technology basics

In this section, some general principles and basics of RFID systems which are required for subsequent chapters are described. For a more in-depth discussion, see also FIDIS deliverable 3.7 'A Structured Collection on Information and Literature on Technological and Usability Aspects of Radio Frequency Identification (RFID)'.

As with all other IT systems, RFID systems can vary in terms of complexity and implementation. However, NIST have defined the following common subsystem building-blocks:

- The RF subsystem: This subsystem consists of the RFID tag and the RFID reader[5] and is the part that performs identification and related transactions over a wireless interface. In this document we will interchangeably use the term RFID system or Front end system for this subsystem.
- The enterprise subsystem: This subsystem comprises of the computers and software necessary to process and store data acquired from the RF subsystem.
- The inter-enterprise subsystem: This subsystem is used to connect different enterprise subsystems to each other if information needs to be shared between organisations. In this document we will collectively refer to the enterprise subsystem and the inter-enterprise subsystem as the backend system.

RFID tags come in many different types and have different characteristics regarding e.g. power source, operating frequency and functionality. Thus they can be classified in a number of different ways. A common way to classify RFID tags in a general way is to divide them into active or passive tags. Active RFID tags have a permanent power supply. Hence these tags can perform "computations" continuously and independent from the environment.

Active tags also generally have much more computational power compared to passive ones. Hence they can do e.g. much better cryptographic operations.

Both properties make active tags much more appropriated for applying security and privacy protecting mechanisms. But on the other hand active tags are orders of magnitude larger than passive ones. Therefore they could not be used in most of the privacy threatened areas of application like unique tagging of objects.

Passive tags can, from a privacy and security standpoint, be further divided into:

- **basic, very low-cost tags**: tags which can mainly store some hundred bits of data and can execute only very limited operations which are far behind the needs for even basic cryptography
- **symmetric-key, low-cost tags**: tags which can do basic symmetric-key cryptographic operations

[5] Note: that the term RFID reader is used for a device that, depending on construction and application, can also write new data to RFID tags or change stored information.

- **public-key, more expensive tags**: tags which can also do public-key cryptography.

According to NIST [5] "the most prominent industry standard for RFID are the EPCglobal specifications and standards for supply chain and patient safety applications". EPCglobal divides the tags into different classes. Tags belonging to the EPCglobal Class-0 or Class-1 of the first generation have no security functionality. Tags adherent to the EPCglobal Class-1 generation 2 standard implement a 32 bit long password which can be used to trigger the kill process, which is used to deactivate a tag. Basic symmetric cryptographic functionality is integrated into EPCglobal Class-2 tags, as well as some form of authenticated access control, but no details are given by the specification.

The operating distance, data transfer speed and tag reading speed of an RFID system is dependent to a large degree on the radio frequency of the tag. In general one could say that the higher the frequency the higher the data transfer speed and the tag reading speed. High frequency tags are also usually designed to operate over longer distances [5]. However, high frequencies are also easier blocked or weakened by obstacles in the signal path. Table 1 summarises the frequencies and gives application examples for the different ranges.

Table 1: RFID frequencies [5]:

Frequency range	Example application
> 500 kHz	Access control, animal tagging, inventory control
1.95 MHz – 8.2 MHz	
13.553 MHz – 13.567 MHz	Access control, item-level tagging, contactless smart cards
433.5 MHz – 434.5 MHz	Supply chain applications
902 MHz- 928 MHz	Supply chain applications, toll road applications
2.40 GHz- 2.50 GHz	Real-time location systems, supply chain applications

RFID readers (or more precise the infrastructure part of the overall RFID system) can mainly be divided into *online* and *offline* types. Online RFID readers generally offer much more design options because they can communicate with whatever is necessary to achieve certain security or privacy goals. They have for instance full access to the whole backend system which can store all necessary data (like cryptographic keys, certificates etc.).

Data can be stored on the RFID tag itself, or in some backend database using the tag identifier as the primary key. Right now, storing the data in central databases and getting the data on-demand is more popular than storing data on tags. This is mainly because low-cost tags have a very small storage capacity. Other reasons are that holding data in more or less central databases offers the possibility of seamless data and software updates, as well as extended access control. Furthermore, one can argue that central databases are superior in terms of securing the data against attackers. Of course there have been a lot of examples of security breaches at large (banking) companies who could not protect user data in their databases.

4 RFID Case Studies and Scenarios

In this chapter a number of scenarios are presented that are later used in chapter 5 to illustrate most of the problems and requirements presented there. The chapter consists of seven scenarios of which scenarios 1-3 are newly constructed for this document, while the others are drawn from FIDIS deliverable 7.7. Some of the scenarios are fictional (scenarios 1-3 and 7) while the others are real world case studies (scenarios 4-6). In scenario 4 we have elaborated on the material as given in D7.7 to clarify certain aspects that we believe are important.

4.1 (S1) Scenario 1: Attack on an RFID System[6]

Transport Logistics Inc. is a logistics service provider. For tracking and tracing of goods they are using an RFID system. This is composed of fixed sensors in warehouses and mobile readers mainly used in lorries. The data stored in the mobile readers is imported into the central logistic system after the return of a lorry to a warehouse. Depending on the value of the goods and the preferences of their customers, per-item-tagging or palette-tagging is carried out.

On the morning of 15th February 2008, a palette with a manipulated RFID tag was scanned in when loading the palette at a customer's depot. The reader reported an error ("data set longer then expected"), but stored the information of the RFID tag. The palette was brought to a warehouse at noon, unloaded and scanned again. Again, the reader in the warehouse reported an error, but submitted the data to the central database. Fifty minutes later the driver of the lorry transferred the data from the mobile reader to the central system. However, the system was processing the data much slower than expected. At that time the system administrators were informed, but were not able to access the database management system any more. The system simply did not react to their requests.

Later it turned out that the manipulated data on the RFID tag was a program code that started being executed in the database. The code was copied again and again, first overwriting existing data sets and then adding data sets to the database until no hard disk space on the database system was left. At that moment (1 pm) the database simply stopped working. The tag was identified the next day and removed from the palette by the police.

The incident management team decided that all transportation activities should be carried out as planned, until no further route information for the lorry drivers was available. At the same time the problem management team started reinitialising the database and reloaded the content from the latest backup which was taken 16 hours ago. This took until 8 pm. At that time only a few lorries were on the road, while most of them were already back in the warehouses. At 8 pm import of the new transportation requests into the systems started. The first lorries could have been on the road again two hours later if the missing data, collected after the backup had been taken, was restored. However, re-collating the missing data started the next morning when all the drivers returned to the warehouses and reported their routes manually or partly automated based on available reader data. Two hours later the system had recalculated the transportation routes and at 11:30 the first lorries left the warehouses after being loaded and scanned.

[6] This scenario was inspired by a paper by Rieback *et al.* describing malware attacks on RFID system (see [46]).

In total the manipulated tag caused a complete downtime in logistic operations of almost 16 hours. The costs for the down time were later calculated at 1.4 M U.S. $.

4.2 (S2) Scenario 2: Enhanced proximity card

Access Ultra Inc. last year issued a new proximity card. In this system, in addition to traditional authentication of the card, the reader is authenticating itself with a relatively simple reader number to the card. The card has limited storage in which access procedures performed are stored decentralised in addition to the central access management systems' log.

The computing centre Calculations Inc. introduced these proximity cards six months ago. Recently, internal reviews uncovered that a secured room was accessed in an authorised way, and property (in this case several storage tapes) was removed unauthorised. Very quickly the number of the access card used was identified, and the corresponding user, a system administrator, was arrested. The data log from his local card was compared with the central log. At this point it became clear that his card was not actually used at the time. Most likely a cloned card had been used to facilitate an unauthorised access. This later also was confirmed by witnesses and a technical analysis. The innocent administrator was immediately released and received a new card.

The system was reconfigured to set an alarm if the card number was reused. Two weeks later the attacker was arrested while trying to gain unauthorised access to another room using a cloned proximity card. He told the police that he used a mobile reader to read out the data from the administrator's card while standing in a queue in a shop and used this data for cloning the card. He had simply followed the man when he went to work, so he knew where to try an attack. The stolen tapes were found in the attacker's home. They were not damaged. As the content was encrypted, the attacker had not been able to abuse the stored data from the tapes.

4.3 (S3) Scenario 3: An Identity Manager for RFID Tags

Article in a mobile computing journal, section "new developments":

Singsang Inc. announces new CKP-509 phone with RFID tag management functions -

Singsang Inc. is going to launch the new exclusive CKP-509 mobile phone onto the market end of February 2011. This phone integrates advanced management functions for RFID tags according to the EPC global 4.0 standard. […]

The phone has an integrated RFID reader and writer and is able to detect RFID tags in reading range. In addition it is able to take over access control by changing the cryptographic key from the vendor's default key to a managed one. It also is able to communicate with V4.0 compliant RFID readers. This enables the transfer of the access key in an encrypted way to the reader so that the tag can be accessed by the reader. Transfer of keys to readers can be done (semi-)automatically based on policies, so that in defined cases no user interaction is necessary. At the same time the phone logs any access to the tag. A sophisticated log file analyser called "data track" allows log file analysis and informs the user of who accessed the tag and for what purpose.

According to the EPC 4.0 standard, all communication between management device, reader and tag is encrypted (AES, 256 bit key). Key exchange is done using asymmetric cryptography. Reader and phone bear a certificate for identification; certificates can be verified against the existing public key infrastructure (PKI), operated by EZ-Trust.

4.4 Scenarios from FIDIS D7.7

4.4.1 (S4) Case study: the Metro Future Store in Rheinberg[7]

In Rheinberg, Germany, the Metro group as the third largest retailer in the world runs the so-called "Future Store", in which the use of RFID is being tested.[8] The testing exceeds the use of RFID tags in the supply chain, as the tags are used directly in the shop with at least a selected number of products. Functions and services that use (or plan to use) RFID are:

- Smart shelves within the store for automated positioning of products and automated ordering if availability of a product falls short of the predefined number
- Smart weighing machines which automatically detect the product and calculate the price
- Electronic price tags at the shelves
- Info terminals, similar to those using barcodes
- Advertisement screens showing videos to advertise products
- Intelligent shopping trolleys (integrating the so-called personal shopping assistants - this assistant works together with the customer loyalty card and allows checking of the customer's bonus account, displays information about products and advertisements received via WLAN)
- Automated teller systems

In addition to the improvements of the logistic chain and better services within the shop, customer loyalty cards with hidden RFID tags were also issued to the customers until April 2004.[9] In combination with hidden readers in the store, the loyalty cards were used to do personalised profiling on the customers. In addition, adjustment of offers to the wishes and needs of the customers is a defined purpose for which this card is used.[10] While this additional purpose was part of the declaration of consent within the contract of the customer loyalty card, the users were not informed about the use of RFID tags in the cards and corresponding readers issued at the "Future Store".

Other interesting aspects of this pilot project are technical abilities of the shopping assistant, a tablet PC integrated into the shopping trolley manufactured by Wincor Nixdorf International.

[7] All web pages cited in this chapter were accessed on 21st of April 2008.
[8] See http://www.future-store.org/servlet/PB/-s/68lq0912kjivf4hqf0149asnp3spni0/menu/1007054/index.html
[9] See http://www.spychips.com/metro/overview.html
[10] See http://www.spychips.com/metro/scandal-payback.html

They enable multi-channel retail, including the following functions: "The shopping assistant tracks the shoppers' movement using wireless LAN software from California based Ekahau and displays location-specific personalised shopping lists, favourites and special offers. The system can offer discounts on items related to those put in the cart. It can also trigger in-store signs. So if the shopper puts Pringles in the cart, an ad for Coca-Cola might be displayed. Shoppers who scan all their items can have the information communicated to a cash register wirelessly and checkout quickly."[11]

While it is documented that hidden RFID tags in the customer loyalty cards were used to activate advertisement displays showing video clips, it is not clear whether this was used in the way described above. After the RFIDs in the customer loyalty cards were uncovered by the consumer protection organisations CASPIAN[12] and FoeBuD[13], the Metro group withdrew these cards and issued traditional ones.[14] Given the ability of the shopping assistant to read traditional customer loyalty cards (via magnetic stripes or barcodes), profiling of customers is still done and adopting advertisements on displays is technically and legally possible.

Comment: Note that it is still possible to do personal profiling without explicit identifiers like loyalty cards. The Art.29 working party gives the following example in [12]: "A further example could be where the use of RFID tags can lead to the processing of personal data, even when RFID technology does not involve the use of other explicit identifiers. Take the hypothesis where person Z walks into Shop C with a bag and the products in it (more likely a jumble of numbers) are revealed. Shop C keeps a record of the numbers. When person Z returns to the shop the next day, he is rescanned. Product Y, that was scanned yesterday, is revealed today – the number is for the watch he always wears. Shop C sets up a file using the number of product Y as a 'key'. This allows them to track when Person Z enters their shop, using the RFID number of his watch as a reference number for him. This allows shop C to set up a profile of Person Z (whose name they don't know) and to track what he has in his shopping bag on subsequent visits to Shop C. By doing this, Store C is processing personal data and data protection law will apply". This example also highlights that the distinction between personal and non personal data becomes more blurred and that the context is becoming an increasingly more important factor when deciding if data is personal or not.

4.4.2 (S5) Case-study: Usage of RFID Technology in Educational Settings

Besides the many applications of RFID technology in logistics and other related fields, end-user scenarios for educational settings (e.g. museums and exhibitions) are also possible usage scenarios. By adding RFID tags and RFID readers to the exhibits, new possibilities with regard to interactive presentation and augmented experience for the visitors arise. Up till now, over a hundred museums worldwide are experimenting with ubiquitous technologies (RFID, Wi-Fi, etc) in their exhibitions [91].

An RFID enhanced educational environment is presented in Figure 1 from the technological perspective. At the start of his museum visit, the visitor gets an RFID token (e.g. as a card or embedded into a personal information device). Furthermore, he enrols himself by storing a

[11] http://www.rfidjournal.com/article/articleview/489/1/1/
[12] See http://www.nocards.org/
[13] See http://www.foebud.org
[14] See http://www.foebud.org/rfid/metro/

user profile into the museums RFID infrastructure. This profile can contain personal information, such as personal interests or the user's age ([92], [91]). When passing an exhibit, the user can use the RFID tag to acquire personalised information about the individual exhibit or trigger the interactive part of an exhibit, when in its proximity.

Depending on the individual context of the visitor and the stored profile, personalised information is delivered onto an information kiosk, which is attached directly to the exhibit, or onto the user's personal information device. Additionally, the system can track the visitor by taking photos and delivering additional resources. After the museum visit, these can be accessed on a personalised webpage on the Internet [91].

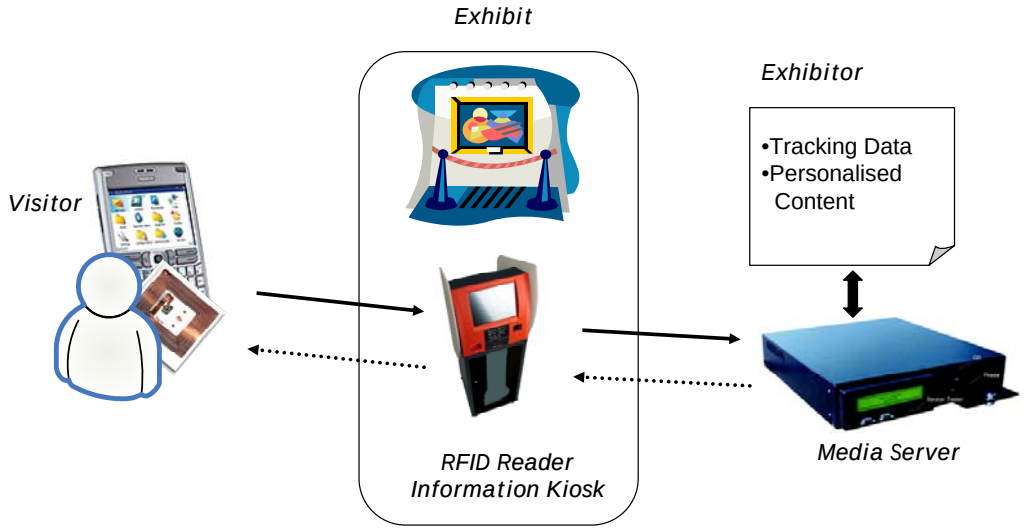

Figure 1: Possible usage scenario for RFID technology in educational settings

Furthermore, the exhibitors get the opportunity to track the behaviour of their visitors in order to enhance the exhibition or in order to gather information about the success of the installed exhibits. While this approach can be beneficial for both parties (visitor and exhibitor) by delivering information that could not be gathered by a static exhibition, usability and privacy protection requirements need to be addressed. Especially with regard to the perceived risk of RFID technology, users might not want to use this kind of technology to be tracked when visiting a museum [91].

4.4.3 (S6) RFID at the CVS Corporation

The CVS Corporation, listed at the New York Stock Exchange (NYSE), is the largest pharmacy chain (based on store count) in the United States, with 4087 stores. Since May 2002 CVS joined the Auto-ID Center at Massachusetts Institute of Technology (MIT) and began in 2003 with the so-called project "Jump Start" ([39]: 201ff.). The target of this project is a full-scale trial of RFID on 10 selected drugs.

There are a number of reasons why CVS is involved with RFID. The main reasons are:

- Pharmaceuticals are different from other consumer products such as, e.g., tooth brushes:
  - They are high value goods.
  - They sometimes have a very long time on the shelf (up to three or four years before they are sold).
  - In the United States, tamper-proofness of pharmaceuticals in the logistic chain and in the shops has been an issue since the Tylenol scandal in 1982, where Tylenol was adulterated with cyanide and as a consequence a number of consumers died.
- Up to 2002, EPC global[15] has not addressed the specific needs of the pharmaceutical industry including:
  - Integrating the National Drug Codes (barcodes) into the EPC;
  - The need for privacy in the health care sector and
  - The regulatory requirements defined by the U.S. Food and Drug Administration (FDA).

CVS is testing RFID on a per item basis. Drug bottles are RFID tagged and transported using standard boxes which are also tagged. There are a number of potential improvements in processes that are tested at CVS. The most important are:

- Improvement of drug management at the manufacturer and in the distribution centres of CVS: errors in the delivery such as wrong types or numbers of drugs can be detected easily;
- Improvement in drug management in the stores: the central systems know how many goods are left in the smart shelves even in cases where they are in the wrong place on the shelf (supply management);
- Improved handling of out-of-date items, recalls, returns and damages;
- EPC stored on RFID can be used to detect certain types of mistakes or manipulations of drugs for example in cases where used or cloned RFID tags are used.

The project comes with a number of technical innovations. A number of improvements with respect to reader technology, such as multiple antennas for one reader or the swivelling of boxes when they pass the reader, were applied. But accuracy of the reading process still is a problem. Further testing for example of two-way tags that act as a proxy for tags transmitting EPCs is needed.

CVS does not hand out drugs tagged with RFID to consumers for privacy reasons. Tags are removed in the shop. To ease this, special tags with a perforation to remove the tag from the adhesive pad are used.

[15] EPC global Inc. is a none-profit organisation doing standardisation work with respect to the use of RFID in retail and the Electronic Product Code (EPC); see http://www.epcglobalinc.org/.

4.4.4 (S7) Scenario for social inclusion

In the framework of the European accessibility policy, the city of Milan (Italy) did some public investments in a navigation support system based on RFID technology so as to equip some administrative buildings of the city. This system will allow disabled people or people with impairment to become self-sufficient and to have access to the offices.

During the first usage period, some problems occurred, but without significant repercussion. However, one day, because of tag-collisions[16], some people got lost and one person suffered substantial damages. He broke his leg by missing some steps of a staircase. According to the device he thought that he was on the second floor, but in reality he was on the third and regrettably, on the second floor there is a staircase with lesser steps then on the third floor. After this incident, it was decided to replace all reader devices by a new type of reader, comparable to the "agile reader"[17] in order to solve the collisions problem.

In order to forget this regrettable incident and stimulate the future users, the newspaper "Periodico di Milano" wishes to publish an article on the new system by interviewing people.

Two friends, one blind and another with low vision capability are very happy with the new navigation support system. They are able without human assistance to reach any room, and any place inside the buildings:

> *"Before, it was very difficult to progress in a building without a good knowledge of it because most of the signalisation is graphical (even for the toilets). And even if the lifts have in general a Braille conversion of the information related to the floors, only very few are equipped with a voice-based interface to indicate where you actually are, for example on the fourth floor or on another one selected by other person.*
>
> *Now, thanks to the navigation system, we are independent and we can move in complete freedom and safety. It is easy: at the entrance of the building a small device is offered and helps us to progress in the building. This device communicates with all RFID sensors and indicates to you by voice interface the right path to follow."*

4.5 Summary

In this chapter, three use cases and four scenarios for future systems using RFID are presented. The use cases refer to existing implementations of RFID systems. The scenarios are fictitious and show in a balanced way positive and negative potential developments of RFID technology and the corresponding use cases.

In the following chapters these use cases and scenarios will be used as a background for the analysis of the problem and solutions domain with respect to RFID from the perspective of various disciplines.

---

[16] Tag-collision: Tag collision occurs when more than one transponder* reflects back a signal at the same time, confusing the reader. Source: http://www.rfidjournal.com

[17] Agile reader: An agile reader is one that can read tags operating at different frequencies or using different methods of communication between the tags and readers. Source: http://www.rfidjournal.com

5 The Problem Space

5.1 Introduction

RFID technology raises privacy concerns that have technical, strong legal, ethical and socio-economic aspects. Hence, we believe that there are problems and issues that will not be addressed or overlooked if treated from only one angle. Moreover, there are privacy problems that cannot be satisfactorily solved by just one discipline. Because of this, we advocate a holistic approach for analysing the privacy problem space of RFID applications. In this section we will look at the problem space of RFID and the possibilities of reaching privacy-enhancing solutions from multidisciplinary perspectives, and so technical, legal, socio-economical, and ethical aspects will be addressed.

Because of the different RFID technologies and the multitude of applications, solutions for a holistic privacy framework for RFID have to solve a great variety of problems and have to take into account a whole range of assumptions, constraints and requirements. Some of them are common within the general problem domain of other holistic privacy frameworks - but many are very specific to the area of RFID.

As mentioned before, RFID related technology and solutions could be divided into two main parts: the basic RFID infrastructure (RFID tags and RFID reader) and the backend system which processes the data and in most cases facilitates the benefits of RFID systems. According to [4], RFID related privacy threats can basically be divided into privacy threats within the reader-tag system (i.e. within the basic RFID infrastructure) and privacy threats at the backend. The problem of unauthorised reading of information stored on a tag when there is absence of appropriate means of protection was illustrated in scenario S2 (Enhanced Proximity Card), where unauthorised read access enabled the cloning of a tag. The possibility to track the locations of persons wearing tags and associated privacy problems were illustrated by scenarios S4 (The Metro Future Store in Rheinberg), S5 (Usage of RFID Technology in Educational Settings), and S7 (Scenario for Social Inclusion). Privacy threats at the backend include function creep, the aggregation of personal data, profiling and monitoring specific behaviour. Scenario S4 illustrated how tags on customer loyalty cards in combination with hidden readers in the store were used to secretly perform personalised profiling of customers in the store.

Besides those privacy threats within the reader-tag system and backend system, there are security-related threats for the integrity, availability and authenticity of personal data stored on the tag or in the backend system, as for instance illustrated by Scenario S1 presenting a malware attack on an RFID system. The backend system usually comprises well known and understood server based technologies. Therefore similar privacy and security related risks arise from the RFID backend as they arise from every other similar infrastructure with the difference that often invisible collection points are used and data subjects might be less aware of the fact that their personal data are collected and processed. To solve the problems in the backend system one could apply the already available security and privacy protecting mechanisms. Nevertheless it has to be emphasised that these protection mechanisms need to be implemented addressing all the known problems with usability, manageability, rising costs, etc.

In this chapter, we will not discuss the problems that the backend systems have in common with any server based technology, but rather take a more detailed look at some of the RFID specific constraints and privacy problems both in the front end and backend system, and at obstacles for reaching privacy-enhancing solutions, from a multidisciplinary perspective, and relate them to our example scenarios in chapter 4. Section 5.2 will discuss the legal aspects while Section 5.3 ponders on the ethical view point. In Section 5.4 socio-economic and RFID technology inherent problems and requirements will be analysed and the technical and administrative security area will be discussed in Section 5.5. The chapter concludes with a summary of the different problems discussed and their relation to our example scenarios is presented.

5.2 Legal aspects

The deployment of RFID applications raises several legal questions regarding privacy and data protection as RFID tags can be used as the medium for collecting, transmitting or storing personal data, as well as tracing devices for the location of natural persons. In this chapter we will set out the legal aspects relating to data protection in RFID applications in order to define the borderlines for their 'Holistic Privacy Framework', examining also what kind of tracking and tracing possibilities arise from the use of an RFID enabled device or from RFID implants.

In the pages that follow it will be examined how far RFID applications raise privacy problems from the legal perspective. For this, we will analyse if, to what extent and in which way the European current legal framework on data protection applies to RFID applications. It will particularly be looked into when the information stored in an RFID tag qualifies as personal data (i.e. whether there is a privacy issue) and falls under the field of application of the data protection directive (see section 5.2.1) and how far the e-Privacy Directive applies (Section 5.2.2). Furthermore, Section 5.2.3 will discuss legal issues concerning RFID that are under debate and/or not straightforwardly answered. Finally, related findings of FIDIS deliverables 7.7 (RFID, Ambient Intelligence and Profiling) and 7.9 (Ambient Law) will be summarised in Section 5.2.4.

5.2.1 Information in RFID tags that qualify as personal data

The provisions of the European legal framework on data protection do not apply *de facto* to all information stored on an RFID tag. The collection and processing of data via RFID technology is covered by the provisions of the data protection directive [9] only when the information stored in the RFID tag refers to an identified or identifiable natural person – thus qualifying as personal data – or when this information can be linked to other personal data (Art. 2 (a) data protection directive).

Besides the obvious cases of having an RFID tag implanted in the body of a natural person, it will be examined if and under what conditions an RFID tagged object or the information stored in an RFID tag can be considered as personal data. Vaguer are the cases when the information on the RFID tag cannot be directly linked to a natural person, or at least some effort is needed. How easy shall the identification be? Recital 26 of the data protection directive reads that in deciding whether data could be used to identify a particular person "account should be taken of all the means *likely reasonably* to be used either by the controller or by any other person to identify the said person" (emphasis added). Thus the recital sets two

criteria for identifiability: the probability and the difficulty, which tend to be interlinked. In any case it is supported that the term 'personal data' should include all data about a person (including economic, professional etc. data) and not only data about the person's personal life [10]. This breadth of the conception of personal data means that data are usually presumed to be 'personal', unless it can be clearly shown that it would be impossible to tie them to an identifiable person (that is, unless the data are truly anonymous) [11]. The interpretation of the Member States regarding the ease of identification differs significantly between them. The data protection laws of France, Germany and Sweden for instance talk about "means for identification which are *reasonably capable* (as opposed to likely) of being put to use" [72], p. 44].

In order to achieve a common approach towards RFID technology at European level, a common notion of what is perceived as personal data and what entails their processing is necessary. The directive applies, without question, when information about an individual, such as his name, age, nationality etc., is directly stored on an RFID tag. Some RFID tags however may contain information that seems anonymous at a first glance. This information might nevertheless be easily associated to an individual, by linking it to information stored in a back-end database for instance and therefore its processing falls under the scope of application of the data protection directive [70]. Such cases that are rather common in relation to RFID technology shall be handled in a common way from the Member States.

As the Article 29 Data Protection Working Party[18] has already pointed out, it is essential in the case of data collection through RFID tags first of all 'to determine the extent to which the data processed relates to an individual and [secondly] whether such data concern an individual who is identifiable or identified.'[12]. In various applications biometrics are stored on an RFID tag. Although in most of the cases the legal framework on data protection applies, as biometric data from their very nature reveal information about a specific natural person, Article 29 Working Party has already pointed out in its "Working document on biometrics"[13] that "*most* biometric data imply the processing of personal data"(emphasis added)[13]. The Article 29 Working Party has recently adopted an opinion on the concept of personal data [90], attempting to clarify the notion of identifiability. The Working Party admitted that when it comes to "directly" identified or identifiable persons, the name of the person is indeed the most common identifier and in practice the notion of "identified person" implies most often a reference to the person's name [90]. However "identifiability" can be interpreted in a very broad way, depending on the circumstances of the case. Therefore in the context of RFID application, when the use of RFID allows the identification of a natural person with high degree of certainty, then the data protection legislation will apply.

In the 'Metro Future Store in Rheinberg' (S4) scenario the personal information about the customers is stored in the customer loyalty cards with hidden RFID tags. The data refer to an identified customer and their processing consists processing of personal data. However, not only the loyalty cards, but also the products were RFID tagged. The Metro Future Store had the possibility by means of hidden RFID readers to combine the products the customers were

[18] Under Article 29 of the Data Protection Directive, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data is established, made up of the Data Protection Commissioners from the Member States together with a representative of the European Commission. The Working Party is independent and acts in an advisory capacity. The Working Party seeks to harmonise the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics.

buying with the information on their loyalty cards in order to do personalised profiling. The customers should be informed that their personal data are being processed and the privacy principles set out in the European data protection legislation (that will be further analysed) shall be respected. In general it is to be mentioned that even if an RFID tagged product does not qualify as such as personal data, when it is linked to an identified or identifiable natural person through the payment via a credit card, an invoice or a loyalty card (as in the aforementioned example), then there is processing of personal data [[14], p. 24].

It is important to note that even if a customer is not identifiable via a credit card, he may be profiled on the basis of his behaviour in the shop and be confronted with refined types of price-discrimination (offers made on the display of his trolley). It is presently unclear whether this turns the data into personal data, and one may doubt whether the profile or the profiling techniques would be accessible as they may be protected by means of intellectual property, or simply be considered a trade secret. In this case the supermarket does not know the customer by name and the RFID technology does not involve the use of other explicit identifiers. According to the Article 29 Working Party (as commented at the end of scenario S4), in our example when a customer can be linked to a unique code on a tag (e.g. his watch) and a profile linked to this unique code can be set up, the supermarket is processing personal data and data protection law will apply ([12], p. 7). However opposite opinions can also be supported. The Dutch Ministry of Justice for instance in its Guidelines for personal data processors states with regard to the issue of identifiability: "A person is identifiable *if the person's identity can be established reasonably, without disproportionate effort* (emphasis added). In other words, you must be able somehow to establish a connection between the data and the person. […] If actual identification is reasonably excluded because of encryption of the data and/or agreements about the access to the data, the person cannot be identifiable. The actual situation is always the determining factor" ([73], p. 13, 14). If this approach is followed, then the example of setting up a profile on the basis of a unique product code on a tag (e.g. the watch of a customer) is not enough to justify processing of personal data, if the identity of the person cannot be established reasonably. [[14], p.24], [[73], p.14]. So it would not be easy to create access, even if art. 12 or 15 of the Directive would apply. The Working Party in its Opinion makes the judgement whether the processing of particular data concerns personal data dependent upon both the purpose and the context where they appear, while even allowing the same data to count as "personal data" with regard to one data controller while not counting as "personal data" with regard to another [90]. The Opinion did not shed clear light on the questions regarding the use of information in RFID applications and when they qualify as personal data. If any data that can at some point be related to an identifiable person is considered as a personal data, then in the case of wide-spread use of RFID systems ALL DATA will be personal data because of the possibility to link them. Of course the final decision will be made on a case by case basis, taking into account the specific conditions of every application or system. The Working Party considers that the technological state of the art at the time of the processing, as well as the future technological possibilities during the period for which the data will be processed, have to be considered. Identification may not be possible today with all reasonable means in use. Since technology is developing with great speed, in many cases it will not be possible for the controller to "guess" the means that might be used within some years, let alone after 10 or more years, a fact that raises the question whether we shall apply the data protection legislation in all RFID applications, following a "just-in-case" model.

5.2.2 What laws / directives apply?

As already described above, when information stored on the RFID tag or when the RFID tag can be linked to other information that refer to an identified or identifiable natural person, the provisions of the data protection directive regarding the processing of those data apply. When RFID tags are used in a medical environment (where health data are processed), the additional protection foreseen in the data protection directive for sensitive data[19] will apply. This means that the processing of health data is prohibited unless the data subject has given his explicit consent.[20] However these data can be processed when they are required for preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services.[21] Therefore when health data are stored in the tag of a hospital patient, what the purposes of the processing of those data are needs to be examined. When the health data are processed for one of the aforementioned purposes, then the processing is allowed. However, it is not allowed to store health data in the RFID tag, when it is used only for enhancing the identification procedure in the hospital. In such a case no health data shall be stored in the tag.

The European legal framework for the protection of personal data consists not only of the data protection directive, but also of the e-Privacy directive, which regulates specific issues regarding the processing of personal data in the electronic communications sector. The directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services and public communications networks.

According to Article 2 (d) of the Framework Directive [15] "*public communications network* means an electronic communications network[22] used wholly or mainly for the provision of publicly available electronic communications services[23]". The term '*communication*' is defined in Article 2(d) e-Privacy directive as "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information".

---

[19] Art. 8 data protection directive

[20] Or one of the other exceptions described in Article 8 (2) data protection directive apply.

[21] Art. 8 (3) data protection directive

[22] '*Electronic communications network* means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed' (Art. 2 (a) Framework Directive).

[23] '*Electronic communications service* means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks' (Art. 2 (c) Framework directive).

The e-Privacy directive aimed at protecting the personal data and the privacy of the users of publicly available electronic communications services, regardless of the technologies used (Rec. 4 e-Privacy directive). However the rapid development of RFID technology has raised concerns over whether the e-Privacy directive applies when personal data are processed in RFID applications. As already highlighted by the European Commission in its Communication on RFID, due to the limitation that the e-Privacy directive applies only to processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks, "many RFID applications fall only under the general data protection directive and are not directly covered by the e-Privacy directive" ([74], p.6). The amendments that will be proposed to the e-Privacy directive in the course of the review of the electronic communications regulatory framework will take account of RFID applications and mainly of the fact that an RFID system in itself does not require a public communications network or a publicly available electronic communications service in order to work and no provider is necessarily present in such a system [71]. Furthermore, a Recommendation on how to handle data security and privacy of smart radio tags to Member States and stakeholders will be published. According to an EU press release, "both the data protection directive and the e-Privacy directive set rules for processing personal data which must be respected irrespective of the underlying technologies, and the Recommendation would further clarify their application to RFID" [75].

Currently the legal scholar needs to examine whether there is processing of personal data within an RFID application in connection with the provision of publicly available electronic communications services and public communications networks in order to decide upon the applicability of the e-Privacy directive. In positive answer and especially when the use of RFID technology enables the provision of Location Based Services[24] by processing location data, Article 9 of the e-Privacy directive will apply. Although the e-Privacy directive does not make use of the term 'Location Based Services', article 2(g) of the Directive defines the term 'value added service' as "any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof". Therefore a Location Based Service could be defined as a value added service which processes location data for purposes other than what is necessary for the transmission of a communication or the billing thereof.

In the 'Metro Future Store in Rheinberg' scenario (S4) "the shopping assistant tracks the shoppers' movement using wireless LAN software", displaying also "location-specific personalised shopping lists, favourites and special offers". It is obvious that for the provision of the location-specific personalised shopping lists, favourites and special offers location data of the customers are being processed. As the hidden RFID reader can read the RFID enabled loyalty cards of the customers, the processing is actually processing of personal data. As already described in the previous paragraph, the legal scholar shall at this point examine whether the processing is taking place in relation to a publicly available electronic communications service or a public communications network. When this condition is fulfilled, then there is a Location Based Service offered and the special provisions of Article 9 e-Privacy directive regarding value added services apply. A similar approach shall be taken in the 'Usage of RFID Technology in Educational Settings' scenario (S5), where it is mentioned that "the system can track the visitor".

[24] For detail about Location Based Services, see FIDIS D11.2 'Mobility and LBS' (under preparation)

5.2.3 Legal issues relevant with RFID applications in data protection[25]

- *Data controller in RFID applications*

According to Article 2 (d) data protection directive 'controller' shall mean 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data […]'. Determining who the data controller is a crucial point in order to specify the natural or legal person that needs to ensure the respect of the principles related to lawful processing of data.

- *Security measures in RFID applications*

According to Article 17 of the data protection directive the data controller must 'implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all unlawful forms of processing'. With regard to RFID technology there is a need to define what such measures are. The possibilities are various: killing of the tag, its physical shielding, encryption, etc. (see section 6.5). The directive does not include a detailed list of the criteria that define the technical and organisational measures as appropriate with respect to the proportionality principle, although it dictates that the measures to be taken shall be stricter when the data processed are more sensitive.[26] In the 'Enhanced proximity card' scenario (S2) the reader is authenticating itself with a relatively simple reader number to the card. Could this measure be considered as 'appropriate', under article 17 of the data protection directive? Some scholars question if the deactivation and removal of the tags could be considered as a technical measure for data security and is an actual obligation of the controller. In the 'RFID at the CVS Corporation' (S6) tags are removed in the shops for privacy reasons.

- *RFID applications in law enforcement sector*

RFID tags are also used for law enforcement - RFID armbands are already used by convicts in several European countries. The field of public and state security falls outside the scope of the data protection directive (of course this might not be the case in all Member States depending on the way the data protection directive has been implemented into their national legislation). In these cases we would need to ensure that the level of protection described in article 8 of the European Convention for Human Rights is guaranteed (necessary, proportional and does not violate human dignity). The danger of leaving personal data that fall outside the scope of the data protection directive completely unprotected has been raised at a European level and there is a draft framework decision about protection of personal data processed in the framework of police and judicial co-operation in criminal matters[27].

[25] The issues related to the data protection principles and the privacy rights of the data subject will be thoroughly examined in Chapter 6.3.1
[26] Such reasoning has also been expressed by [18]
[27] See also FIDIS deliverable 6.7: Forensic Profiling

5.2.4 Related Findings from FIDIS D7.7

5.2.4.1 Introduction

In this section we will summarise the findings of FIDIS D7.7 (RFID, Ambient Intelligence and profiling) related to the legal aspects of the problem space, while in chapter 6 we will explain some of the work in progress in FIDIS D7.9 (Ambient Law) as one approach to privacy-enhancements. Ambient Law (AmL) has been suggested as a solution to some of the problems encountered, in the legal section of FIDIS D7.3 (Actual and Possible Profiling Techniques in the Field of Ambient Intelligence). AmL aims to improve the effectiveness of legal norms concerning data protection, privacy, fairness and due process while at the same time providing democratic legitimisation for the use of technologies that may entail a new 'enforceability' [78]. Ambient law can provisionally be defined as:

'the embodiment of legal rules in the emerging technologies they aim to regulate'.

To explain the rationale behind AmL we need to briefly trace the relationship between privacy, democracy and the rule of law. In a constitutional democracy privacy is not just a private good that can be traded at will, but also an important public good that empowers citizens to develop and sustain the boundaries of the self in constant negotiation with his personal, social and material environment. If we follow the working definition of [79] privacy can be defined as:

'the freedom from unreasonable constraints on the construction of one's own identity'.

Privacy as such, is never a given, pre-existent fact of life, but always a fact that has to be created by means of institutional arrangements and interactional processes. It cannot be taken for granted. Emerging technologies like RFID change the fabric of the environment in which we create and maintain our boundaries, requiring an update of the institutional arrangements that protect the identity-building processes that sustain our humanity. For many centuries law has articulated itself in the written and printed script, empowered and constraint by the possibilities generated by writing and printing. Facing the digitalisation of our environment law may need partial re-articulation in the technologies that mediate our everyday life. The reach of the written or printed word is limited and administrative laws like data protection legislation seem paralysed and retarded in confrontation with real time monitoring of the type enabled by RFID systems.

AmL should provide more adequate means to combine the *legitimacy* of legal protection with its *effectiveness*. As machine to machine (M2M) communication technologies may provide a new enforceability, not available to written law, such enforceability needs the legitimisation of democratically generated legislation (instead of categorising it as neutral means of implementation), while at the same time data protection legislation needs to augment its enforceability (effectiveness) in the age of real time exchange of data.

5.2.4.2 Findings of D7.7: the need for PETs and TETs

In FIDIS deliverable 7.7 we have investigated the relationship between RFID systems, Ambient Intelligence (AmI) and profiling, from a technological, legal and sociological perspective. Together with e.g. sensor technologies RFID is clearly one of the enabling technologies of AmI, creating wireless embedded networks that constitute multi agent systems (MASs), which form the technological infrastructure for AmI.

From a technological perspective we found that the 'always on' nature of today's mainly used RFID tags introduces new types of problems, especially in combination with the invisibility of the tags. Once a ubiquitous reader infrastructure (fixed and mobile reader) with a seamless network connection is in place, this will allow real time automated data collection and processing. Taking into account that at this moment large parts of RFID systems are easily accessible, one can foresee a host of security and privacy problems, as listed in this chapter.

As regards the legal perspective (and as also discussed above in Section 5.2.1), D7.7 also detected a major problem in relation to the applicability of the Data Protection Directive 46/95/EC, because it is as yet unclear whether data collected from a person without identifying that person in terms of name, address etc. qualify as personal data. As Dötzer [83] points out, there is a substantial difference between 're-recognition', and 'identification', that is relevant here. He defines re-recognition as 'keeping identifiers and relating them to other received identifiers', while defining identification as 'correlating the identifier with a real-world identity'. If a person is wearing an RFID tagged pair of shoes, a shop may store this data as an identifier, which is re-recognised every time this person enters the shop (as noted also in the comment to scenario S4). As long as the shop does not link this identifier to the real-world identity of this person (name, address etc.) this person is not identifiable in the traditional sense of the term. That could mean that the data on the tag are not personal data in the sense of the Directive, unless and until the data are linked in a way that makes the person identifiable (c.f. section 5.2.1). In this document, a very broad view is taken of what constitutes personal data, encompassing both re-recognition and identification. It is important to note that even if the directive would apply to such re-recognition, in practice this will not have many consequences because (1) the invisibility of RFID tags implies that people will not be aware of leaking personal data or of data that are being remotely collected, (2) it seems practically impossible to require their consent or to inform them of the processing of the data as this would require real time M2M communication between the RFID system and the PDA of the person concerned, plus the availability of an interface on the PDA that makes the process comprehensible, and (3) this still does not imply access to profiles except in the case that art. 15 of the directive is applicable.

This last point, which was already raised in the legal section of FIDIS deliverable 7.3 (on profiling and AmI), concerns the fact that data protection legislation is mostly focused on the protection of personal data, while the more serious threats to privacy and several other constitutional values (equality and fair treatment, due process) derive from the application of (group or personalised) profiles. The legal status of profiles, generated by means of data mining, is as yet unclear. Compared to data (which are either noise or information, depending on the perspective, purpose and context of the user), profiles are a kind of *knowledge*, because they denote relevant patterns discovered in databases. Profiling is what has been called knowledge discovery in databases (KDD, cf. [84]; [82] and FIDIS deliverable 7.2). Precisely because profiles constitute knowledge, not mere data, their application can have serious

impact on citizens, while they are mostly unaware of being categorised. However, this type of knowledge may be protected as a trade secret or as forming part of a database that is protected by means of an intellectual property right. Only when art. 15 (and 12) of the directive apply, some form of protection against profiling may be available. Art. 15 reads:

> Article 15
>
> Automated individual decisions
>
> 1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
>
> 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
>
> (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
>
> (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

In the case of AmI, decisions will have to be automated, to allow smooth and real time adaptation of the environment to inferred preferences. In as far as this implies transactions and contracts, with legal consequence, or significantly affects a person, he has the right not to be subject to such 'decisions'. However, as Bygrave [81] has noted, this does not necessarily imply that such decisions are unlawful. It just implies that a person can exercise his right and demand that such decisions are not taken in an automated fashion. If people do not exercise the right, the processing of data is lawful. For a user of a smart environment that runs on autonomic and proactive computing it makes no sense to start exercising this right. In that case, art. 12 at least provides a transparency right:

> Article 12
>
> Right of access
>
> Member States shall guarantee every data subject the right to obtain from the controller:
>
> - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

However, the issue raised by Bygrave [81] applies here as well. If I choose not to exercise the right, this logic need not be disclosed. We add that for exercising the right a person would

have to be capable of understanding algorithmic processing of data, which is not a standard part of our education. Again, practically speaking, in the case of the automated processing of data derived from RFID systems, due to the invisibility and the 'always-on nature' of the tags, most people will not be aware at which point their data are being collected and they will probably lack the time and the resources to exercise a right to the knowledge of the logic involved.

This has led the authors of D7.7 to conclude that to preserve and enhance constitutionally protected values like privacy, fairness, equality and due process we may need to develop transparency enhancing tools (TETs), integrating legal rights of access to data as well as profiles with the technological devices that can actually provide such access and translate the findings into understandable information. This should at least decrease the asymmetry between profilers and profiled, following a principle of minimisation of knowledge asymmetry[28] instead of focusing all efforts on data minimisation (the main objective of PETs). AmL's tasks would thus be (1) to integrate the written norms of data protection into the technological infrastructures that are being put in place at this very moment and (2) to create a legal right of access to profiles that may impact one's life, while also integrating this right into the technological infrastructure. Integrating norms or values into the design of technological devices or infrastructures has been the core focus of constructive technology assessment [88] and work of scholars and policy advisors like Flanagan, Howe *et al.* [85] on value sensitive design.

5.3 Ethical aspects

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[19]*

Typically, the problems induced by RFID applications in the context of informational privacy concerns do generalise those encountered in profiling in general.[29] In the domain of profiling, the individual can to some extent pay attention to not leave too many traces bound to the same identifier or to different identifiers which can be related to an individual and which are very easily linkable, in order to circumvent the collection of data. In the case of RFID however, the tag itself typically is bound to the object for the whole lifetime of the object. If the object is indeed a human person[30] then the RFID is bound to this person for a long time, especially if the tag is implanted, as this needs some (easy) surgery. This means that profiling using the information of the RFID, a typically unique identifier, can be done over some long time if no precautions are being in place.[31]

---

[28] Inspired by Jiang, who speaks of minimisation of data asymmetry, [20]
[29] As explained in [21]. See also the scenarios S2, S4 as well as S7 for examples.
[30] Think of RFID implants for different reasons, e.g. the experiments done by Kevin Warwick (http://www.kevinwarwick.com/) or the bars using implants as identification for their customers as described in http://news.bbc.co.uk/2/hi/technology/3697940.stm (12/04/08).
[31] RFID tags can be made untraceable, see for example [22], and references contained therein.

This clearly brings us back to problems encountered in biometrics[32] as non-changing implanted RFID tags can also be considered as biometrically measurable items of the carrier. Hence in their simplest form, RFID tags bear the same problems with respect to ethical issues as biometrics do[33]. In this context, biometrics and RFID applications will in the future also increasingly be used in combination, and – in the best case – help to fight privacy problems, or – in the worst case – create new privacy concerns due to lack of protection measures.

This problem is not only bound to RFID implants in human or animals, as there are lots of items which are in fact carried by the same person for a very long time, especially for the 'interesting' part of the day, i.e. when one is awake. The "behaviour" of such items is very close to those of implants, as a strong one-to-one connection between carrier and tag is in place over time. The simplest example is a pair of glasses which is carried almost always by some persons, the only exception typically being while one is asleep. Other examples are watches, shoes, clothes, but also cell phones, PDAs, etc (as also already discussed above). Hence in our understanding the border between implants and external devices will vanish more and more, especially when "wearable" devices become more widespread and eventually every part of our clothing bears some RFID tag.

In our opinion, the main problems of RFID applications with respect to privacy concerns is generated by the lack of user control of the RFID tag, i.e. it can typically not be turned on or off, set into some state (listening only, inactive, ...), easily destroyed, nor can its content easily be read by humans (cf. FIDIS D7.7). Furthermore, no control is possible over the communication partners of the tag in the most primitive setting of RFID tags, nor the communication itself can typically even be discovered easily. Hence the user cannot exercise control over the technical item.[34]

In the context of surveillance, the techniques and processes of data mining, data warehousing or profiling in general are usually looked at from the perspective of human persons. The *Report on the Surveillance Society* [23] mentions that "Surveillance society poses ethical and human rights dilemmas that transcend the realm of privacy" and stresses that "ordinary subjects of surveillance, however acknowledgeable, should not be merely expected to have to protect themselves" [23].

Further, "ordinary people can and do make a difference especially when they insist that rules and laws be observed, question the system or refuse to have their data used for purposes for which they have insufficient information or about which they harbour doubts" [23]. This is an important point as the carrier of the item (the RFID) generating the date for profiling must himself react to the misuse of data, and must especially be able to act, hence really be in a position to know what is processed where by whom and what for. While this is easy to say, which individual is able to control whether – say – the laws on data protection are respected by some company? Or as said in the report on the surveillance society, i.e. "individuals are seriously at a disadvantage in controlling the effects of surveillance" [23].

---

[32] In this context see for example the reports of the BITE Project – Biometric Identification Technology Ethics, http://www.biteproject.org/ a European Commission funded action (contract SAS6-006093).
[33] See for example the policy paper "Ethical Implications of the Informatization of the body" of the BITE Project (cf. footnote 28).
[34] This problem is also addressed in scenarios S1 to S4.

Another major concern must be the transparency of the processes used for generating, storing, connecting, transforming data. This is a necessary condition for the profiled user to be able to react. If he does not know that the very process of – say – profiling is taking place, he cannot react appropriately. In fact he cannot react at all.[35]

On the other hand, the report is rather pessimistic with respect to codes of practice for example in the world of RFID: "Codes of practices may be beside the point, and easily ignored, even if they could be devised" [23]. The second problem must be faced as a really not trivial one, i.e. the very creation of rules of conduct is a difficult task, and typically no-one is willing to pay for its creation.

The potential for invasive use of RFID technology is also mentioned in the report of EPTA, the European Parliamentary Technology Assessment network: "RFID is a technology with enormous potential privacy impact as it allows the allocation of unique identification codes to virtually any object, animal or person." The main threats to privacy are then "the possibility of remote and undetected reading of the RFID tags" and the "uniqueness of the tag" [24]. The first threat can – at least partially – be eased by shielding the tags or using encryption, the second one by using re-programmable RFID tags.

An example of how customers dislike the use of profiled information is mentioned in a study [25] commissioned by the German Federal Ministry of Education and Research where in a survey[36] about 9 out of 10 people did not agree with shorter queuing times for "good" clients (in the context of a hotline of a mobile phone company). This means that typically users want to be informed about the data that is stored about them and the decision procedures applied to this data.

Another dimension is trust in the goal of the development and in the key players in this process, or as Bird and Spier put it: "Are these developments really intended to help people? How do we ensure that the industries developing these technologies really care about people and not just about profit?" [26] [37]

5.3.1 Codes of ethics and conduct

This section focuses on two well known codes of conduct and their influences on ethical considerations.[38] Neither of these codes of conduct focuses specifically on application in the field of RFID, but instead are for computer scientists in general. However, as such they can (at least partly) be applied to our situation. We are going to discuss the parts directly connected to the subject of interest below.

Typically there is a difference between codes of ethics and codes of conduct. While codes of ethics are more focused on giving visions and objectives for a computer society, codes of

[35] Again, public awareness is a first step, cf. also scenarios S1 to S4. See FIDIS deliverable 7.7 that concludes there is an urgent need for Transparency Enhancing Technologies that allow users to track and trace what happens to their data and how it is correlated with other data. See Section 5.2.4.2.

[36] Original text in German "Die Teilnehmer wurden befragt, ob sie es in Ordnung finden, wenn sie hören, dass ein Freund in der Warteschlange eines Mobilfunkbetreibers länger warten muss als andere Kunden, da er ein schlechterer Kunde ist. 90,4 % der Befragten der Gesamtstichprobe finden solch einen Umgang mit Kunden nicht in Ordnung oder gar nicht in Ordnung."

[37] In the same sense, as ethical regulations are typically not possible, the corresponding principles are to be formulated clearly. Cf. also especially scenarios S2 to S5 and S7 for the problems appearing in this context.

[38] A large collection of codes of ethics and conduct can be found in [27].

conduct on the other hand are typically written for the professionals themselves [27]. The target audience is different and codes of conduct targeted at computer specialists are more normative in nature, but both kinds reflect the main values in a comprehensive way for their audience.[39]

5.3.1.1 The ACM Code of Ethics and Professional Conduct

This code [29] is directed at members of the Association for Computing Machinery ACM and contains 24 imperative statements which every ACM member shall follow. The statements "are intended to serve as a basis for ethical decision making in the conduct of professional work" [29]. It also mentions a common problem, namely the sometimes ambiguous definitions in the field of ethics, which implies that there cannot be detailed regulations everyone follows, but rather "general" statements. In the same sense, "questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations" [29]. Here we pick some of the rules which bear ethical parts, mostly implicitly.

The second rule, "1.2 Avoid harm to others" [29] must be interpreted (as it is mentioned in the guidelines of the code) very generally, also in the sense of harm unexpectedly generated by "well-intended actions" [29].[40] It is stated that the members must assess social consequences of the system to project harm which could possibly be produced. Clearly, ethical questions implicitly arise in this context: what is 'well-intended'? Which consequences produce socially significant harm? However, clearly no general answer to such questions can be given within the code of conduct.

The third rule, "1.3 Be honest and trustworthy" raises the question of first the definition of the two central terms of honesty and trustworthiness and – even more complicated – of how to test them.

The fourth rule, "1.4 Be fair and take action not to discriminate" [29] is in our eyes the central one under the section title "General Moral Imperatives". It states that "the values of equality, tolerance, respect for others, and the principles of equal justice governs this imperative" [29]. Again, open ethical questions remain for each member in how to test the values mentioned.

In the context of privacy frameworks for RFID applications, the seventh rule might in fact be key, namely "1.7 Respect the privacy of others" [29]. The statement is formulated in a very general manner and directly applicable to our situation. The guidelines accompanying the code of conduct make the rule a bit more explicit, and mention problems and measures especially from profiling[41].

The last rule in the first section is "1.8 Honor confidentiality" [29]. Hence, extending in some sense rule 1.7, one should always respect confidentiality with respect to all "partners", say employers, but also clients and users. This is an important point in RFID technology, as there it is not always clear who is the user or client and who is not, i.e. who and what has which role and which rights.

[39] See also [28] for a comparative study of codes of ethics and conduct.
[40] Cf. also especially scenarios S2 to S4 where "harm" is typically to be interpreted as "loss of privacy".
[41] Cf. also [21]

From the second part of the rules under the title "More Specific Professional Responsibilities", we want to mention explicitly the fifth: "1.5 Give comprehensive and thorough evaluation of computer systems and their impacts, including analysis of possible risks" [29]. This extends in some sense rules 1.2 and 1.3 in a probably less considered way of thinking. Yet this appears central to gain trust of clients and users, especially if dealing with sensitive data and information which is useful for profiling. If the user does not know the risks, how should decisions be taken? And how could even (more or less) objective statements about the risks be made?

The second part of the rule "2.7 Improve public understanding of computing and its consequences" [29] is especially important in the present setting as usually the power and the problems of RFID techniques are not well known to the general public. Hence, in order to allow people to judge the technique and its problems and understand the problems related to privacy, it is crucial to have a good understanding of the basic techniques, not from the technical level but the conceptual level of data processing by RFID.

5.3.1.2 British Computer Society Code of Conduct

This code [30] consists of a set of rules which each member of the British Computer Society BCS must follow. It clearly states that every member must himself let his personal actions be governed by the rules, but explicitly also cites the Society's disciplinary procedures when not following the code. Hence compared to the ACM code or ethics, the BCS code of conducts is more normative in nature.

The first rule "1. You shall carry out work [...] in accordance with the relevant authority's requirements and the interests of system users" [30]. Clearly, as the guidelines accompanying the code mentions also, the possible conflict between the requirements of the authority and the rules followed by oneself. In the context of RFID, we shall focus especially on the interests of system users, or in other words work not implicitly or explicitly against these interests.

Important in the context of profiling, we may consider the rule "3. You shall have regard to the legitimate rights of third parties" [30] and understand this also in the sense that profiling of persons can only be done if controlled by some privacy preserving authority.

From the ethical point of view, the central rule is "5. You shall conduct your professional activities without discrimination against clients or colleagues" [30]. This rule is clearly important in the field of privacy and especially techniques such as RFID, but its application might often raise ethical conflicts with respect to requirements of the employer, etc. How to not discriminate some clients when the employer clearly wants to select the "good" customers by some data mining program?

In the section entitled with "duty to relevant authority", we find rule "8. You shall not disclose [...] or use for personal gain [...] confidential information [...]" [30] which in our opinion is problematic if not matched against the third rule cited above, and should only be applied with the explicit consent of the profiled persons.

5.3.2 Constructing Codes of Conduct

Starting from the two codes of conduct discussed above, one might wonder if there is a reason to define a new code of conduct applicable with respect to privacy frameworks for RFID

applications. Clearly, the general rules are already contained in the codes above, but formulations with less distance to privacy and RFID should be feasible.

Yet following discussion of generating such codes[42] one must see the problems inherently contained in such a process. As an example, "IFIP[43] does not intend to provide the IFIP member organisation with word-for-word guidelines for codes, but will advise them to consider the suggestions defined by a set of consensus topics [...] when writing [...] their specific codes" [31]. Furthermore, there was a growing consensus that not a "definitive ethic" should and can be imposed on the different members and countries bearing different historical, cultural, ethical, religious background, but certain principles can be outlined which should be taken into account when individual (organisations) are defining their codes of conduct. For that purpose, a huge amount of codes of ethics was reviewed and finally a set of twelve conditions was formulated which any code specific to some application domain should follow, resulting in what is called "The Toronto Resolution"

When thus facing the problem of constructing a code of conduct for privacy frameworks in the domain of RFID applications, one should start considering the elements of this resolution and finally test one's code carefully against every one of the twelve conditions.

These conditions were formulated with the goal of being applicable in wide range of problems as a "common moral framework" [32] which possibly all researchers and scholars might agree to. However there was also the intent to then develop specific codes of conducts for each discipline. As the conditions do not explicitly define notions of "good" and "bad", they try to be applicable to situations coming from different cultural backgrounds not necessarily bearing the same notions.

5.3.3 Conclusions

Lots of codes of conduct have been provided by different organisations for different application domains, but no general code of conduct can be developed applicable to any situation, even in the "restricted" domain of computer science. Facing this, any code of conduct for the present context of privacy frameworks for RFID techniques shall follow at least "The Toronto Resolution" [32]:

> "*A code provides guidelines; education provides direction; action provides progress. Since we have a code in ACM then our next steps should be [...] to take action to find ways to insert ethical awareness into our schools and corporations, to provide positive alternatives to inappropriate activities, and to bring our spiritual power in step with our scientific power.*" [31]

[42] Consider the discussions in the context of the draft of the IFIP code.
[43] International Federation for Information Processing IFIP, http://www.ifip.org

5.4 Socio-Economic and RFID technology inherent considerations

5.4.1 Impossibility of Avoidance

It is claimed that the usage of RFID technology leads to measurable positive economic effects through optimised processes especially in the area of production and logistics [33]. Moreover we are just at the beginning of wide industrial application of RFID technology. Therefore many experts expect a boost in cost reduction when RFID becomes a well established technology.

In fact the expected cost reduction and rising productivity are the main drivers behind RFID technology. The economists hope that in the end the usage of RFID technology will result in competitive advantages in a world with ongoing globalisation. Note that these are not negative goals in themselves. However, as these are the primary goals they set clear restrictions, constraints and requirements for any approach towards a holistic privacy framework for RFID.

Due to globalisation, one has to respect that any solution (including regulations) which just targets at the national level will not be successful. For the global problem one needs to develop globally applicable solutions. In order to give just one example of the difficulties arising from this, it would not be possible to suggest security or privacy protecting technologies which require cryptographic mechanisms which are forbidden in certain countries. Otherwise it would imply that one has to produce different RFID tags and related infrastructure for different countries which will result in an increase of costs - which would be fundamentally contradictory to the primary goals of RFID.

Another related aspect is that there already exists a lot of worldwide accepted RFID related standards and specifications[44]. Hence any additional security or privacy protecting technology has to be as close and compatible as possible to these existing norms. They were, on the other hand, often not developed with security or privacy in mind making the integration of security and privacy technologies even more difficult.

As a real world example, one can look at the development of the machine readable travel documents which are equipped with an RFID tag and offer only very limited protection mechanism due to the constraints implied by the necessary world wide agreements on them. Another problem which is exemplified by the machine readable travel documents (MRTD) is the multiplication of problems if two technologies carrying a number of known risks are combined (like combining biometrics and RFIDs in the case of the MRTD). This combination may not only lead to a new quantity of problems but very often also to a new quality of them [34]. Taking into account that RFID is a key (or enabling) technology for ubiquitous computing and ambient intelligence it can be foreseen that the security and privacy problems of both technologies will be multiplied in much the same way as it happened in the MRTD case.

As mentioned above, one of (or maybe the main) driver behind RFID from an industrial point of view is cost reduction. One has to take this into account especially because many of the

[44] ISO 14443, ISO 15459-x, ISO 15961, ISO 15962, ISO 15963, ISO 18000-x, EPCglobal standards (http://www.epcglobalinc.org/standards) etc.

RFID related use cases would address the mass market. Some of the visions are that every single item sold for instance in a supermarket will have at least one RFID tag attached in order to reduce the logistics costs. This clearly implies that there have to be RFID tags which are extremely cheap. Otherwise these visions are unrealistic. The implications regarding security and privacy protection are manifold: Security and privacy protecting technologies applied in these RFID applications have to be very cheap. From the state of the art and the experience with existing general purpose security technologies and their usual cost one can deduce that the cost restrictions will lead to some kind of "security and privacy protection *ultra light*". Depending on the use case this does not need to be an inadequate solution for the given use case. However, given the fact that such cheap security solutions will exist, it can be foreseen that they would even be applied in use cases where they are not adequate. This will even be the case in situations where the usage of more expensive (and also more secure and privacy friendly) solutions would be in principle viable (from an economic point of view).

Forcing the producers or users of RFID technology to implement uneconomic but more secure solutions by means of laws and regulations seems to be at least problematic. If this is not done at a global scale (which is unrealistic in itself) it will mean that a certain country has to give up its potential competitive advantages.

5.4.2 Lack of Awareness

Surveys on the value of privacy for individuals (in terms of cost one is willing to accept for its protection) clearly indicate that the usual European citizen sacrifices his privacy even for small amounts of monetary advantages [25]. This is just another reason why any security or privacy protecting technology in the area of RFID has to be extremely cheap.

Moreover RFID advocates might claim that there are no new privacy problems related to RFID, because existing technologies like discount/consumer cards, mobile phones etc. could be used for all kinds of profiling. Similar to discount cards, consumers are enticed with monetary advantages and therefore the privacy risky behaviour of the consumers would be similar in the RFID case.

One possible counterbalance against the economic driven usage and development of RFID technology could be the normal citizen whose privacy is affected by that technology. However, not only might citizens accept giving away privacy for small monetary advantages - the situation is even worse because people are often not aware of the risks. According to a Capgemini study [35] from 2005, 85 percent of the European consumers have no idea what RFID means or how this technology works. Therefore they cannot make any real decision for or against it. Nevertheless, as RFID becomes more and more in the focus of public attention, scientific literature and other media start to report more about the privacy related problems and risks.

A difficulty with explaining the privacy risk of RFID technology to the masses is that RFID advocates can argue that RFID is no more than just a number on a thing (as this is one of the main implementations of RFID at the moment). Hence the RFID (tag) in itself is not *per se* a privacy harming technology - it might even be possible that in a given area of application of RFID no personal data at all will be processed as discussed in Section 5.2.1. Very often the problems only arise from combining the core RFID technology with other supporting technologies (backend processing etc.). This could lead to a reduction of privacy piece by piece, whereby every single piece in itself is not a big risk to privacy (as we have seen it in

many other areas). At the end one could raise the question: Which technology is responsible for the privacy problems? Is it really the RFID tag or the data warehouse behind it?

If one just has a dip into the RFID related literature one could get the impression that the privacy problems of RFID are not only well understood but also many solutions exist which can solve all the problems. This impression arises from the fact that almost all RFID related publications have a section which deals with privacy/data protection problems. However, apart from noting that privacy and data protection is a real problem, they actually do not offer useful solutions for most scenarios of application of RFID. They very often just anticipate solutions sometime in the future. If they do indeed offer some solutions, then the proposed solutions are very often very abstract and sketchy, so that in most cases they will not work well or are not feasible in practice. One of the main problems for privacy and data protection arising from such publications is that RFID advocates can promise that data protection is of crucial importance to them - as one can easily see from the huge number of pages they dedicate to this topic. We refer to FIDIS deliverable 7.7 for an approach that takes into account the far reaching consequences of untimely adoption of RFID systems.

5.4.3 Controllability, perceived Control and Usability

One factor which supports and explains the unawareness among customers is the very small size a typical RFID tag has [36]. They are simply invisible or even embedded within the material a certain thing is made of. Besides the negative impact on awareness, this kind of physical manifestation also leads to problems for implementing security or privacy protecting mechanisms - especially because it is impossible in most cases to have an adequate user interface directly on the RFID tag. Hence it is difficult to develop convincing and trustworthy privacy solutions for RFID because one cannot directly interact with the source of the problem or may not even see it. The technology trend goes to the direct integration of RFID tags into the material of the components / parts of things. Therefore a decoupling of RFID tag and RFID marked object is usually impossible.

In the end it leads to the question of control from different perspectives. From the users' perspective various questions are relevant, such as:

- Do I take part as a "user" in an RFID system? Which one(s)? Who is operating it (or them)?
- Are benefits and risks of these systems balanced in a way I personally can accept?

From the operators' or vendors' perspective:

- Which factors influence the acceptance of RFID from the users' perspective? The results of recent research [37] gives evidence, that (1) the social power and trustworthiness of the operator or service provider, (2) perceived usefulness, (3) perceived ease of use and (4) perceived control (or balance of control) in the context of RFID systems by the user play a major role in addition to personal preferences with respect to technology.
- How to convince the user that a privacy measure like deactivating the RFID tag really happened? In other more "classical" areas this could be done much easier. As an

example just think of a hard drive with some personal data on it, where the revealing of this data would be a privacy breach. In this case one can imagine applying all sorts of physical destruction to the hard drive to convince themselves that the data on the magnetic slices could not be reconstructed with reasonable investments. In the case of RFIDs, it is however really hard to be convinced that whatever attempts of destructions one has done was really successful.

Moreover, destroying the RFID tag as a measure for deactivating them is, in many scenarios, not the goal of the users. Normally the users wants to benefit from RFID too (as already said, security and privacy are not the primary goals of RFID technology), but in a controlled, self-determined and balanced way. Control by the user in many cases is not understood in the same way as security or data protection specialists understand it. Technology acceptance research generally shows possession of parts of the system (a piece of technology) as a strong factor influencing the perception of control in a positive way [37]. But in the context of RFID systems this influence seems to be very limited due to the limited capability of RFID tags. Hence the question is: how to convince the user that he can control the RFID system and thus the data associated with the tag? This becomes even more difficult because of the wireless communication capabilities as well as the wireless energy absorption possibilities. The problem is not only that the data transmission uses a technology inherent broadcast (at least at the lowest communication level). It is also extremely difficult (or even impossible for human beings) to recognise if a certain data transmission is happening right now or not. Moreover, the same difficulties exist just for recognising / influencing the communication capability / inability as well as the functioning of an RFID tag. Here the situation is completely different to the one that a user normally knows from everyday experience with usual computers. If one wants to ensure that a normal PC does not reveal any secret data nor does any other unwanted processing of them, one can simply unplug the network and power cables. A comparable measure does not exist in case of RFID tags (besides the already discussed and often unwanted destruction of the RFID tag). Although blocker tags and other devices to disrupt the communication at the physical layer are being developed [38] or at least there is some research going on, they are up to now neither as efficient as necessary nor are the legal issues with these kinds of blockers solved. But even if these difficulties could be solved the fundamental problem of uncertainty and thus a reduction in perceived trustworthiness still remains the same.

5.4.4 Reduction of Expense weakens Capabilities

Resulting from the pressure of cost and the physical manifestation (e.g. small size) the overall resources in terms of energy, storage and computing power available to the RFID tag are very limited. This makes a simple adoption of well known and studied PETs (Privacy-Enhancing Technologies) which are used in the world of “normal” computers and networks unfeasible. Looking for instance at cryptography related solutions - it turns out that many of them tend to have the same problems: the capacity of the cheap tags is too low to apply strong security mechanisms (key sizes are too short, random number generators are not available or do not produce truly random numbers, etc.), the key management is unsolved: how can you manage the keys for millions of things like banknotes, cars, milk-bottles, etc.?

One way of reducing the costs when producing RFID tags is to produce some kind of “general purpose” RFID tag, rather than developing and producing more specialised (or tailored) RFID

tags for a given use case. This "general purpose" capability of an RFID tag might sometimes be "hidden" as the producers will "deactivate" some of the functions of the "general purpose" RFID tags to sell them as "special purpose" (i.e. tailored) RFID tags. History teaches us that often such things could be "converted back" into "general purpose" ones. One example of a negative impact this might have in the area of security is that one can expect that RFID tags in general will not only be readable but also writeable. Moreover the range of RFID transmissions might be greater than necessary for the given area of application of RFID technology, etc.

Many of the proposed solutions for privacy enhanced RFID technologies concentrate on one of the three main layers (physical, network or application layer), but a solution on one layer may be countervailed by an attack on another layer (e.g. pseudonyms on the application layer vs. traceability on the physical layer). Therefore a holistic privacy framework for RFID has to incorporate a multi-layered approach.

Moreover, after "solving" the privacy problems the RFID related research and development can continue to go on in technology directions which are mostly counterproductive for privacy like enhancing the range of RFID tags, enhancing the transmission speed, enhancing the capability to read a huge number of RFID tags simultaneously, reduction of the vulnerability to failures through environmental influences (like metal or water, jamming signals etc.). The latter even includes the consideration of the requirements of RFID technologies when planning new buildings. It is likely that our surroundings will be planned and implemented "RFID compatible" within the next few decades.

Eventually the term "RFID" subsumes all kinds of different technologies with very different capabilities, conditions and prerequisites. Moreover it seems to be very difficult to draw a clear line between what belongs to RFID and what does not. Resulting from the huge range of different technologies and areas of application involved it seems to be very hard to develop a common holistic privacy framework, which covers the whole spectrum of technologies and applications used.

5.5 Technical and organisational security aspects

5.5.1 General security risks

As already mentioned in the introduction chapter, the backend system comprises of typically server based infrastructures. Therefore the well known and studied security mechanisms for that type of infrastructure could be applied. Besides the simple fact that these mechanisms really have to be applied, no speciality of RFID based scenarios exist.[45] Therefore the following analysis of security mechanisms for RFID will concentrate on the more challenging parts of the core RFID infrastructure: the RFID tags, the RFID readers and the communication between them.

One can list five general security risks when using RFID technology:

1. **Sniffing**: eavesdropping on the communication between tag and reader.

[45] "Security Analysis of the Object Name Service (ONS) for RFID" describes weaknesses of the DNS-like backend system for RFID. Thus, security measures for DNS can be applied for ONS as well.

2. **Spoofing**: forged RFID tags can be used to simulate other tags, thus gaining their privileges. This is illustrated in scenario S2 where a proximity card is spoofed.
3. **Unauthorised writing**: the information or part of the information on the tag is altered or information is added by an unauthorised party.
4. **Replay-Attacks**: after a sniffing attack an attacker can use the eavesdropped data to replay the communication.
5. **Denial-of-Service Attacks**: any attack which disturbs the authorised communication, like jamming the radio or destroying tags.

5.5.2 Privacy Risks in relation to Security

The goal of the EPC-standard is to provide each single RFID tag with a unique identifier. This will give the vendors and operators many opportunities to monitor and track their products, but it also presents new risks for the privacy of the users and consumers. Without any security measures, it is easily possible to read-out all the tags a person carries in a split second, for example whilst this person is walking through the doors of a grocery store. The store could then display personalised advertisements or provide a virtual shopping guide which addresses the preferences of the user. These read-outs can in theory take place from distances of over a couple of meters.

An attacker may also eavesdrop on the connection between reader and backend, thus gaining information about requested product information or other data. The scanning of tags on a person may in addition lead to the creation of movement-profiles, when the person is scanned frequently. Of course this implies a highly pervasive RFID infrastructure.

So, the attacks on the privacy of people via RFID can be categorised as:

1. unauthorised detection of properties of persons,
2. tracking and identifying of persons, and
3. profiling of persons.

5.5.3 Information Security

Information security is an essential basic for privacy in IT systems. It has to be noted though that information security is required, but not sufficient to ensure privacy.

One can distinguish between open and closed RFID systems. Closed systems are characterised by homogeneity, locality, known operators and users as well as a central administration and little interaction and cross-linking to other networks. Open systems are the contrary of the described closed systems. A typical example for a closed system is a single library, whereas a library in combination with other libraries and book-stores could be seen as

an open system. It is evident that closed systems are easier to secure in terms of privacy than open systems.

Information security has three central goals: confidentiality, integrity and authenticity, and availability. Confidentiality can be divided into confidentiality of communication *contents* (e.g. e-mail text) and confidentiality of communication *circumstances* (e.g. anonymity of sender and receiver or location privacy).

The gained security of a given system is dependant on the following factors:

1. Can established security schemes and methods be used with or at the deployed devices?
2. Is a scalable key management (as needed by most of the known cryptographic protocols) possible?
3. Is the design of systems and protocols secure?
4. Is there a correct and valid implementation of the designed system?
5. Can the system be used in a hands-on way (usability)?
6. Are the users adequately informed and trained?

Without doubt there are a number of security issues for RFID systems. The security discussion in this section will be, as mentioned earlier, centred on the tag/reader aspects since, the security issues of the backend system are similar to standard computer systems. In order to classify them, we used the standard ISO 13335-1 grouping for the different security issues. In some cases these issues are (as noted previously) essential for privacy as well as security while in other cases they might be a threat or a hindrance for privacy mechanisms.

Building up an integrated security concept for an RFID system according to international standards such as the ISO/IEC 27000-series requires managed control and clearly assigned responsibilities with respect to technical components used in the system and the users' and administrators' behaviour with respect to the implementation of organisational security measures. In this context RFID systems share many characteristics of systems publishing services via the internet (lack of control with respect to users' behaviour and client-security) and WLANs (lack of control with respect to the physical communication layer according to the OSI layer model of network communication). Security measures applied for the central components of RFID and backend systems need to take into account these characteristics.

5.5.3.1 Confidentiality aspects

The confidentiality requirements on an RFID system are highly context dependent. If the information stored and transmitted by the system is personal, can be considered as personal during some part of the tag's life or is sensitive in some other way (e.g. classified information within one organisation), then the information in the RFID chip or the backend system should not be revealed to unauthorised parties. This is true even for the very simple RFID systems since just the plain serial numbers could give competitors, stalkers or thieves information on the content of containers, boxes or the bearer of the tag [39], [40]. Having access to the information also makes it possible to clone the tag, as illustrated by scenario S2, or make use

of the information to fool different types of peers or servers in e.g. service or payment protocols[46]. Traditionally cryptography is used in order to assure confidentiality, but this will only work in tags or systems that have the capability of performing advanced calculations. Cryptography will also introduce the problem of key handling as stated in Section 5.4.4. These problems, especially weak implementation of cryptography and key handling issues can be observed in the context of Basic Access Control (BAC) and RFID used in Machine Readable Travel Documents (MRTDs) [25].

For cheaper systems, other and more economical mechanisms need to be developed. Within this area some suggestions have already been proposed that partly solve the confidentiality problem: Fishking and Roy suggest using the signal to noise ratio of the reader to determine the distance to the reader in order to thwart unwanted remote monitoring [39]. Juels *et al.* suggest using blocker tags to make it harder for readers to gain unwanted access to the tag [38]. Juels also suggests using tag pseudonyms in order to prevent illicit tracking of tags [45] and discusses other mechanisms in [41]. Needless to say that if the information is protected on the tag, it needs to keep at least that protection, albeit maybe not with the same mechanism, in the whole chain i.e. the radio link, the reader, the middleware and the backend system. The confidentiality problem in RFID might also be time dependent since one entity that is authorised to read the information at a specific point in time might not be authorised at an earlier or later time in the life of the tag. This will make key management even harder. Blocker tags might be a solution here, but we probably still need encryption to guarantee confidentiality in the whole chain e.g. protecting against eavesdropping on the radio interface or in the communication within the backend system.

5.5.3.2 Integrity aspects

Integrity must be seen as essential in most applications of RFID systems since the whole idea is to use some of the information stored on the tag as an identifier for a specific purpose and the other part as attributes in some way associated with that identifier. From this follows that nobody should be able to alter a tag (or any other part of the system) in an uncontrollable way. Failure in integrity might lead to a number of issues e.g. virus attacks as illustrated by scenario S1, insertion attacks [46], forgery, remarking of products to gain a lower price, change expiration dates and storage conditions or theft in the distribution chain without the possibility to trace where it took place or be able to blame other links in the chain[47]. An obvious solution to this problem is to use read only tags. However, (as is pointed out earlier) the quest for cheap production of tags might imply that read only tags are only disabled versions of general purpose tags where it might be possible to reverse the read only state of the tag. Signing of data is also one possible solution but brings on the issues of PKI (Public Key Infrastructure) handling amongst a large number of entities. Just as with confidentiality integrity needs to be maintained throughout the chain.

5.5.3.3 Availability aspects

We believe that the problem of availability in the RFID context is centred on the ability to read the tag in any authorised situation. Attacks in this context are targeted towards the tag or

[46] For discussions on cloning possibilities see, e.g. [41], Appendix G in [42] and [39]. For real examples of cloning see, among others [43] and [44]
[47] For a more in-depth discussion and scenarios/examples see [41] and [39].

the reader. In the tag case it probably will consist of either shielding or destroying the tag, something that, from a security perspective, unfortunately is not hard to do. Regarding the reader case, it can be flooded, jammed or destroyed. An example of a flood attack is the blocker tag which gives the reader more information than it can handle. Jamming usually strives to break or disturbing the radio link. Even though blocker tags can be used by individuals to protect their data, availability attacks for malicious purposes might also lead to e.g. theft of goods or denial of service or exclusion for persons. These types of attacks tend to be very difficult to protect against and are usually solved in traditional computer systems on the logical level by redundancy, over provisioning or intelligent filtering and on the physical level by locking in or in some other way physically protect the entities. This might be a tough problem to solve on the radio link.

5.5.3.4 Accountability aspects

The whole purpose of accountability is to make people or organisations liable for their actions (e.g. for accessing personal data of other persons) and to be able to trace events "after the fact". This is usually accomplished with the help of immutable log files or digital signatures or a combination of both. Logging in an RFID environment might be a problem due to the limited storage space on the tag. It might be possible to create some form of central logging system in specific cases. However, if the tag travels through many different organisations during e.g. distribution, this might be cumbersome or even politically impossible to achieve. On the other hand using digital certificates would require every entity in the chain to have its own certificate and of course a PKI to handle the certificates. This might be administratively unfeasible. There might be a possibility to combine technologies to a feasible solution or it might be possible to use ideas from the DRM (Digital Rights Management) field. If we want to have a chance to see who retrieved personal information and to whom it was passed we need accountability and it needs to be compulsory and not voluntary. More aspects on how such privacy supporting logging can be done will be discussed in the upcoming FIDIS deliverable 14.6 "From regulating access control on personal data to transparency by secure logging".

5.5.3.5 Authenticity aspects

The authenticity of the information is interesting from both a pure security perspective and a privacy perspective. Which of the perspectives that is dominant depends on the viewpoint taken and on the application. On the privacy side are the issues of identity theft and all the problems associated with it. On the security side is the question on how much trust one should put in the information e.g. as an identifier in transactions or as a token of authenticity. If the information can be cloned or modified in an unauthorised manner, then it is of no use as an identifier since we cannot guarantee its authenticity [39]. The same argument holds if it is possible to remove or exchange the tag on the item it is supposed to identify [39]. This area calls for both logical and physical security measures.

5.6 Problem Summary and Conclusions

In this section we will summarise the different problems and constraints for reaching the privacy-enhancing RFID applications discussed above. To exemplify we will tie the specific problems to our example scenarios from chapter 4 and grade them in terms of relevance for the each specific combination of problem and scenario. Besides the specific problems

illustrated by the scenarios, here we also list general problems for which all of our scenarios apply.

From the different perspectives, the following list of problems can be distilled from the discussions above.

5.6.1 Legal

P01 Information stored in an RFID tag does not always qualify as personal data. The collection and processing of data via RFID technology is covered by the provisions of the data protection directive only when the information stored in the RFID tag refers to an identified or identifiable person (thus qualifying as personal data) or when this information can be linked to other personal data (Art. 2 (a) data protection directive).

Scenario relation

Highly related: S4 (The Metro Future Store in Rheinberg): The comment added to the end of the use case S4 with the Art.29 WP example illustrate that customer profiling can also be done without real identifiers.

P02 Personal data must be processed fairly and lawfully. This principle is not always respected in RFID applications.

Scenario relation

Highly related: S4 (The Metro Future Store in Rheinberg): In this use case there were no grounds for making the data processing legitimate, as the consent given when the customers applied for a loyalty card were not valid since the customers were not properly informed (see P03).

P03 Consent is a legitimate ground for data processing. However consent is not valid when the data subject is not properly informed. How can we handle the consent problem in an RFID environment?

Scenario relation

Highly related: S4 (The Metro Future Store in Rheinberg): In this use case the customers were not properly informed about the use of RFID tags in the loyalty cards and all purposes for which his data would be processed, and consequently the consents given when they applied for loyalty cards were not valid.

P04 The data protection directive grants the data subject several rights (right to be informed, right of access, right to object, right to delete, etc). The data subject cannot exercise these rights in RFID applications, as for instance he is not always informed about the processing of his data.

Scenario relation

Highly related: S4 (The Metro Future Store in Rheinberg), where the customers were not informed about the use of RFID tags. Also in use case S5 (Usage of RFID Technology in Educational Settings), the users were probably not properly informed about the extent of the personal data processing. Labels should inform the users about the use of RFID tags and readers in the exhibits and the RFID token given to the visitor at the beginning of the visit.

P05 In cases of automatic processing of the data, the data subject is entitled to know the logic involved in this (Art. 12 data protection directive), which is not always the case in RFID applications.

Scenario relation

Related: S4 (The Metro Future Store in Rheinberg)

P06 Consumer profiling is not allowed when it is based on illegal means. This principle is not always respected in RFID applications or can be questioned due to the consent problem.

Scenario relation

Related: S4 (The Metro Future Store in Rheinberg)
Marginally related: S5 (Usage of RFID Technology in Educational Settings)

P07 The data controller has to take 'appropriate technical and organisational measures' to protect personal data (Art. 17 data protection directive). However it is not obvious which measure are considered 'appropriate'.

Scenario relation

Related: Scenarios S1 (Attack on an RFID System) and S2 (Enhanced proximity Card both provide examples were we can assume that no appropriate security measures were taken.

P08 Article 9 e-Privacy directive contains specific provisions regarding Location Based Services (or value added services in general). For article 9 to apply the service needs to be offered via a public communications network and it is not always clear when this is the case in RFID applications.

Scenario relation

Related: S4 (The Metro Future Store in Rheinberg) illustrates how location tracking

was done by the shopping assistant for displaying location-specific personalised shopping lists. Also scenarios S5 (Usage of RFID Technology in Educational Settings) and S7 (Scenario for Social Inclusion) are based on location tracking via RFID technology.

P09 The processing of personal data shall take place in a transparent way. Lack of transparency implies breach of the data protection legislation.

Scenario relation

Highly related: S4 (The Metro Future Store in Rheinberg) gives an example where the processing and profiling of personal data via RFID tags are not transparent to the customers. S3 (An Identity Manager for RFID Tags) illustrated how the "data track" functionality can enhance transparency for the end users.

5.6.2 Ethical

P10 RFID in combination with profiling can be a major privacy concern.

Scenario relation

Highly related: Privacy problems of profiling via RFID systems are illustrated by S4 (The Metro Future Store in Rheinberg) and S5 (Usage of RFID Technology in Educational Settings).

P11 As detailed regulations of ethical issues are typically not possible, the fundamental principles themselves have to be formulated in an easily applicable and understandable way. How do we do this?[48]

P12 The central point of "respect the privacy of others" asks for PETs focusing on RFID. However, in our view, there are currently no such PETs for RFIDs covering the whole lifetime of the tag and providing appropriate protection during that lifespan.

Scenario relation

Highly related: S3 (An Identity Manager for RFID Tags) and S6 (RFID at the CVS Corporation, where special removable tags were used) describe some possible PET approaches.

[48] This is a general problem and not only related to RFID. However, it is included for completeness.

P13 The central problems, privacy issues and impacts of RFID, must be formulated in a "comprehensive and thorough evaluation". How do we perform such an evaluation?

P14 Public awareness and understanding of the possibilities of use and abuse of RFID must be raised. How is this handled best?

P15 The applicability of codes of ethics and conduct in the context of RFID systems must be widespread.

5.6.3 Socio-Economic and RFID technology inherent problems

P16 Both the core RFID infrastructure (RFID tag and RFID reader) and especially also *the backend system* have to be secured.

Scenario relation

Highly related: S1 (Attack on an RFID system) and S2 (Enhanced Proximity Card) describe attacks where the RFID infrastructure and/or backend system were not properly protected.

P17 PETs for RFID have to be *globally applicable* - this could prevent the usage of certain security technologies.

P18 Cheap RFID tags used in most of today's RFID systems offer very limited control of the system's behaviour or the process of data processing from the perspective of the user. This potentially also hampers technology acceptance.

Scenario relation

Highly related: S3 (An Identity Manager for RFID tags) illustrates how an additional mobile Identity Management device can enhance user control.
Related: S4 (The Metro Future Store in Rheinberg) is an example where the use of cheap RFID tags for supermarket applications limits the possibilities of user control.

P19 PETs for RFID have to respect existing standards and specifications which were not made with privacy in mind - this will lead to all sorts of restrictions and workarounds.

P20 *National* laws and regulations are not feasible - the needed international agreements will introduce obvious drawbacks (e.g. long term implementation, consensus on a minimal base, etc.)

P21 PETs for RFID have to be *extremely cheap* - this however does not allow effective protection of the valuable asset of privacy in many situations.

Scenario relation

Highly related: S4 (The Metro Future Store in Rheinberg) is an example where the use of cheap RFID tags for supermarket applications limits the possibilities of privacy protection.
Related: S1 (Attack on an RFID System) and S2 (Enhanced proximity card) illustrate security problems.
Marginally related: S6 (RFID at the CVS Corporation) provides an example for inexpensive solutions (removable tags), which can be applied for some privacy-sensitive applications such as the management of pharmaceuticals.

P22 PETs for RFID have to cope with the *physical manifestation* of the RFID tag (e.g. very small size, embed within the material etc.) and *related limitations* (energy, storage, computing power etc.)

P23 PETs for RFID have to solve the *problem of control and uncertainty* in order to achieve trustworthiness

Scenario relation

Highly related: Scenarios S4 (The Metro Future Store in Rheinberg), S5 (Usage of RFID Technology in Education Settings), S6 (RFID in the CVS Corporation) are examples of the privacy-sensitive applications where trustworthiness plays an essential role.

P24 PETs for RFID have to deal with problems and risks arising from the *wireless communication*

Scenario relation

Related: S1 (Attack on RFID System) , S2 (Enhanced Proximity Card), S7 (Scenario for Social Inclusion) illustrate security incidents that were possible as wireless communication risks were not properly addressed.

P25 PETs for RFID have to implement a *multi-layer approach* - this would require integrating privacy enhancing technologies on various layers which could often not be done straight forwardly.

P26 PETs for RFID have to consider a *huge variety of different kinds of RFID* tags and readers (active, passive, etc.) as well as areas of application - this makes a "one-fits-all" privacy framework more difficult or impossible.

Scenario relation

Highly related: S7 (Scenario for Social Inclusion) where types of agile readers were used.

5.6.4 Technical security aspects

P27 It must be possible to control access to the information on the tag if it contains personal or otherwise sensitive information. This is usually handled by some form of access control/encryption mechanism. However, current limitations in the computational capabilities of RFID tags makes this types of solution unfeasible or too expensive. How do we solve this dilemma?

Scenario relation

Highly related: S3 (An Identity Manager for RFID tags) illustrates a possible approach to address this problem.

P28 It must be possible to control the ability to alter the information if it is possible to change it in any way and if we need to rely on the information stored. How can this be achieved within the economical and technical constrains of an RFID system?

Scenario relation

Related: S1 (Attack on RFID System) which illustrates the consequences of lacking access control.

P29 If the tag is to be used successfully as an authenticator then it needs to have both confidentiality mechanisms as well as integrity mechanisms regardless of the information stored. Further, there must be a way to guarantee that it is not possible to physically remove or switch tags. How do we solve this in an RFID system?

Scenario relation

Related: S2 (Enhanced Proximity Card) illustrates cloning attacks that are possible due to inappropriate protection. In S6 (RFID at the CVS Corporation) the risk has to be addressed that tags for pharmaceuticals cannot be easily removed or switched inappropriately.

P30 In order to guarantee accountability we need a tamperproof mechanism that in some way can record who did what and when. How do we construct such a mechanism in an RFID environment?

Scenario relation

Related: S2 (Enhanced Proximity Card) describes how the cloning attack was not detected in time due to missing accountability measures. Scenario S3 (An Identity Manager for RFID Tags) provides with the "data track" functionality an example for technical means for enhancing means for accountability.

One can conclude that there exists a lot of privacy related problems with RFID technology. The main difficulties for a solution arise from the wide range of constraints and pre-conditions which have to be respected if one wants to develop a successful holistic privacy framework for RFID. This clearly restricts the possible solution space.

6 A Holistic Approach to Privacy-Enhancements

Developing a holistic privacy framework for RFID is an ambitious task as emphasised in Chapter 5. One has to bear in mind the overall system as well as the three main components: RFID tag, RFID reader and backend system. For each of them one has to develop security solutions for the different protection goals like confidentiality, integrity, availability, etc. This has to be done with a clear specification of the attacker model a certain mechanism offers protection against. However, technical solutions alone are not sufficient. No matter how good a technical solution is, it will not be implemented unless the solution is socially and ethically acceptable, legally compliant and trustworthy.

In this chapter we will discuss legal, social, technical and ethical aspects that influence the design and deployment of privacy-enhancing RFID systems and give an overview of proposed legal, technical and ethical solutions or efforts towards them. The text flow in this chapter does not follow the strict division used in Chapter 5. This is an intentional choice we made in order to try to follow a more holistic approach. In essence, we have taken a development approach, where the first part gives guidelines and discussions to be used in deciding what the European legal Privacy Framework and society require from the system and the system owner. The latter parts then provide suggested technical and non-technical solutions and guidelines to some of the requirements and also hint at how a first simple evaluation of the privacy friendliness of a proposed design could be made.

In a little more detail, the chapter is divided as follows: Section 6.1 discusses factors that influence technology acceptance of ambient intelligence environments and highlight the importance of self control. Section 6.2 defines the cases in which there are legal obligations according to the European legal privacy framework, as the data that are processed classify as personal data. Section 6.3 summarises the most essential legal privacy requirements that RFID applications have to fulfil. It therefore provides a summary of legal privacy principles for system design that should be used as guidelines when designing new RFID systems. Ethical considerations, principles for designing codes of conduct and public awareness issues in regard to RFID applications are discussed in section 6.4. In section 6.5, technical approaches to privacy friendliness are discussed and an overview on current technical solutions is presented. Section 6.6 presents a check list based on the discussions in this chapter that could be used to evaluate the privacy friendliness of different RFID systems or to find privacy shortcomings in the design of the systems. Section 6.7 presents an overview of Ambient Law which is a work in progress and once more highlights the need for transparency. Finally, Chapter 7 concludes this chapter and summarises its main results.

6.1 Factors for technology acceptance and their importance in ambient intelligent environments

Spiekermann and Rothensee (2005) suggested a modified technology acceptance model for ambient intelligent environments which was already introduced in FIDIS deliverable 7.7 ‘RFID, Profiling and AmI’ (Hildebrandt, Meints 2006: 62-65). In this model the reaction of the user with respect to ambient intelligent technologies is understood as a balancing process of different tendencies. The different factors and their influences on tendencies and the resulting decision are summarised in the following figure:

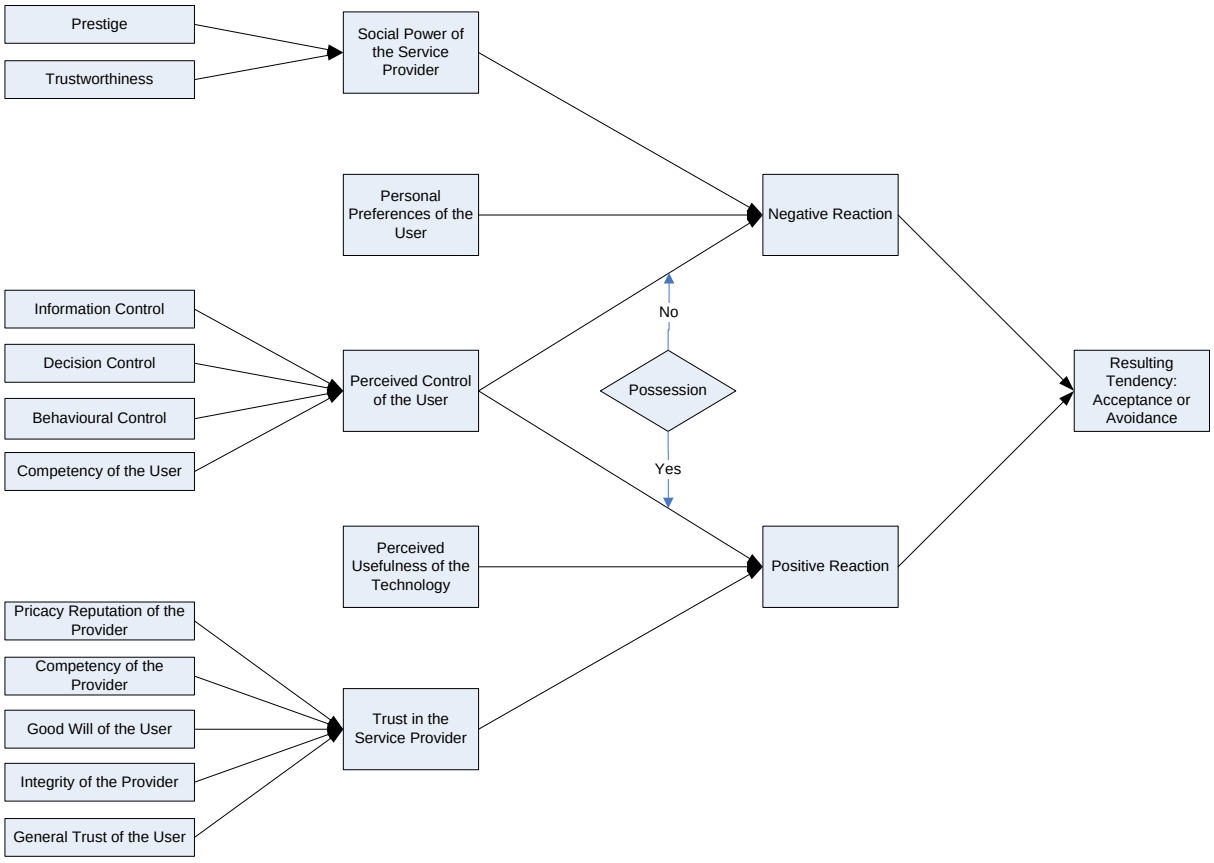

Figure 2: Factors for the acceptance of ambient intelligent systems

Spiekermann and Rothensee [37] came to the conclusion that the balance of control has an important influence on the acceptance of an AmI-related technology and subsequently on a potential decision to buy a related product. One of the limitations of this model was that the importance of the influencing factors and their direction of influence were not sufficiently investigated.

6.1.1 Results of the TAUCIS Study

To investigate these aspects for selected influencing factors, Spiekermann carried out a survey in 2006. Details of the selected methodology of the survey and the results are published in the study TAUCIS (technology assessment – ubiquitous computing and informational self-determination; [25]: 172). The study was carried out in two groups: a group of 4741 participants in an online survey and from a socio-demographic perspective representatively chosen reference group of 200 participants who were interviewed (paper survey). Taking the chosen methodology and the number of participants of this survey into account, it overall is not representative but it gives an indication on which influencing factors are important.

To the participants of the survey four scenarios taking place in 2015 were presented:

1. An intelligent refrigerator able to re-order consumables
2. Automatic speed control integrated in a car
3. An "intelligent" computer workplace
4. A car able to detect the need for maintenance and to order support in a garage

All scenarios were presented to the participants in one of two randomly chosen subtypes: (a) a subtype where the user had some control, e.g., the choice of using the automated support functions of the system or not, and (b) another subtype with low or no control where the system supported the user automatically and mainly informed him about the choices taken for her. The scenarios 1, 2 and 4 include the use of RFID or related wireless communication.

The presentation of the scenarios was followed by a questionnaire. Most of the questions were to be answered using a scale from -5 (negative reactions) to +5 (positive reactions).

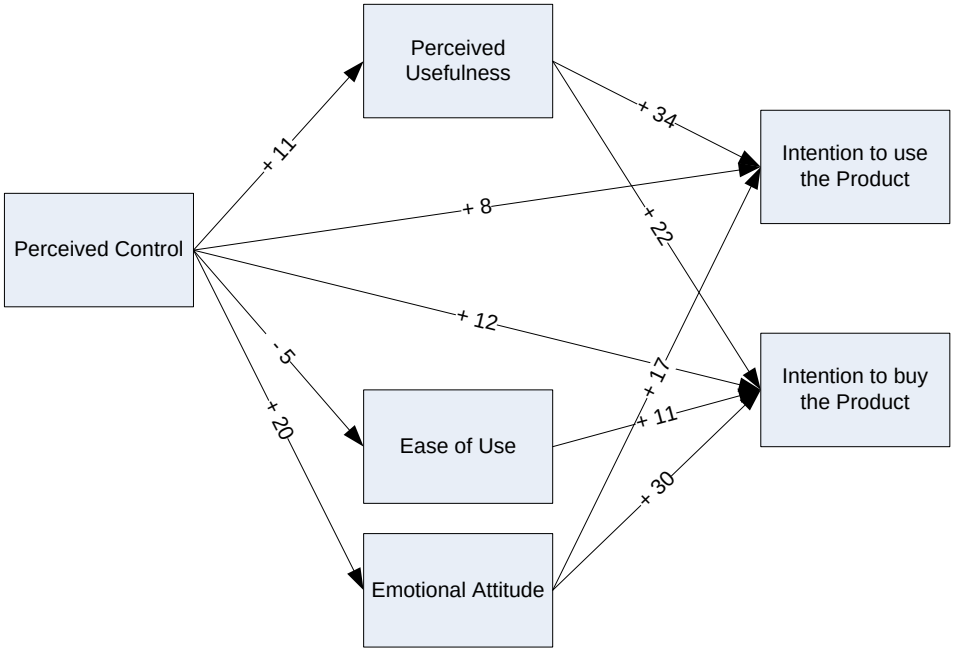

Figure 3: Influence of perceived control on the intention to use or buy the presented AmI products

One of the major results of this survey was that users generally felt quite a high need for control (values were between 3.4 and 4.8). Perceived control of the user for all scenarios showed negative values (between -0.4 and -1.9). So it clearly can be concluded that in these scenarios the users generally had less control than they would have liked to have. But does this fact really have an impact on the intention to use or buy these technologies? Figure 3

shows the results of the regression analysis based on the paper survey (influence presented as beta-values[49] *100, taken from [25]: 194).

In comparison to the other factors of influence that were analysed in this study, perceived control showed the largest influence on the emotional attitude of the (potential) user towards the investigated AmI products and thus indirectly significantly influences the intention to buy the product. The most significant influence was observed in the scenario with the automatic speed control integrated into cars.

The survey also showed that higher control has a direct influence on the risk perception of the user. The answers of the participants showed that the higher the (effective) control, the lower the perceived risk, the fears that the product could be limited in use, the private sphere could be invaded and that the system could work inefficiently and consume a lot of time. It has to be noted that privacy concerns and data protection related considerations in this study are part of perceived control only, but an important one. Privacy concerns also influence indirectly other influencing factors as shown in Figure 2 ([25]: 162).

Another result of this study was that the participants in general did not well understand what potential consequences of pervasive data processing could be, though a difference could be observed between the participants of the online survey (higher awareness) and the paper survey (significantly lower awareness). Though commercial data processing is well known, there seems to be a large lack of transparency of what this could mean to the individual customer. In general the participants showed a high trust in the effectiveness of protection by laws. In addition, the large majority of the participants neither expected nor accepted discriminatory effects from commercial data processing ([25]:195).

6.1.2 Recommendations on technology acceptance

Spiekermann (in [25]: 195) concludes that for vendors of AmI systems from a market perspective it is of high importance to give effective control to the users. This would be a proactive management of various fears of consumers mentioned in the study and would effectively lower barriers to enter the market. She further suggests that politicians should check whether user control should become a general guideline for manufacturers and vendors of AmI systems (regulatory or self regulatory approach).

These results should be transferred into the market to enable manufacturers and vendors to develop AmI solutions accordingly. This should be politically supported. In addition further research should be carried out to check these results and possibly adopt them to other, more complex use scenarios of AmI.

In case no response to these research results can be observed from manufacturers and vendors on the market, it should be checked whether market failure occurred. If this is confirmed, a regulatory approach as suggested by Spiekermann as an additional option should be implemented and enforced.

[49] Beta-values are the regression coefficients used in the regression analysis. Typically beta-values are esteemed from the results of the survey. An example for the application of regression analysis and the use of beta-values can be found at http://socio.ch/arbeit/t_crottilandolt2.htm (Accessed 21/04/08)

6.2 RFID technology and the notion of personal data

In this section we will provide guidelines for which cases legal privacy provisions, as discussed in the next section, have to be taken into consideration. In order to decide upon the application of the data protection legislation, it is crucial to define whether personal data are involved in the RFID application or in the RFID system in question. As is illustrated in Figure 4 below, when the information does not relate to an individual, then the information does not qualify as personal data.

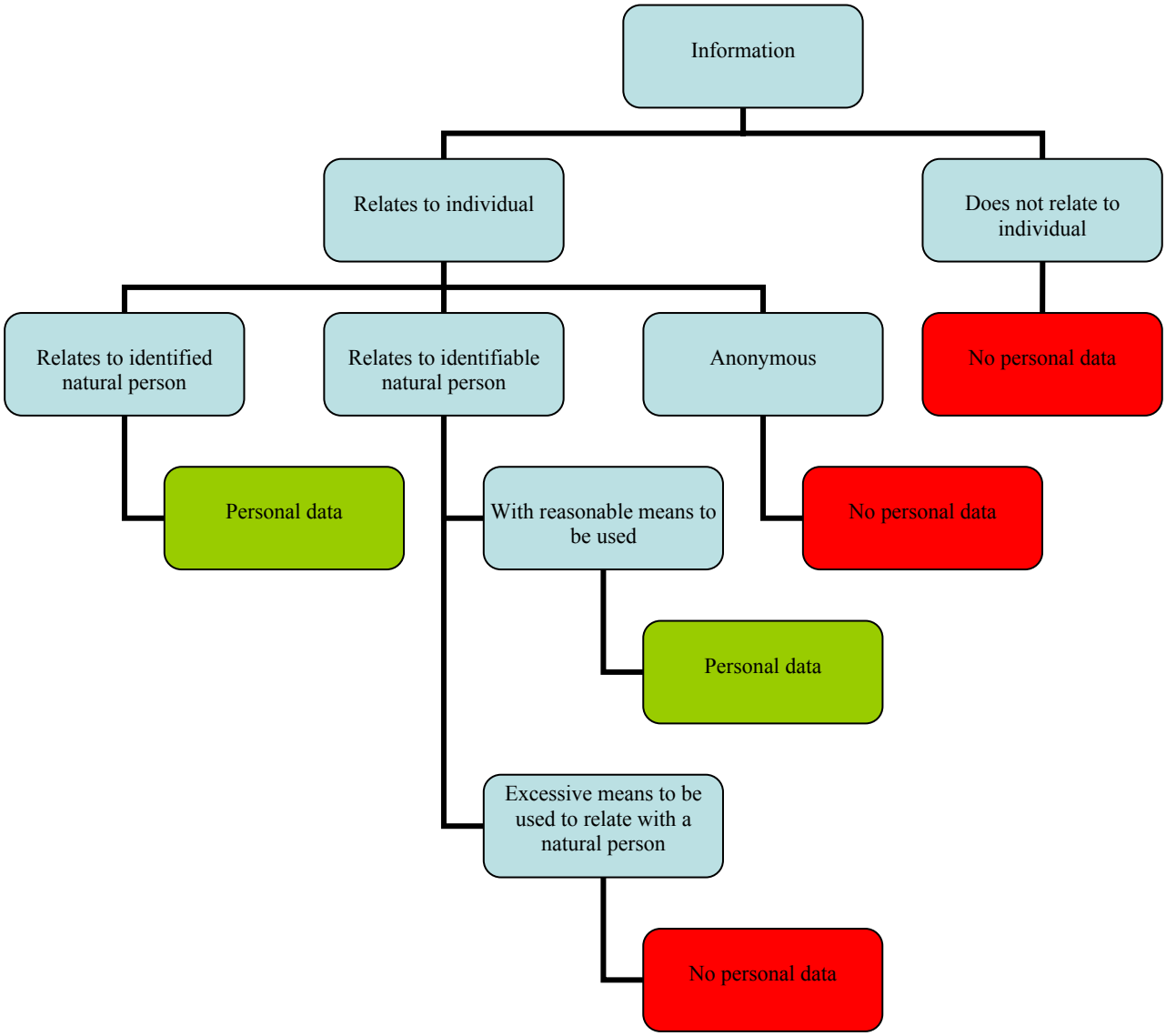

Figure 4: The process of defining whether there is personal data involved in an application

In the opposite case, when the information is related to an individual, the following options are possible: (a) when the information relates to an identified natural person, e.g. via an RFID implant, then it is personal data; (b) when the information is anonymous and it cannot be linked with a natural person, then it is not personal data; (c) when the information relates to an identifiable natural person, the following distinction has to be made, as already discussed under Chapter 5.2.1: (c.1) when the information can be linked to an individual with reasonable means to be used, such as via an RFID tagged access card, it is considered as

personal data; (c.2) when the means to be used in order to finally link some information to a natural person are excessive, then the information does not qualify as personal data.

6.3 Processing of personal data in RFID applications and systems

This section provides an overview to the main legal provisions, according to the EU Directives, that have to be taken into consideration when RFID applications processing personal data are designed and operated.

6.3.1 Obligations for making data processing legitimate

The processing of personal data is allowed only under the grounds mentioned in Article 7 of the data protection directive and shall be respected when the processing of personal data is taking place in RFID applications. This means that for each processing of personal data - collection, recording, storage, adaptation, alteration, retrieval, consultation, disclosure, dissemination, etc. - the controller has to verify if the processing falls under one of the criteria for making data processing legitimate. These grounds can be coded according to Article 7 data protection directive as follows:

1. the data subject has unambiguously given his consent; or
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
3. processing is necessary for compliance with a legal obligation to which the controller is subject; or
4. processing is necessary in order to protect the vital interests of the data subject; or
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

The processing of personal data in relation to RFID technology has to be based on one of the aforementioned grounds and be compliant with the principles that are set out in Article 6 of the data protection directive.

One basic principle for the processing of personal data is that the data shall be processed fairly and lawfully (Art. 6(a) data protection directive). In the 'Metro Future Store in Rheinberg' scenario (S4) the processing of personal data is based on the consent of the consumers which is given when they apply for their loyalty card. Although consent is a legitimate ground for the processing of personal data, it has to be freely given, specific and informed in order to be valid. In the declaration of consent for the loyalty card, the users were not informed about the use of RFID tags in the cards and corresponding readers in the store, although it was stated that "adjustment of offers to the wishes and needs of the customers is one of the purposes for which this card is used". In this case the customer was not properly

informed about the purposes for which his data would be processed and the given consent is not valid. Furthermore the intelligent shopping trolleys in conjunction with the RFID enabled loyalty cards enable customer profiling.

The data controller shall also ensure that the collected data are "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Art. 6(c) data protection directive). The procedure followed for the collection of data shall be transparent for the additional reason that in this way the criteria used for choosing the specific data as appropriate can easily be checked. The data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (Art. 6(e) data protection directive). Furthermore, the data shall be 'accurate and, where necessary, kept up to date" (Art. 6(d) data protection directive).

The European data protection legislation distinguishes between the data controller and the data processor. The controller is defined as a person (natural or legal) which alone or jointly with others "determines the purposes and means of the processing of personal data" (Art. 2(d) data protection directive), while the processor is a third party who simply processes personal data on behalf of the data controller without controlling the contents or use of the data (Art. 2(e) data protection directive). This distinction is of great importance in the processing of personal data within RFID applications for several reasons. The data controller (and not the data processor) is the one who will carry the obligations described in the data protection directive and is the one to define the details of the data processing. As a rule of thumb, it can be said that the data controller is liable for violations of the data protection legislation, while the role of the data processor is reduced [[11], p. 62]. However, RFID technology enables the unnoticed collection of personal data and therefore, questions arise as to how the users can be informed about the identity of the data controller in order to exercise their rights.

6.3.2 Information to be given to the data subject and his privacy rights

- *Information to be given to the data subject*

When data are collected from the data subject, the data controller must provide him with some information relating to the processing of his personal data. Such information includes the identity of the controller and of his representative, if any, and the purposes of the data processing. Additional information may be also necessary, such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply. Furthermore the controller should inform the data subject about the existence of the right of access to and the right to rectify the data, in so far as such information is necessary (Art. 10 data protection directive).

In cases of providing Location Based Services through RFID technology the controller must, before obtaining the consent, provide the individual additionally with specific information regarding the type of location data that will be processed, of the purposes and the duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the Location Based Service (Art. 9(1) e-Privacy dir.). Furthermore the user shall be given the opportunity to withdraw his consent for the processing of location data at any time.

Even if the legislation is meant to be technology neutral, some legal provisions are quite difficult to be fulfilled in the field of RFID technology. For instance a major issue is how the user will be informed about the collection of his personal data and how the information is to

be given to him, in the absence of screens or via the minimal user interfaces of some RFID applications [69].

- *Transparency*

One basic and simple but still necessary measure towards a holistic privacy framework for RFID is therefore the demand for transparency. Each RFID reader and RFID tag must be clearly labelled. The main reason for this is to raise awareness of the RFID technology (and the potential threats to privacy) among the European citizens. As stated in the introduction, awareness at the moment is at a very low level, and the physical appearance of RFID tags and RFID readers will not have a positive impact on the awareness as both of them are mostly invisible or "undetectable" by human beings.

The proposed labelling is already a well established and accepted preliminary in other privacy related areas (like in case of surveillance cameras) or areas with potential threats to human beings (like the labelling of bioengineered food). Nevertheless in the area of RFID analogical laws and regulations need to be adopted. Regarding the enforceability of such rules, RFID technology has the advantage (e.g. compared to surveillance cameras) that the existence of RFID readers (or more precise the attempt of an RFID reader to actually access an RFID tag) could be easily detected due to the fact that the communication uses radio waves. Although detecting an RFID tag is somewhat harder, research has shown that with little investment devices could be built which at least can detect the existence of standard compliant RFID tags (e.g. ISO-14443 RFID tags). Therefore it seems feasible that at least the authorities can check if a producer (or retailer etc.) embeds RFID tags without labelling the affected products correctly.

Note that there exist some kind of paradox: On one side it is a goal of PETs for RFID that the RFID tag only communicates with authorised readers (to circumvent all kinds of threats like eavesdropping of the communication, tracking, etc.) on the other side this privacy measure hinders the detection of hidden tags. It seems that at least the authorities need some "backdoor" to allow them to communicate even with privacy enhanced tags just to detect them. But history teaches (like in the crypto regulation related key escrow debate) that the weakening of a PET (or security) technology on purpose will often lead to unintentional side effects. How this problem could be solved is an open research question. Nevertheless, as the main privacy threats arise from reading the tags (and not just from their very existence) laws and regulations which oblige labelling of RFID tags and RFID readers are still meaningful and enforceable.

- *Rights of the data subject in RFID applications*

The data controller shall also ensure that the rights of the data subject are respected. The Scenario on 'An Identity Manager for RFID tags' (S3) illustrates the 'data track' log file that allows the users to get information on who accessed the tag and for what reason. However in RFID scenarios it is not always easy to safeguard the rights of the data subject to get information about his data that are processed, the right to access and right of rectification or deletion of data[50], when necessary. In the field of RFID applications, the data subjects shall be informed about the presence of both RFID readers and RFID tags on products, which is not the case in the 'Metro Future Store in Rheinberg' scenario (S4). In this case for instance pictograms should inform the customers of the presence of both RFID readers and RFID tags

[50] Art. 12 Data Protection Directive

on the products. In the 'Usage of RFID Technology in Educational Settings' scenario (S5) labels should also inform the users about the use of RFID tags and readers in the exhibits, and the RFID token given to the visitor at the beginning of the visit.

When personal data are collected, the data subject has the right to be informed by the data controller in a clear and intelligible way about the form of the data undergoing processing, as well as about the means and precautions the data controller has taken to adhere to the data protection principles[51]. Furthermore, in cases of automatic processing of the data, the data subject is entitled to know the logic involved in this.[52] In the 'Metro Future Store in Rheinberg' scenario (S4), the RFID tags in the customer loyalty cards were used to activate advertisement displays. The user was however not informed about the procedure and the logic followed for this.

The European data protection legislation grants the data subject some rights that have to be safeguarded by the data controller. The data subject has the right to be informed whether his personal data are being processed. He has the right to know the purposes of the processing, the categories of data concerned and the recipients to whom the data are disclosed. The information shall be given to him in an intelligible way. Moreover, in cases of automatic processing of the data, the data subject is entitled to know the logic involved in this (Art. 12(a) data protection directive). In the 'Metro Future Store in Rheinberg' scenario (S4), the RFID tags in the customer loyalty cards were used to activate advertisement displays. The user was however not informed about the procedure and the logic followed for this.

Article 12 further grants the data subject a right to ask for the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the directive, in particular because of the incomplete or inaccurate nature of the data. According to Article 14 of the Directive, Member States should grant the data subject the right to object, on compelling legitimate grounds relating to his particular situation, to the processing of data relating to him.[53] In the 'An Identity Manager for RFID tags' scenario (S3) the 'data track' log file assists the user in the exercise of his rights, as he gets information on who accessed the tag and for what reason.

Among other initiatives, the rights of the consumer relative to RFID applications have been expressed in an RFID Bill of Rights prepared by Simon Garfinkel. According to Garfinkel, consumers should have the right to know whether products contain RFID tags, they have the right to have RFID tags removed or deactivated when they purchase products and to use RFID enabled services without RFID tags, the right to access an RFID tag's stored data and the right to know when, where and why the tags are being read [50]. These rights correspond to the rights of the data subject that are safeguarded in the European data protection directive.

6.3.3 Obligation to provide appropriate technical and organisational measures

Article 17(1) of the data protection directive addresses the issue of data security, requiring data controllers to take 'appropriate technical and organisational measures' against unauthorised or unlawful processing, and accidental loss, destruction or damage to the data.

[51] Art. 12 Data Protection Directive
[52] Art. 12 Data Protection Directive
[53] The general rights of the data subject are elaborated in FIDIS D11.3 'Economic aspects of mobility'.

To the extent that this principle covers the security requirements and robustness of the network itself, this principle overlaps with the security and confidentiality requirements laid down in articles 4 and 5 of the e-Privacy Directive, when there is processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. Taken as a whole, this principle imposes a statutory obligation on data controllers to ensure that personal data are processed in a secure environment. This means that the data controllers must consider the state of technological development and the cost of the implementation of any security measures. Bearing in mind these factors, the security measures that are adopted by the data controllers must ensure a level of security that is appropriate to both the nature of data to be protected and the likely harm that would result from a breach of this principle [[77], p.58]. It follows that the more sensitive the data, the more adverse the consequences of a security breach would be for the data subject, and therefore more stringent security requirements should be put in place. This is specially the case as regards the processing of health-related data. In any case, the data controllers should implement appropriate security measures to ensure that non-authorised personnel are not able to gain access to personal data.

This general obligation for the deployment of technical and organisational measures to ensure the adequate implementation of the data protection principles shall be specified in the field of RFID technology. The use of appropriate privacy enhancing technologies will assist the user to enhance his privacy. Standardisation initiatives regulating the design of RFID tags, RFID readers and RFID applications in general can prove extremely helpful "in minimising the collection and use of personal data and also in preventing any unlawful forms of processing by making it technically impossible for unauthorised persons to access personal data" [12]. In cases when the RFID tag contains personal data, they should be encrypted and in order to prevent unauthorised reading of the tag, the authentication of the reader should be necessary before it can access the data [12]. In the 'Enhanced proximity card' scenario the reader is authenticating itself with a relatively simple reader number to the card. It is not clear whether such kind of authentication is appropriate according to Article 17 of the data protection directive.

6.3.4 Privacy principles for system design

Following the discussion above there is a strong need already to take privacy principles into consideration in the design phase of RFID systems. One list of principles or guidelines on how to deal with data so that the application could be regarded as privacy-friendly, according to [48], is:

- *Avoidance of data collection and making sparing use of data:* Protection of data privacy does not only demand regulation on how data is being stored, processed and passed on, but also on how to avoid certain data being collected in the first place.
- *Intended purpose:* The intended purpose for data collection must be explicitly declared.
- *Prohibition of clandestine reading:* Clandestine reading of RFID tag data, tracking of persons either directly or indirectly, tags in shared space such as in sales rooms and tags embedded in money, or personal identification documents must be prohibited or otherwise rendered intractable.

- *No additional burden for the citizen:* There must be no additional burden on citizens to protect themselves, e.g. the long-winded and yet incomplete deactivation procedure at the Metro Future Store (S4).
- *Privacy must be the default:* Privacy should not be an optional extra feature, but the core property to be preserved in any application.
- *Legislation must be forward-looking:* Data being collected today even if regarded uncritical may get a different meaning in the future.

The European privacy and identity management project PRIME[54] has elaborated seven very similar principles for designing privacy enhanced (identity management) systems [49], which should also be applied when designing privacy-enhancing RFID applications:

- Design must start from maximum privacy;
- Explicit privacy rules govern system usage;
- Privacy rules must be enforced, not just stated;
- Privacy enforcement must be trustworthy;
- Users need easy and intuitive abstractions of privacy;
- Privacy needs an integrated approach;
- Privacy must be integrated with applications.

6.4 Code of conduct approaches to privacy friendliness

6.4.1 RFID Bill of Rights by Garfinkel

Another approach to circumvent the privacy problems introduced by the usage of RFID systems are the "RFID Bill of Rights", as mentioned before, proposed by Simon Garfinkel [50]. According to him consumers should have:

- The right to know whether products contain RFID tags.
- The right to have RFID tags removed or deactivated when they purchase products.
- The right to use RFID enabled services without RFID tags.
- The right to access an RFID tag's stored data.
- The right to know when, where and why the tags are being read.

Garfinkel sees "these not necessarily as the basis for new law, but as a framework for voluntary guidelines that companies wishing to deploy this technology can publicly adopt. Consumers could then boycott companies that violate these principles."

[54] http://www.prime-project.eu/

6.4.2 Constructing Codes of Conduct – The Toronto Resolution

Problem P10 indicates that detailed regulations or similar notions of ethical issues etc. are usually not possible. However, we think that there are, as already mentioned in section 5.3 "Ethical Aspects", general, fundamental principles that can be formulated in a way that is understandable beyond the limits of computer scientists. The major problem is however to find an understandable but also precise enough formulation of those principles and further to work hard on the readability and applicability of that formulation (cf. section 5.3.2**)**.

This means, that a "meta code of conduct" should be specified, or better, a methodology for constructing codes of conduct appropriated for the specific situation, technology, application, environment, etc. This was indeed one of the focuses of the "Toronto Resolution" [32] formulated at a workshop on ethical considerations. This resolution tries to build a common framework based on the idea that specific codes for any given application area are to be constructed. It is a sort of baseline specifying the elements to be treated by any code, and as well an examination guideline for testing those codes against a set of considerations.

The resolution consists of two parts, one specifying a general preamble to be included in future codes of conduct. This preamble tries to place a future code of conduct in the general context, i.e. insists on the moral duty for respecting life on our planet as well as the duty of scientists to not only consider their "restricted environment" (e.g. a university) but to look at implications of their work on anyone and anything. The preamble reads as follows:

"Living in a world in which all forms of life are interdependent, we recognize that human activity since the scientific revolution now threatens the future of life on the planet. This threat stems in part from reckless exploitation of the earth's resources and massive pollution of the biosphere by humankind, exacerbated by rampant militarism. To help solve these problems, scientists and scholars, and all those concerned with the welfare of life on earth, need to unite in a world-wide moral community, in which considerations of beneficence and justice at a global level are fundamental. We recognize that knowledge gives power; that power tends to corrupt and may be used for dangerous and destructive purposes; and that consequently scientists and scholars, who share the privilege of participating in the advancement of knowledge, many under the shelter of academic freedom and in the tradition of open publication, have a particular responsibility to society for the effects of their work. All should make a determined individual and collective effort to foresee the implications and possible consequences of their scholarly and scientific work, and avoid studies that are likely to harm the quality of life.

We should recognize that knowledge also gives enlightenment and promises emancipation from disease, poverty and other social evils. As an alert and enlightened community of experts and concerned citizens, scientists and scholars should participate in the social process of directing their research and its applications to benign ends, while educating their students and the public concerning this, the proper role of scholarly and scientific knowledge." [32].

This preamble is very general and can only specify the context in which the more specific rules are to be considered and eventually interpreted, because – as already mentioned – we cannot specify unique rules for ethical considerations which are applicable without interpretation in every context.

The second part of the resolution consists of twelve conditions mentioned hereafter. These conditions are the ones each new codes of conduct should follow and be tested against.

Clearly there is space for interpretation which must take part in the sense and context formulated by the preamble - while codes of conduct are not easy to formulate, basic guidelines to be followed by them are not either.

1. "a code should articulate as far as possible the underlying assumptions and guiding principles of a working ethic;
2. a code should indicate specific measures designed to ensure that signatories adhere to its principles;
3. a code should be sufficiently general to encompass scholarly work and basic, applied and technological research as well as the actions of practitioners engaged in the discipline or profession;
4. a code should oppose prejudice with respect to sex, religion, national or ethnic origin, age, sexual preference, colour, or physical or mental disability;
5. a code should take into account that, while in general it is difficult to anticipate all the consequences of research, scientists and scholars have a responsibility, individually and collectively, to try to foresee, and to keep themselves aware of, the developing applications of their work, and to choose or redirect it accordingly;
6. a code should recognize that actions designed narrowly to benefit humankind may in fact threaten the survival of all species, since the ecosystem is a seamless web;
7. a code should forbid research directed towards developing or using methods of torture, or other devices and techniques that threaten or violate individual or collective human rights;
8. a code should direct scholarly and scientific activity towards the peaceful resolution of conflict and universal disarmament; since all research has military potential, every scientist and scholar should seek to resolve the ethical problem that knowledge, which should enlighten and benefit humanity, may be used instead to harm the planet and its people in war and in preparation for war [...];
9. a code should encourage its adherents to comply with established procedures for the scientific and (where appropriate) ethical peer review of research studies conducted under its auspices and, where such procedures do not exist, a code should specify them;
10. a code should urge its adherents to make all basic research results universally available;
11. a code should urge its adherents to identify and report violations of its terms, and should correspondingly ensure their protection from retribution by their fellow-scientists, professional and learned societies, and the judiciary for such exposure;
12. *a code should be widely disseminated through the school and university curricula, to educate the rising generations, as well as practicing scientists and scholars, about their emerging responsibilities."* [32].

One thing is the successful making of such a code. Another thing is its application and wide dissemination, which is discussed hereafter.

6.4.3 Raising Public Awareness

Constructing codes of conduct – as discussed in the previous section – is all well and good, yet it does not help anything if public awareness of the problems is not raised to the same extent. In an ideal environment, codes of conduct are followed unquestionably by the corresponding entity, yet in practice a client must have the possibility to check this in a feasible way and to even eventually question the very interpretations of the code.

In the present context, we have to focus specifically on privacy concerns implicated by RFID (ab)use, but such concerns are by themselves today often not as widespread as we would like them to be. Look for example at the problems introduced through the internet. Hence while raising public awareness of use and abuse of RFID is a priority objective, first one must indeed focus on privacy concerns themselves.

A major issue, as also mentioned in problem P12, is that a larger focus must be put on the comprehensive part of the formulations and finally a comprehensive and thorough evaluation of the issues and impacts.

Problem P13 focuses on the public awareness issues of RFID techniques and especially on how this awareness of the citizen can be raised, problem P14 more on the dissemination problem. There is quite some work being done in these directions, consider for example the news on Heise Online [63] where "Data protectionists call for RFID code of conduct", i.e. the German federal data protection commissioner calling companies to develop themselves guidelines and codes of conduct for their applications working with RFID techniques. It is also referring to the self control initiative [64] of the industry, an issue however which is subject to very controversial discussions in the respectively accompanying comments (see [64]).

The central point clearly is and will be the consumer. If his fear of negative consequences (in his own understanding) of using RFID techniques willingly or unwillingly is raised, using such techniques might be a negative publicity issue for the company. One source of fear can be little or no information about the technique itself and its possibilities and dangers, which is for the moment the case. So the consumer must be more informed about this technique [66], restricting knowledge about its problems not only to professionals and experts[55] but allowing the larger public to enter discussion. In a recent publication on "RFID and Consumers" [35], it was noted that the consumers (or the small percentage of them knowing about RFID) are most concerned with either the augmented possibilities of targeted marketing or consumer data used by third party, hence a major issue for industrial partners using RFID must be the development of RFID code of conducts not only for their own purposes but also for demonstrating its strategies and goals to their clients.

While articles on the data protection aspects of RFID (e.g. [67]) are being developed, respective documents on ethical issues and codes of conduct are not yet widespread. Consider however the article on "An RFID code of conduct" [61] which – starting from problems in the health care sector – asks for consideration of more than privacy protection by law: "In addition, the Fair Information Practices devised by the Federal Trade Commission provide a blueprint for an industry code of conduct" [61]. A first step in this direction is also done by "A UK code of practice for the use of radio frequency identification (RFID) in retail outlets" [62] which focuses on informing the consumer about the very presence of RFID tags and the possibilities of disabling, removing, etc. them after purchasing the corresponding article. It further asks for publishing policies on using, processing etc. data generated by RFID frameworks. Clearly, it is not addressing ethical issues on its own, but it might be a first step in the right direction and must be regarded only as a first step.

---

55 Clearly discussion in the expert domain is going on in Europe, see for example the "RFID Consultation Website" http://www.rfidconsultation.eu/ with its slogan "Towards an RFID Policy for Europe; the "European Group on Ethics in Science and New Technologies" http://ec.europa.eu/european_group_ethics/ (21/04/08); and [68] specially focusing on ICT implants.

On the other hand, it is also crucial to not only mark the RFID tags themselves but also their "counterpart", i.e. the antennas which are used to communicate with the tags. Hence what is for example missing in the code of practice [62] is a clear recommendation on how antennas are to be marked in order to make them visible. This augmentation of visibility also goes in the right direction of augmenting the awareness of consumers. A side effect of not marking an antenna would then also be that, in case the antenna is nevertheless found by someone, by default it will be considered as a "dangerous" antenna.

6.5 Technical approaches to privacy friendliness

The following two phenomena are largely responsible for the existing privacy problems of RFID applications:

- **Leakage of information about the object that an RFID tag is attached to:** if there exists (a more or less publicly known) linkage between the data stored in the RFID tag (e.g. an ID as used in the EPC standards) and the information about the object (like the Object Name Service (ONS)), then by learning the data stored on the RFID tag one also gets information about the related object. Depending on the kind of object this might be a serious threat to privacy (just think of RFID tagged medicine). Note that this kind of threat does not require any long term attack and therefore does not need much effort.
- **Possibility of Tracking RFID tags:** if an RFID tag emits somewhat static data / information (i.e. data which is specify for the given tag), then the attacker can trace the movement of an RFID tag and link additional (external) information which are related to that tag. An often cited example is that a customer buys an RFID tagged object using a credit card. If the attackers get knowledge about the credit card information, he can link the RFID tag to the identity of the customer and by this means track the customer. Note that this type of attack often requires some long-term effort. Also note, that even if a single tag does not emit enough identifying information to make it possible to distinguish that tag from a bunch of similar tags, this would not be sufficient to prevent tracking attacks. One can assume that with increasing deployment of RFID tags a person will carry a whole mix of different tags. This mix in itself would then be distinguishable from other sets of RFID tags (and thus be traceable).

Besides the core privacy threats, current RFID technology is also vulnerable to authentication attacks. The latter problem is mentioned here because some dependencies between both exist. In [41] the authors state that:

"Loosely speaking, RFID privacy concerns the problem of misbehaving readers harvesting information from well-behaving tags. RFID authentication, on the other hand, concerns the problem of well behaving readers harvesting information from misbehaving tags, particularly counterfeit ones."

Moreover and of special importance is the fact that well designed **RFID privacy will strengthen RFID authentication**. This might be counterintuitive as privacy is often interpreted as a mechanism which weakens authentication. However, generally cloning an RFID tag requires scanning that violates the privacy of its holder. Or to say it the other way

round: if privacy mechanisms prevent any unauthorised reading of RFID tags, then cloning of a tag becomes a much harder task for an attacker.

When designing security and privacy technology in the area of RFID, one has to deal with a great variety of RFID tags and RFID readers with different capabilities.

An often cited statement is that a low-cost RFID tag should not cost more than 5 U.S. cents. According to [47], that means that the cost of tag's processor electronics should not exceed 2 cents. In [52] the authors conclude that at the end this would limit the number of logic gates (the elementary building block of a digital circuit) to 7.5 to 15 K. Given that storing a 100 bit ID (like that proposed by EPC) requires 5 to 10 K gates, there are only 2.5 to 5 K gates left for security mechanisms. This is by far too little for implementing the kind of cryptographic mechanisms and algorithms (like public-key cryptography) on which most of the known privacy enhancing technologies (in the area of usual computers) are based.

Moreover the high demand for very low-cost RFID tags hinders implementation of any measures which strengthen it against tampering. Therefore one has to assume that any RFID tag internal data (e.g. some secret key etc.) may be leaked through physical attacks.

Another boundary condition is the transmission speed. For low-cost RFID tags it would limit the amount of data which could be transmitted to around 500 bits[56]. Note that due to the wireless communication between RFID tag and RFID reader all data transmitted is vulnerable to eavesdropping.

Another important point one has to bear in mind when designing or analysing security and privacy solutions for RFID is related to the various types of "ranges" which could be identified for the communication between RFID tags and RFID readers (mainly taken from [41]):

- **Nominal read range:** RFID standards and product specifications generally indicate the read ranges at which they intend tags to operate. These ranges represent the maximum distances at which a normally operating reader, with an ordinary antenna and power output, can reliably scan tag data. ISO 14443, for example, specifies a nominal range of 10 cm for contact-less smartcards.
- **Rogue scanning range:** The range of a sensitive reader equipped with a powerful antenna–or antenna array–can exceed the nominal read range. High power output further amplifies read ranges. The rogue scanning range is the maximum range at which a reader can power and read a tag.
- **Tag-to-reader eavesdropping range:** Read-range limitations for passive RFID result primarily from the requirement that the reader powers the tag. Once a reader has powered a tag, a second reader can monitor resulting tag emissions without itself outputting a signal, i.e., it can eavesdrop. The maximum distance of such a second, eavesdropping reader may be larger than its rogue scanning range.
- **Reader-to-tag eavesdropping range:** In some RFID protocols, a reader transmits tag-specific information to the tag. Because readers transmit at much higher power than tags, they are subject to eavesdropping at much greater distances than tag-to-reader communications.

[56] Assuming that reading the tag data should not exceed 1 second.

- **Detection ranges:** This is the distance at which an attacker can detect the presence of RFID tags or RFID readers.

Various technical problems must be overcome to secure RFID tags against the basic threats mentioned above. The proposed solutions could be roughly classified as follows:

- **ID confidentiality**: if the ID stored on an RFID tag could be kept secret from the attacker, then the information leakage problem would be solved
- **ID anonymity**: all the data / information emitted by an RFID tag should either change on a regular base (additionally it has to be impossible for an attacker to link different data / information as belonging to the same tag) or a large group of RFID tags has to emit exactly the same data / information. Both principles are well known general privacy approaches. The first one can be seen as a kind of transactional pseudonym and the latter expresses the general anonymisation technique to make things equal. A special kind of ID anonymity can be achieved by making the tag output indistinguishable from truly random values.

Naturally the entire well known principles for designing (general purpose) security and privacy enhancing technologies should be respected when developing mechanisms for RFID systems. This covers for instance a property called forward security: even if an attacker learns some secret information, he should not be able to deanonymise or reveal secret information involved in past activities. Forward security is especially important in the area of low-cost RFID tags, as this kind of tag will not offer any tamper resistance. Therefore (as said above) it is reasonable to assume that an attacker may learn secrets stored on the RFID tag.

In the next sections an extract of proposed RFID security and privacy mechanisms is presented. The goal of this is to describe the current state of the art.

6.5.1 Privacy Enhancing Measures and Technologies

The following sections will introduce technical measures enhancing the privacy of users utilising RFID tags.

6.5.1.1 Preventing unauthorised read-outs

In order to prevent data readout from an RFID tag, the crudest method is to destroy the tag. Another possibility is to remove the antenna from the RFID tag core (like IBM's "Clipped Tag"[57]). However, these approaches have several drawbacks, the biggest being that after the destruction, the tag cannot be used anymore. There are many situations in which destroying the tag is not an option. Imagine the case where an RFID tag is used to handle warranty, destroying it may cause the warranty to be void. Or the illustrious smart fridge. Maybe the user wants to prevent arbitrary scanning and recording of the contents of his shopping bag, but at home he may want to benefit from the smart fridge, which relies on working tags. Another big drawback is that destroying a tag requires some active user interaction, which many are too apathetic for, and indeed it may well be impossible to destroy a tag without destroying the product as well.

[57] See: http://www.youtube.com/watch?v=95VOxKp0s74 (21/04/08)

So destroying tags for privacy-measures seems to be ill advised. Another solution could be to permanently deactivate the tag. As stated in chapter 3, tags adhering to the EPCglobal Class-1 generation 2 standard must implement a password-protected kill command for the deactivation. The password is necessary to prevent unauthorised tag-killing, which could lead to denial-of-service or similar attacks.

6.5.1.1.1 The Kill-Command

Killing a tag has several drawbacks. First of all, the kill-command is not secure. The secret to kill a tag is only 32 bits long and so brute-force attacks could take place. Additionally, in many cases it cannot be assessed by the user whether the tag has been killed correctly or not, because the user cannot (visually) verify a successful kill. Thus, the user has to trust both the implementation of the kill command on the tag, and the reader which is responsible for sending the (correct) kill command.

6.5.1.1.2 The Sleep-Command

A way to temporarily disable tags is putting them to sleep [54]. A reader provides a tag with a hashed value[58] of a key: *meta-id=hash(key)*. This provision must take place securely, e.g. by near physical contact. After a tag received a *meta-id*, it is in a sleep mode, replying to requests with its *meta-id*. In order to wake a tag up, the reader has to send the *key* to the tag, which builds the hash of this value and compares it with the stored *meta-id*. Upon a match the tag is "awake" again and can provide the reader with the requested information.

The main problems with this concept are that it is very hard to convince the user that a tag really was sent to sleep. Furthermore, the *key* is sent in clear-text to the tag. Other problems arise in terms of traceability. A sleeping tag answers all requests with its *meta-id*, so it can still be tracked by this information.

Figure 5 shows an example scenario whereby putting tags to sleep could be used. Assume that the goods at a supermarket are equipped with RFID tags. At the checkout the tags are put to sleep by providing them the proper secret. The secret has to be stored in a database together with the products when they enter the store. The secrets for all purchased products are given to the customer. Maybe some kind of "PrivacyCard" exists, as depictured in the illustration. The checkout could provide the needed data to this card. The user then can activate the tags by using the secrets stored on his personal PrivacyCard. So the tags could be used for the smart fridge, but on the way home, no one could scan the contents of user's shopping bag.

[58] "A hash function is a reproducible method of turning some kind of data into a (relatively) small number that may serve as a digital "fingerprint" of the data. The algorithm "chops and mixes" (i.e., substitutes or transposes) the data to create such fingerprints, called hash values. […] Cryptographic hash functions are used for various purposes in information security applications." So called one-way hash functions are irreversible, i.e. it is (computational) impossible to find the input value for a given hash value.

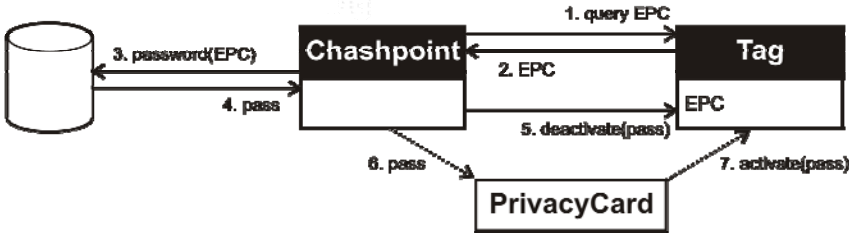

Figure 5: Supermarket example for putting a tag to sleep

The problem is that the user cannot be sure that the supermarket has not kept the secrets it handed out to the customer. Furthermore, this scheme requires user interaction. That said, in a world of discount cards, a PrivacyCard could well be adopted by the consumers, or the PrivacyCard functionality could be integrated into discount cards from the beginning.

In [55] an enhanced "sleep-version" is introduced, called "Randomized Access Control". Here, the tag responses to a request with a random number *r* and a value *h=hash(r || id)*. The reader has to search its database in a brute-force fashion to find the corresponding *id*. It is obvious that this scheme is only applicable in a system with relatively few tags otherwise the search for the *id* would take too much time. Another problem is that tags have to implement a random number generator[59] which produces good random numbers.

6.5.1.2 Blocking Access to the tags

The term "Blocking access" refers to practices which prevent any communication between reader and tag. A basic approach is the Faraday cage. A Faraday cage in theory blocks all read or write attempts to tags by blocking the radio-waves from the reader to the tag, thus ensuring confidentiality and integrity of the data on tags. A popular example is wrapping an RFID enabled electronic passport into aluminium foil. It is disadvantageous that the user has to be active in order to get the protection. Furthermore, it is difficult to determine if a given Faraday cage can actually block read/write attempts in all situations. It also does not seem feasible to put all tags into Faraday cages: e.g. tags which are sewn into clothes or which are merged with a product which does not work from within a Faraday cage, like a mobile phone.

6.5.1.2.1 Blocker Tags

Instead of destroying, killing or putting to sleep, another approach is to block the communication between reader and tag. In [38], Juels *et al.* introduce such a concept. This is done by disturbing the anti-collision protocol which takes place at the network layer. Collision avoidance protocols are used in dense networks to prevent two or more tags to send at the same time. There are two popular collision avoidance protocols, the ALOHA protocol and the tree-walking protocol. The latter works by traversing a binary tree, which spans the available address space of the tag identifiers. The address space is narrowed down at each step, until only a single tag is answering, thus no collisions occur. The reader then communicates with this tag.

The blocker introduced in [38] disturbs the reader's selection process by simulating tags for each possible identifier, i.e. by answering each request of the reader. Thereby the reader will

[59] A Random Number Generator (RNG) produces random numbers upon request. The generation of real random numbers is very hard to realise, thus in practice so called Pseudo RNGs (PRNG) are often used. PRNG do not produce real random numbers, but numbers which are close to random.

always get collisions, thus never stop the tree-walking protocol and its attempts to single out one tag.

This simple approach has a couple of drawbacks. The blocking scheme in [38] does not work with the ALOHA or other proprietary collision avoidance protocols. Also, the success of the blocking depends on the physical arrangement of the blocker and the tags and so its efficacy is therefore hard to know. Equally, it seems difficult to block only the tags of the user wearing the blocker-tag and not tags of other users close-by. Another issue is that the users have to actively apply the blocker-tag, which makes up an obstacle in usage. This is boosted by possible extensions of a simple blocking-tag, in which a user can define trusted readers which are not blocked.

6.5.1.2.2 Using external devices

The third example scenario is about blocking too, but at a more sophisticated level. In this scenario, a mobile phone takes over the control of tags and controls access to them via privacy policies, which are defined by the user (as illustrated in scenario S3).

This section engages in proposed solutions which rely on some kind of external device to give the user control over his personal information and data. The basic idea is that external devices are much more powerful than any RFID tag, especially the passive RFID tags. Thus, the devices can take over privacy functions which are unfeasible to integrate into RFID tags.

In the so called "proxying approach" a trusted device (sometimes called "watchdog") acts as a kind of surrogate between reader and tags and controls access to the tags according to user defined privacy rules.

Instead of a direct communication between reader and tag, the reader first communicates with the proxy-device (watchdog), which analyses the request made by the reader and decides whether a reader may access the data of a given tag or not. Thus, this watchdog can secure the confidentiality of the tags (see Figure 6).

Figure 6: Scheme of the "proxying approach"

The proxy-device first collects all the necessary data from the associated tags (**1.** and **2.**) and afterwards it, instead of the tag, communicates with the reader (**4.** and **5.**). The tag is either sent into a sleep mode or similar status, in which it cannot communicate with any reader, or the privacy-sensitive information on the tag are overwritten by the proxy-device (**3.**).

At this point a major drawback shows up: if the data is overwritten permanently, or if the tag is killed or destroyed instead of put to sleep, the usability of the tags depends on the watchdog. Furthermore, the user has to carry a trusted device (which needs to exist in the first place, which is not the case right now) and the watchdog device needs to be actively configured by the user according to his wishes. Further, this trusted device needs some way to acquire and probably release the tags of the user. Problematic in particular are cases where the

tags have PINs associated with them, which control access to their data. These PINs have to be accessed and transferred in a secure way from the tags to the watchdog.

6.5.2 Controlling Access by Authentication

Authentication is an important cornerstone of secure computing. In order for the tag to authenticate a reader, i.e. to check whether a reader has the rights to access the tag's data, secure authentication methods must exist. This is also the case when a reader wants to authenticate a tag.

In general, these secure authentication protocols and mechanisms exist, but it is difficult to port these schemes to low-cost, passive RFID tags. The following text shows existing and newly developed measures for authentication.

6.5.2.1 Symmetric cryptography

Symmetric cryptography means cryptography using a shared secret between the involved entities. The secret is used to encrypt and decrypt data sent between the entities. By proving the possession of the secret, authentication can be applied.

The classic but weak authentication mechanism uses a password. The tag stores a password and only reveals its information upon receiving the correct one from a reader. Thus a shared secret exists between reader and tag (in Figure 7 it is '*key*'). Since the password should not be sent in clear-text, a challenge-response scheme is often used: the tag challenges the reader with a (randomly) chosen value (cp. step **1.** in Figure 7); the reader encrypts ('*enc*') this with the key (steps **2.**, **3.** and **4.**) and sends the cipher text back which can be evaluated by the tag. It is crucial that the value is chosen randomly else replay-attacks are possible. Therefore a random number generator (RNG) is necessary at the tag as well as the possibility to encrypt and decrypt messages.

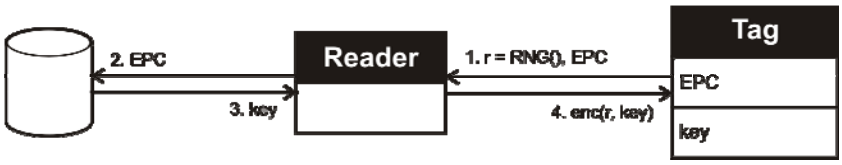

Figure 7: Reader to tag authentication via the shared secret '*key*'

The current password functionality of the EPCglobal standards does not protect the reading of the stored tag identifier (EPC). To ensure privacy, the standards have to be extended for read-authentication without the provision of the tag EPC.

In many industrial scenarios the authentication of tag to reader is very important, e.g. to detect forged goods, a tag has to authenticate itself to the reader in order to prove the originality of the object that the tag is fixed upon. Again, authenticating the tag to the reader via a pre-installed shared secret is possible, and again a challenge-response mechanism should be used in order to avoid sending the secret in clear text.

The tag to reader authentication is also the key point in the scenario S2. A user identifies himself using his proximity card. The card authenticates itself to the reader, thus the bearer of the card gains access to the facility. Additionally, the reader authenticates itself to the card, too. But as the scenario states, a breach in security is possible by simply scanning the tag and

creating a new tag with the scanned data. The new tag is a digital copy of the original tag, which the reader cannot recognise without further security measures. To prevent such attacks, more sophisticated security principles have to be applied. The next section deals with asymmetric cryptography, which can provide more security than mere passwords.

6.5.2.2 A combination approach

In [93], another approach for solving the privacy problem of RFID tags while preserving their business values is described. This approach has at least the following 3 aspects:

- Changing mode of operation (like the explained "sleep" and "kill" modes)
- Usage of an external device (see section 6.5.1.2.2)
- Controlling access by authentication using symmetric cryptography (see 6.5.2.1)

The basic idea is that the owner of an RFID tag has some personal device which stores RFID tag related secretes, i.e. secretes shared between the tag and the device used for mutual authentication and secret information about the tag, e.g. its EPC code. A given RFID tag will only communicate if it receives a request that fulfils the requirement that the sender must have known the shared secret. This way an attacker who does not know the shared secret will not even learn if the tag is present or not. Moreover, the messages exchanged during the authentication process are different each time so that a given tag could not be tracked by eavesdropping on the execution of the authentication protocol. Finally, the tag itself does not store any privacy invasive information (like the EPC code) so that neither eavesdropping on the RFID tag communication nor physical attacks on the RFID tag would reveal that information.

The authentication protocol uses only computationally "cheap" operations (XOR and hash function) making an implementation feasible. However, the RFID tag needs to be writable. The reason for this is that during the lifetime of an RFID tag the ownership of the RFID tag usually changes and therefore so should the related secrets stored on the RFID tag. Additionally the authors of [93] propose that the RFID tag should support two modes of operation: the EPC mode where the tag works like a normal EPC RFID tag and the privacy mode where the tag works as described above. The idea is that the tag acts as a normal EPC tag during the whole supply chain and in-store. At the point of sale, the privacy mode will be enabled and the ownership of the RFID tag will be handed over to the customer. As the RFID tag is not "killed" the customer can integrate his RFID tags into his home automation environment, e.g. allowing the washing machine or the refrigerator to communicate with the RFID tag. Of course the owner can also reactivate the EPC mode if this is necessary, e.g. for warranty handling or waste management.

From a technical point of view, this procedure solves many of the "after buy" privacy related problems of RFID tags. However, concerns regarding vulnerabilities in the solution have been raised by [94]. Further, there are many open issues. The in-store traceability of customers is not solved. It is very questionable if people will be able to manage actively all their RFID tags. Depending on the usage scenarios another problem might be that a device which wants to find out which RFID tags are present (e.g. a washing machine) has to enumerate through all the shared secrets of known RFID tags.

6.5.2.3 Asymmetric cryptography

Two usage scenarios exist for asymmetric cryptography: one is encrypting a message with the public key and decryption with the private key, the other is signing with the private key and verifying a signature with the public key. A general drawback of asymmetric cryptography is that its mechanisms need more effort compared to symmetric cryptography. Thus asymmetric cryptography usually is much slower than the symmetric counterpart.

Cryptography with private-public keys does not require a shared key, but a so called Public Key Infrastructure (PKI). A PKI is required for the mapping between a key and its holder, because a public key is only valuable if the ownership of the key can be verified. This also implies that a Certificate Authority (CA), which issues the public key certificates, has to be available[60]. Certificates then can be used to verify the ownership of a certain public key to an entity, here tag or reader. Translated into scenario S2, both the reader and the tags should have been equipped with certificates. Upon a request by the reader the tag asks for the reader's public key, signed by a higher ranking certificate authority. A challenge-response protocol could then verify that the reader is also in the possession of the private key. Only when the public key is valid and the reader could prove that it has the appropriate private key, the tag will answer any requests. A request could be another challenge-response protocol, initialised by the reader. The reader sends a request to the tag and the tag encrypts this with its private key which can be verified by the reader using the available tag's public key.

Using their public keys, the tag and reader could exchange securely a secret which after a successful authentication could be used to encrypt data. Thus, the communication would be protected against eavesdropping.

Using this kind of approach, the read-out of the proximity card in scenario S2 through an unauthorised reader could be prevented. The attacker's reader is not in possession of the required private key, thus it could not authenticate itself to the tag.

Although this approach is realistic for a security-application like proximity-cards, it is not applicable for low cost scenarios. Asymmetric cryptography is expensive, not only in terms of power-consumption, but also in terms of fabrication of the tags. Furthermore, a public key infrastructure has to be established, which is complex and expensive too.

Regardless of the kind of encryption used, key management stays an important factor, and there is no easy solution in sight.

6.5.3 Using cryptography to enhance privacy

As stated in the beginning of this section, it is vital that the tags can be produced very cheaply otherwise it is very unlikely that any major support by RFID vendors will take place. Thus, it is crucial that security and privacy methods are designed which can be easily integrated into the existing RFID designs and which can be produced in a low-cost manner. Current cryptographic functions and measures often concentrate on achieving a maximum level of security. Resource consumption has rarely been the focal point of research. But for RFID tags resource consumption is a key issue. Tags have to be cheap in production, need to be small in (physical) size and can only work with a limited amount of energy which is provided by RFID

[60] See also FIDIS deliverable 3.2: A study on PKI and Biometrics

readers. Hence it is vital that any cryptographic method is suitable for the special needs of RFID.

6.5.3.1 "Minimalistic Cryptography"

In [45], Ari Jules presents a concept called "Minimalist Cryptography for Low-Cost RFID Tags". The idea is to equip RFID tags with a list of pseudonyms instead of just a single one. The tag rotates randomly through the pseudonym list and returns another pseudonym for each request. Instead of directly transmitting the pseudonyms to the reader, a kind of challenge-response protocol is executed, by which means the submitted value changes for each transmission, even if a pseudonym is requested more than once.

The tag communicates with verified readers only, i.e. with readers knowing a shared secret. Readers supply the tags with so called pads, which are used to "mask" the pseudonym before transmission. A tag combines a received pad with *m* previously transmitted pads, so that an attacker must eavesdrop on all previously sent *m* pads to mount an attack. Attacks refer to the swapping of tags and to breaking the confidentiality of the pseudonyms.

The paper introduces a couple of restrictions on the attacker. First, a weak attacker is assumed, i.e. an attacker may only interact a limited time with a tag before this tag communicates again with a trusted reader. Then there is the assumption that the attacker has a restriction on the ability to mount a man-in-the-middle attack, since it seems realistic to assume that a user is moving a lot with a tag, thus making it difficult for an attacker to mount such an attack at each point where the user goes. Especially the later assumption only applies to weak attackers, because more sophisticated attackers can of course easily "simulate" a direct interaction between tag and reader by transmitting the necessary data over long distance networks like the nearly ubiquitous Internet.

Practical problems arise from the fact that the proposed protocol requires multiple flows of data between the tag and the reader, which might diminish the effectiveness with which RFID tags can be read. Furthermore it is required that readers are online. All in all this seems to be an interesting proposal, but the attacker model has to be revised carefully. The proposed protocol would be an extension of the existing RFID standard rather than a modification.

6.5.3.2 Universal Re-encryption

An approach to minimise traceability could be to change the identifying part of the tag repeatedly. Problems occur when the changed identifier of the tag cannot be reversed to the original identifier, thus rendering desired functionality useless. A concept is needed by which the ID of tags can be changed unpredictable for an attacker, but reversible for a valid user, e.g. the owner of the tag. In [56] such a scheme is proposed, called "universal re-encryption". The identifier of a tag is encrypted with the help of a public key, probably the one of the user, i.e. the owner of the tag. Whenever the user moves by an enabled RFID reader, the reader reads out the current encrypted ID and *re-encrypts* it, without knowledge of the private or public key. The newly encrypted ID is written to the tag, and can be changed by the next reader. Thus, the tag identifiers change in a seemingly random way.

A common example is the scenario in which a user walks home from shopping and at certain points, e.g. banks or other publicly available trusted points, readers readout all the tags the user carries in the shopping bag and change their IDs. At home, the user uses his private key

to decrypt all the tags, in doing so restoring the original IDs, which can subsequently be used by e.g. the smart fridge.

The proposed scheme does not require any cryptographic functionality on the tags themselves, but an infrastructure of RFID readers which can perform the re-encryption. The problem is that the scheme does not prevent tag swapping nor does it offer integrity safety. The latter is addressed by Ateniese *et al.* with an extension of the scheme ("Untraceable RFID tags via insubvertible encryption"), which uses signatures of a central authority.

6.5.3.3 Proof for simultaneous scanning of tags

Cryptography can be used not only to avoid something, like traceability, but also to ensure certain properties, e.g. the integrity of data stored on the tags, or that two tags have been scanned simultaneous. Whereas the first example does not need further explanation, the latter needs some clarification on its usefulness.

For example, medicine purchased in pharmacies must contain a leaflet describing the usage and side-effects of the medication. It would be desirable to have a proof by which it can be stated that one tag has been scanned simultaneously with another tag.

In [57] such a method is described (see Figure 8). Every tag has a counter and a secret. A reader starts the protocol by requesting $a = (A, c_a, r_a)$ from Tag A, where A is the identifier of A, c_a is tag A's current counter and r_a is a secret (composed of the current counter and the secret key). Now the reader requests the so called MAC of B, which B computes using a and its counter: $m_b = MAC_{xB}[a, c_b]$. This MAC is sent to tag A via the reader, which can now create its own MAC: $m_{ab} = MAC_{xA}[a, b]$, whereas $b=(B, c_b, m_b)$. m_{ab} is returned to the reader, which creates $P_{AB} = (A, B, c_a, c_b, m_{ab})$, which can be used by a verifier V knowing the secrets of the tags A and B (i.e. x_a and xb) to verify that both tags have been scanned at the same time.

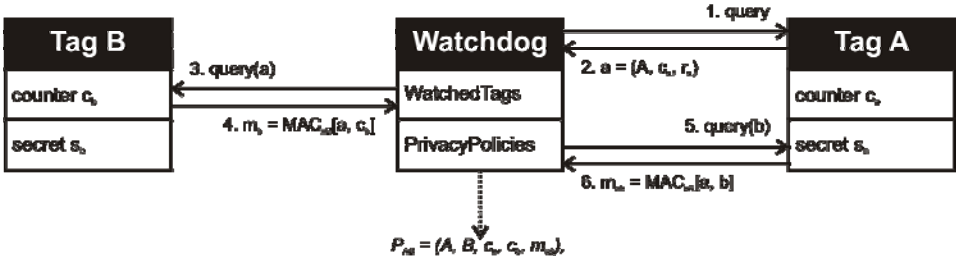

Figure 8: Scheme of the simultaneous scanning of two tags with generated proof P_{AB}

For this scheme to work the following prerequisites have to be met: The tags have to be tamper resistant, the tags need some kind of timeout functionality to detect problems and last of all the readers have to be trustworthy. If these conditions are fulfilled, proofs can be created. Right now, this concept works only for two tags. It has to be investigated if and how this scheme can be modified to support an arbitrary number of tags.

6.5.4 Tracking

As mentioned earlier, one of the risks which may emerge by utilising RFID in everyday applications is the problem of tracking. RFID tags can be read out without direct contact, without the knowledge or consent of the person concerned and without leaving any traces.

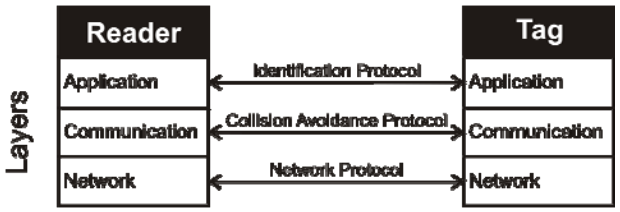

Figure 9: Tracking at different RFID layers

Tracking is a multi-layer problem. Next to tracking a tag via its EPC (unique global identifier), i.e. at the application layer, tracking may occur as well at the communication and the network layer (the three different layers are illustrated in Figure 9).

6.5.4.1 Tracking at the communication layer

The communication layer defines the communication between reader and tag, e.g. collision-avoidance protocols resides at this layer. One popular collision-avoidance protocol is the tree-walking protocol, which has been described in chapter 6.5.1.2. When this protocol is used, tracking can take place by monitoring the tree-walking protocol and its results instead of the EPC.

To avoid tracking at the communication layer when using the tree-walking protocol, [55] introduces the so called “silent tree-walking protocol”. It differs from the normal tree-walking concept insofar as the bits sent from the reader to the tags are encrypted. For the encryption, the reader and all the tags must share a secret.

To avoid key management issues, the shared secret can be derived from something the tags have in common. For example, assume that the tags have the same vendor, thus the first part of their EPC is equal. The reader asks for the “next” bit after the equal part of the EPC, i.e. the first “next bit” is the first bit of the object-specific part. At some point the first collision will occur, i.e. some tags will send a 0, some a 1. Now the reader must specify which tags should go on, and which should be singled out. Therefore, the reader sends *lastBit* XOR *nextBit*. The tags know which bit they sent last, so they can XOR the received value and determine if their next bit matches the requested bit. If so, they answer again. If a collision occurs, the reader request the next bit, encrypted by the previous bit, else if no collision occurs, the reader just requests the next bit. In this way, the data from the reader to the tags is encrypted by the previous sent data, but the data from the tags to the reader is not encrypted but sent in plaintext.

This can only work if we adjust the attacker model such that an attacker may only eavesdrop on the forward-channel (from reader to tag) and not on the backward-channel, i.e. the channel from tag to reader. If this assumption is valid, this scheme yields confidentiality of the tag data. Additionally, the tags need to have the ability to compute XOR functions.

In a more general scenario, one can use the limited range of the backward-channel to submit secrets from a tag to the reader. For example, a tag generates a random number and sends this to the reader via the short-range backward-channel. The reader can use this data to encrypt the data sent on the forward-channel. Again, if an attacker has access to the backward-channel, i.e. can eavesdrop on the backward-channel, he can learn the secret and thus break the encryption.

Another approach to avoid tracking at the communication layer is given in [58]. The singulation process requires an identifier for a tag which can be different from the EPC. Also, it is not required that this identifier is static. Avoine and Oechslin suggest using random numbers to provide identifiers. The random numbers change on a session-based manner, i.e., when a reader requests an identifier for the singulation process, the tag starts a session, for which a random number as a new identifier is created. The session is closed when the reader signals that the singulation process is finished or after a timeout. The timeout could be implemented simply by using a capacitor.

Next to the technical problems like random number generation and reliable timeout on passive tags, this scheme is particularly problematic since it requires changes to current specifications like the EPC draft 5 or existing products like the ICode1 Label IC. Furthermore, the collision avoidance protocols used in current RFID systems are often proprietary closed source algorithms, making an in-depth analysis difficult.

6.5.4.2 Tracking at the physical layer

The physical layer of the communication between RFID reader and tag defines the used transmission modulation, the frequency, timing, etc. Tracking at this layer does not take place by using some identifier like the EPC, but rather by analysing certain patterns and behaviour of different tags. The basic assumption is that each tag is in some way unique, even if it has been produced by the same vendor in the same factory on the same production line. Minor differences in the way the transmission modulation, the frequency or the timing can lead to a kind of unique fingerprint for each tag.

These properties cannot be avoided, but by reducing the diversity of standards used for the physical layer of tag to reader communication, the differences between the tags can be reduced, thus leading to more similar fingerprints which are harder to distinguish, at least at a reliable level. However, it is likely that manufactures will want to experiment with different technologies to produce tags in order to optimise performance, price or size, rather than sticking to a few standards.

6.5.5 Privacy enhancements by pseudonym usage

The use of pseudonyms could prevent the leakage of the EPC where secure communication between reader and tag is not possible. The Hash-Lock method uses pseudonyms. In chapter 6.5.1.1.2 the concept of putting a tag to sleep is introduced, which can be seen as a way of supplying a tag with a pseudonym. The tag always replies with its meta-id as a pseudonym, until a reader can provide it with the correct key. The key is used to build the pseudonym in the first place.

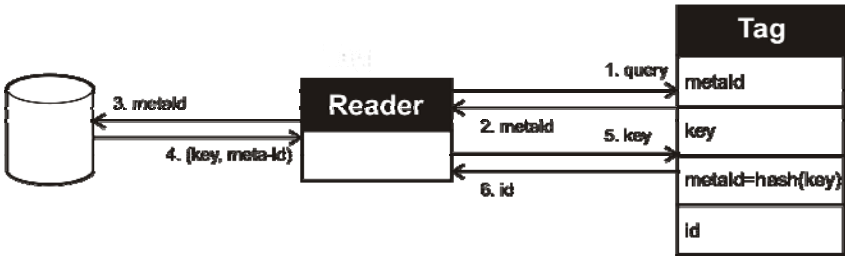

Figure 10: Scheme of the Hash-Lock method

Figure 10 depicts the hash-lock method. A tag replies to a request (**1.**) with its pseudonym, i.e. its *metaId* (**2.**). The reader then connects to a back-end database (**3.**). In the database *(metaId - key)* pairs are stored, which are returned to the reader (**4.**). The reader then sends the retrieved *key* to the tag (**5.**), which runs a hash-function with the *key* as the input and compares the result with its stored *metaId*. Upon a match the tag returns the *id* (**6.**). The main disadvantage of this approach is that the *metaId* can be used for tracking too, since it is static.

An advanced scheme is the "Random Hash-Lock" method that returns a hash-value with the tag-id and a random number *r* as the input to the reader (**2.** in Figure 11). The reader has to execute a brute-force search in a database for a match (**3.**), i.e. the database has to execute the hash function for all *ids* in the database with the given random number *r*. Because of the brute-force search, this method is only applicable in settings with a relatively small amount of tags.

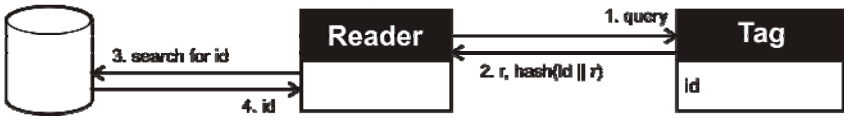

Figure 11: Randomised Hash-Lock scheme

An interesting problem occurs when considering forward security. Assume a scheme like that proposed by [45], i.e. where each tag has a bunch of pseudonyms which it uses randomly, thus avoiding traceability. A user carrying such a tag will leave weak traces, because databases will store different pseudonyms over time, thus only giving an imperfect image of the movement of a user. But if sometime in the future an attacker gains access to the list of pseudonyms stored on a particular tag, the attacker could re-trace all steps, since he now knows all used pseudonyms. A late tracing process could start. Problems like "back-tracing" must be prevented, even if a tag or the data stored on the tag is compromised.

To this end, [52] proposes the following solution: Each tag has an initial secret *s*. When a reader requests the id of the tag, the tag sends $a_i=G(s_i)$, where *G* is a one-way hash function. After sending this hashed secret, the tag renews its secret to $s_{i+1}=H(s_i)$, where *H* is another hash function. The reader needs access to a database where s_i is stored. After receiving $a_i=G(s_i)$, the reader has to do a brute-force search in the database, matching a_i to the secrets. After finding s_i, the database can identify the tag. Now s_i has to be updated at the backend to a_i. The backend database and the value stored at the tag are equal again.

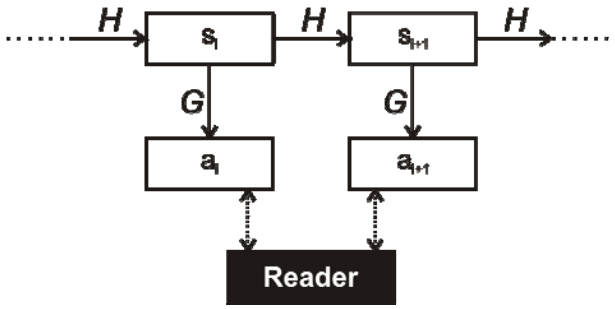

Figure 12: Forward security with chained-hashes; *H* and *G* are hash functions

This scheme is forward-secure because, even if an attacker gains knowledge of the current secret stored in the tag, this attacker can only reconstruct the last point of access by a reader. All previous scans cannot be checked by the attacker, since the current value is a hash-value of the previous value. And since the hash-functions are one-way only, it is practically impossible to find the previous id. Thus an attacker cannot track the movement of the tag.

The problems with this scheme are evident: the reader must conduct a brute-force search, which takes a lot of resources. Then, the secret stored in the tag and the data stored in the database have to match. This property makes the scheme vulnerable to denial of service attacks. The method can be adjusted to be more fault-tolerant (thus less vulnerable to denial of service attacks), at the expense of a more expensive search. And thirdly, the tags have to implement two one-way hash-functions, which is expensive.

6.5.6 Privacy by voluntary commitment

Enforcing privacy via technical measures like cryptography or watchdog tags is one approach. Another way could be some kind of self-control or voluntary commitment, meaning that companies commit themselves to not misusing collected data and additionally to only collect data the users have given consent to.

6.5.6.1 Soft-Blocking

Juels and Brainard propose so called “Soft Blocking” [59]. The idea is that users define a privacy policy in which they determine which data can be collected by which readers at which time, etc. RFID readers have to implement a policy-engine (in either hardware or software) which evaluates privacy policies and determines if scanning of a certain tag is valid and in which way the collected data may be used. Thus the concept relies on individual user-made privacy policies which the readers respect and obey.

The three main problems with this concept are:

1. The user has to define complex privacy policies, and vendors and operators have to implement according (complex) policy-engines.
2. The user has to trust that the readers will comply with the given rules and control is hard to give (see below Section 6.5.6.2).
3. Attackers would not adhere to any rules, no matter how many privacy policies a user defines.

The main-danger with concepts like this is that they are complex for the users to apply, which will lower the acceptance and usage. Furthermore, even if users embrace this concept, no real

security and privacy is given, but the users may well falsely imagine themselves in safety. As an example, the P3P project aims to bring voluntary commitment to web-pages (mainly commercial ones), but it seems that this project cannot accomplish its self-imposed goals, the industry has no real interest in adhering to any privacy regulations in a voluntary way.

6.5.6.2 Controlling the voluntary commitment

In order to provide the user with trustworthy information on whether a reader adheres to defined privacy policies, [53] proposes a trusted computing concept. A reader is split into three parts: the core, a policy engine and a consumer agent. The core should be small enough such that the integrity measures of trusted computing are feasible, i.e. secure booting, secure operating system, etc. The policy engine should enforce privacy policies. The consumer agent eventual should allow individuals or organisations like privacy commissioners to monitor the activities of the RFID reader in order to detect any privacy breach. Furthermore, remote attestation in combination with the core should enable checks on whether a certain policy engine is trustworthy or not. The remote attestation can be used by concerned individuals to ensure that a reader runs a certain reader core, policy engine and consumer agent. Thus, privacy regulations can be controlled and the owner of the reader can furthermore check if the reader has been compromised.

The reader core, which is a so called "sealed storage", can store secrets needed for secure authentication or communication between reader and tag. The secret is secure even if the reader is controlled by an attacker. Thereby, confidentiality of transmitted data between an RFID tag and a reader can be ensured.

This concept has a couple of drawbacks. First of all, trusted computing is quite a new concept, and it is not evident that it can really provide the promised security, such as not revealing stored secrets when being compromised. Further, the introduction of the consumer agent is not reasonable: either one believes in the trustworthiness of trusted computing, and so the consumer agent is redundant, or one does not believe in trusted computing, and so one cannot trust in the consumer agent either since it could be compromised too. Moreover, having the CA implies additional risks to privacy as the reader's logs are transferred to some external (potentially untrustworthy) third party.

6.6 A first approach

One of the basic security paradigms, applied in many other domains, which should be applied in the context of RFID is the paradigm of *multilateral security* [60]. According to this paradigm, each party, entity or stakeholder of a system has its own security goals and does not *per se* trust the other parties concerned. Hence the conflicting interests require a negotiation to find a compromise which could be accepted by each party.

Applied to RFID, this means that the conflicting interests of costumers, producers, retailers, etc. have to take into account developing Privacy Enhancing Technologies (PETs) for RFID. Moreover, at least the design of the three main components should not rely on the assumption that the other components are trustworthy and secure. Instead, when designing the whole RFID system, each component should be treated as potentially insecure. If this would lead to the impossibility of developing the RFID application, meaning that certain components need

to fulfil certain security properties, then all the underlying assumptions have to be explicitly named.

This could be exemplified using scenario S1. Here the backend system implicitly assumed that the RFID tag is secure, i.e. the data stored on the RFID tag could not be manipulated. Clearly there is no reason for this kind of trustworthiness and security assumption especially because there are no mechanisms implemented which ensure this kind of manipulation protection. If the system was designed with the "trust no-one" presumption in mind and would have explicitly named any assumptions which violate this, one would easily detect the missing mechanisms to protect the backend against malicious or manipulated RFID tags or readers.

Based on the principles proposed by [48] (see 6.3.4) and the general ideas of multilateral security, [48] and [51] proposed a checklist with which PETs for RFID can be evaluated. The content of this checklist is as follows:

Table 2: The Privacy Enhancing Technology (PET) concept:

C1: enforces making sparing use of data?[61]	**C12:** does not interfere with active protection measures?[62]
C2: makes privacy the default?[63]	**C13:** avoids creation and use of central database(s)?
C3: transfers control to citizens?[64]	**C14:** avoids creation and use of databases at all?[65]
C4: sends tags to a secure mode automatically?[66]	**C15:** enables functionality after point-of-sale in a secure way?[67]
C5: can prove that automatic activation of secure mode always works?[68]	**C16:** can be achieved without changing RFID physical technology?
C6: prevents eavesdropping of tag-reader communication?	**C17:** does not make tags much more expensive?
C7: protects citizens from producer?	**C18:** does not make tags more expensive?
C8: protects citizens from retailer?	**C19:** does not introduce additional threats to privacy?
C9: protection includes in-store problem?[69]	**C20:** introduces additional benefits for privacy?
C10: protects tag in secure mode against presence-spotting?	**C21:** provides benefits for the retailer?
C11: does not require citizens to take active protection measures?	

[61] Making sparing use of data shall not just be a nice-to-have, but shall be enforced by the design of the PET concept.
[62] E.g. using blocker tags. Active protection measures are controversial but there should be no loss in privacy protection through interference with other privacy protection mechanisms.

[63] It is not sufficient only to demand certain default settings - citizens' privacy protection must be the fundamental principle of the PET concept. In particular, applications that might affect a citizen's privacy must require explicit permission from the citizen. If no action is taken there must not be any privacy violation.
[64] In particular citizens must be given complete and exclusive control of every tag that they carry, or that can otherwise be related to them, where today the manufacturer and retailer have this control.
[65] Databases allowing creation of associations between objects and people either directly or indirectly
[66] Unsafe tags are disabled forever ("killed") automatically

[67] E.g. intelligent fridges or washing machines
[68] It must be possible to prove rigorously that the system used for deactivating the tags will always deactivate every tag and that this system cannot be circumvented by the producer or the retailer.
[69] The "in-store problem" describes the situation inside the store where citizens may carry RFID tags and may be tracked, before any tags are deactivated at the point-of-sale.

6.7 Work in progress in FIDIS D7.9: Ambient Law

6.7.1 Conceptualisation of Ambient Law

Ambient Law (AmL) should articulate the relevant legal norms into technological devices:

- the mandatory rules of D46/95 EC should be *inscribed* into the technological infrastructure and its devices, *making the violation of these rules impossible by design* (transparency, use limitation, purpose specification, consent, data quality, participation, accountability of the data controller)

    - **transparency:** history management of one's personal data and access to processed personal data with data controllers should be made possible via M2M communication
    - **purpose specification & use limitation**: such transparency should enable one's PDA (M2M) to check which purposes are declared, and to check whether the principles of purpose specification and use limitation have been complied with
    - **consent**: one's machine-proxy should be capable of negotiating the supply and processing of personal data, according to one's personal preferences, while taking into account the mandatory aspects of data protection legislation
    - **data quality & participation**: one's machine-proxy should be capable of matching data stored in databases with the one's accurate personal data, and be capable of requiring adjustments if data is not correct (anymore)
    - **accountability of the data controller**: at all times one's machine-proxy should be capable of *identifying* the data controller that reads, collects, stores, and/or processes data, including all others that have access to these data

- a legal right for citizens to access profiles that may be used to categorise them, irrespective of whether these profiles have been derived from one's own or other's (personal) data. The relevant criterion is not how the profile has been inferred (looking back) but how it can be put to use (looking forward). The point is whether the profile can be used to influence the opportunities or risks one is attributed (price discrimination, which is fine in itself as long as consumers are aware of the differences made, otherwise we have a market failure).

We could paraphrase: Ambient law in fact **uses the technologies** that data protection aims to legitimate while protecting against their undesired consequences, **in order to facilitate this protection**. This is a bit of a paradox, but not a negative one.

6.7.2 Three scenarios of AmI

The need for AmL was detected in the course of investigating the legal framework relevant to Ambient Intelligence. In FIDIS deliverable 7.9 three scenarios have been developed to

acquire a more accurate picture of the need for AmL. These scenarios are relevant here because they all involve many RFID enabled interactions.

Scenario I is user-centric: the user is empowered in AmI, carrying a device with which to control the environment, for example, by determining which data can be exchanged between user and environment. This may be a 'privacy-friendly' and perhaps a commercial doom scenario. Key concepts are 'data minimisation', 'contextual integrity', 'partial identities' (pseudonyms).

Scenario II is provider-centric: AmI is controlled by the providers of services (and goods, if there are still are goods by then). The environment knows exactly who is where and will interact without consent, and perhaps without knowledge, of the user. Data flows freely between users and their devices, service providers, and perhaps third parties as well. This may be a 'user-friendly' and commercial Valhalla scenario. Key concepts are 'data optimisation', 'networked environment' and 'distributed intelligence' (the intelligence flows from the interconnectivity).

Scenario III is a mix: in acknowledging that hiding data can make the environment less intelligent, while unlimited access to data can make individual citizens vulnerable to undesirable profiling, this scenario aims to achieve some kind of balance by minimising knowledge asymmetry.

As regards privacy, it is interesting to note that in all three scenarios the division between public and private is problematic - it seems to make more sense to think in terms of contexts. This is effectively already the case today: work may be done at home, private email may be exchanged from one's office, private conversations made on a mobile phone in the train or at a restaurant, CCTV cameras may register one's every movement 'on the road'. Traditional conceptions of privacy limit the relevance of the concept to the realm of private, while in visions like the 'Internet of Things' and AmI, the dividing line between public and private crumbles even further than in today's world, rendering any conception of privacy that is based on such a division redundant. According to Nissenbaum [87] the traditional understanding of privacy tends to employ a universal definition of privacy that restricts privacy to:

- limiting surveillance of citizens and use of information about them by government agents
- restricting access to sensitive, personal or private information
- curtailing intrusion into places deemed private or personal

The first scenario seems inspired by such an understanding of privacy, while the second scenario is the shameless negation of any effective concept of privacy. Nissenbaum instead proposes to understand privacy in terms of 'contextual integrity', in order to prevent the association with a separate private space. Her proposition follows an analysis of the violation of 'privacy in public', a violation that cannot be conceptualised in terms the private/public divide. The problem we face in visions of a smart interconnected world of things is the

increasing reach of public surveillance technologies that make people transparent in their public behaviour. These public surveillance technologies need not be under control of government agents, they can very well be the monitoring devices of the service providers that sustain the AmI environment. Instead of the general, a-contextual definition of privacy referred to above, Nissenbaum argues for the more sophisticated concept of 'contextual integrity', which entails:

- norms of the *appropriateness* of a specific information flow
- norms of flow or *distribution* of information

In an AmI environment that aims to combine citizens' autonomy with smart proactive computing, the determination of a violation of privacy should depend on the context and take note of the power imbalances prevalent between an individual citizen and the service provider that controls the flow of information. Such contextual determination implies flexibility and a keen eye for detail, but it does not mean that 'context is all' in the sense that general rules lose their meaning. According to Nissenbaum, norms of appropriateness and norms of distribution need to be inscribed at the constitutional, the legislative, the administrative and the judicial level: this would acknowledge the fact that privacy is an underdetermined concept with an open texture, though not entirely undetermined and not open to the extent that it can mean anything. Appropriateness comes close to several of the fair information principles, e.g. the purpose specification and the use limitation principle, but appropriateness seems to be more flexible. Instead of demanding that purposes are declared and the use of data limited to the declared purpose, norms of appropriateness demand that the purpose is appropriate, taking into consideration the context within which the data are exchanged. Distribution comes close to transparency rights, but again distribution seems a more responsive way to deal with information flows, as it takes into account the reciprocity between data subject and data controller.[70]

Nissembaum's concept fits well with the mixed scenario: other than in the case of user control, the intelligence of the environment is distributed (which is also the case in the second scenario), but:

- the flow of information is not unlimited (not every exchange of data or profiles is *appropriate*), and
- the transparency of consumer-citizens is countered by transparency of profiles (the flow of information is reciprocal, generating a fair *distribution* of knowledge and information)

Nissenbaum has made her concept of 'contextual integrity' operational in collaboration with John Mitchell of Stanford University [80]. This is an example of what she has called 'values

[70] Cp. the principle of reciprocity introduced by Roussos *et al.* in the context of mobile identity management, see Roussos, G., D. Peterson, *et al.* (2003). "Mobile Identity Management: An Enacted View." *International Journal of Electronic Commerce* 8 (1): 81-100. In FIDIS deliverable 11.1 this principle has been introduced to check on the power (im)balance between user and service provider. See also [20].

in design' [85], which comes close to AmL in as far as it denotes the articulation of specific human values in the design of a technology.

Nissenbaum and Mitchell have formalised aspects of the concept of 'contextual integrity' in a framework of temporal logic, thus articulating norms of transmission of personal data into technological devices [80]. One can imagine – if nanotechnologies[71] move in – that by the time AmI turns from vision into reality, RFID tags will have enough computing power to facilitate the type of M2M communication needed to realise AmL. This is not to say that we should wait for nanotechnology to create a holistic privacy framework for RFID. It rather means that computer engineers and lawyers should sit down – together with those versed in constructive technology assessment (CTA) – at this very moment, to construct the enabling socio-technical infrastructure for AmI in a way that inscribes the legal norms of privacy and transparency discussed above.

[71] See also FIDIS deliverable 12.2 'Study on Emerging AmI technologies'

7 Conclusions

The emergence of RFID technology provides the potential for vast and varied applications, bringing with it both promise and peril. The use of RFID technology in several contexts and its role as a prime Ambient Intelligence enabler raises important data protection and privacy threats.

The basic principles of the current European regulatory framework on privacy and data protection apply in cases when processing of personal data takes place in relation to RFID technology. The specific provisions of the e-Privacy directive are not however always applicable, as they presuppose processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. RFID technology however neither needs a publicly available electronic communications network nor involves respective providers. Therefore the European Commission in its Communication on RFID has identified this problem and will publish a Recommendation on how to handle data security and privacy of smart radio tags to Member States and stakeholders.

Many proposals for PETs for RFID exist - but only a few of them really seem to be feasible. One of the main problems is that low-cost RFID tags cannot offer any solution for strong privacy. Nevertheless in the short term the mechanisms suitable for a given area of application should be implemented in order to increase the level of privacy that the RFID systems offer. In the long-term many actions need to be taken to accomplish the goal of a holistic privacy framework for RFID which complies with strong privacy as well as security requirements.

In fact, the descriptions above only mention technology building blocks which might be of use for a holistic privacy framework for RFID - but they do not explain how these technologies could be orchestrated to achieve this framework. The reason is that the state-of-the-art at the moment is to have a privacy patchwork for RFID rather than a holistic and integrative approach. Major effort in terms of research and development seems to be necessary to achieve a true holistic privacy framework for RFID.

These necessary actions are associated with different levels:

- ***on the technical level***
  - cost effective RFID tags with hardware efficient cryptographic hash functions, symmetric encryption, message authentication codes, random number generators and timeout mechanisms need to be developed.
  - new RFID protocols need to be developed which use new possibilities to enhance the already known privacy and security mechanisms for RFID
- ***on the political and regulative level***
  - transparency and awareness need to be increased e.g. by laws which oblige the labelling of RFID tags and readers
  - research in the area of security and privacy for RFID needs to be intensified
  - the incentives for manufactures and users of RFID technology to develop more privacy friendly and secure solutions need to be increased

As problem P10 indicates, the combination of RFID and profiling, eventually coupled with many other means and techniques, may be a major privacy concern. Clearly, profiling itself already bears these problematic issues (e.g. [21]). In the context of RFID this problem – as already discussed in section 5.3 – is of major importance.

Clearly solutions to problems P16[72] and P17[73] are of major interest for solving the holistic problem. For the focus of P16, there is lots of work to be done, yet there is also lots of knowledge and routine in securing backend systems. The more general ethical considerations must be integrated more thoroughly in this context, but this must be seen in a more general view not only fixed to RFID techniques, as backend systems are used in various environments for different goals.

The more intrinsically problematic issue of PETs for RFID being globally applicable is on its first step a technical one, caused by the especially low capabilities (in storage and computing) of passive RFID tags.

Clearly there are different needs for different applications, there are applications that contain no (and will never contain) personal data at all and in those cases there is no need for privacy solutions. Then there are applications where the tag or the system as a whole contain some form of non-sensitive personal data (or data that might in some period of the tags life be considered non-sensitive personal data) in these cases some form of protection is needed otherwise there will be no possibility to control access to this data. Then finally there is the case where the tag contains (or could be linked to) sensitive personal data or data that in some period of the tags life could be classified as sensitive data. This case requires explicit consent of the data subject or needs to fulfil the other requirements in Article 8 of the data protection directive. In this case one would want the strongest possible (or justifiable) protection in order to stop unauthorised entities reading or altering data.

However, some of the information on the tag is always an identifier of the tag itself and if that tag is linkable to a person then the sensitivity of the information gained or derived from the tag is not only dependent on the information read from the tag but also on the context of where it was read. So part of the problem is in some sense application independent (or could even differ within an application). Because of this it is extremely difficult (if indeed not impossible) to give general guidelines on applications because a lifecycle analysis of the tag needs to be conducted and the possibilities that the tag in some part of its life or in some context will be personal or sensitive personal information needs to be estimated in some way. In essence this is a risk management problem. The question here is who should manage the risk - the person that is subject to the risk or some other party that is not affected by the risk. The person in control of the information is the one that can or at least has the possibility to manage this risk. We believe that the data subject should be in control of its own data or at least to the identifier of his/her information and in order to do so the means (and from the user perspective the real life ability) to exercise control needs to exist. The key to having this control regarding the RFID specific problems is to control the access to the tag. How strong this access control needs to be is in a risk management sense dependent on the value of the information, but who decides that value? Based on this we feel that it is very hard to give

[72] Both the core RFID infrastructure (RFID tag and RFID reader) and especially also *the backend system* have to be secured.
[73] PETs for RFID have to be *globally applicable* - this could prevent the usage of certain security technologies

general advice based on application types more than the division between strictly non-personal or possibly personal data. With more research into life cycle analysis methods for RFID systems that would give a clearer view of the data flows throughout the applications life a more fine-grained set of recommendations might be developed.

8 Bibliography[74]

[1] Warren, S.D., Brandeis, L.D., *The Right to Privacy*, Harvard Law Review, No. 5, 1890-91, pp.193-220.

[2] Westin, A.F., *Privacy and Freedom*, Atheneum, New York, 1967.

[3] Hogben, G., Annex A, *PRIME project deliverable D14.0a, (Framework V0),* June 2004.

[4] Lieshout, M. van, Grossi, L., Spinelli, G., Helmus, S., Kool, L., Pennings, L., Stap, R., Veugen, T., Waaij, B. van der, Borean, C.. *RFID Technologies: Emerging Issues, Challenges and Policy Options.* Sevilla: IPTS, EN22770. 2006, http://www.jrc.es/publications/pub.cfm?id=1476

[5] National Institute of Standards, *Guidelines for Securing Radio Frequency Identification (RFID) Systems* Special Publication 800-98, April 2007.

[6] CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), http://www.nocards.org/index.shtml

[7] EPIC (Electronic Privacy Information Center), RFID privacy page, http://www.epic.org/privacy/rfid/

[8] Bundesamt für Sicherheit in der Informationstechnik, *Risiken und Chancen des Einsates von RFID Systemen – Trends und Entwicklungen in technologies, Anwendungen und Sicherheit*, SecuMedia, 2004.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, hereinafter the "Data Protection Directive", Official Journal, L 281/31 – L 281/39.

[10] Dammann, U., Simitis, Sp., *EG-Datenschutzrichtlinie*, Nomos Verlagsgesellschaft, 1997, p. 109

[11] Kuner, C., *European Data Privacy Law and Online Business*, Oxford University Press, 2003, p.51

[12] Art. 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, WP105, 19 January 2005, Available at: http://www.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

[13] Art. 29 - Data Protection Working Party, *Working document on biometrics*, WP 80, 1 August 2003, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf

[14] Privacyrechtelijke aspecten van RFID, report prepared by the ECP.NL. Platform voor eNederland for the Dutch Ministry of Economic Affairs and in cooperation with the RFID Platform Nederland and GSI Nederland, May 2005, (p. 24), available online at http://www.rfidconsultation.eu/docs/ficheiros/Privacyrechtelijke_aspecten_van_RFID.pdf

[74] All on-line references last accessed 21/04/08

[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J. L201,37, 31 July 2002

[16] Theodora Toutziaraki, *Ein winzig kleiner Chip, ein riesengroße Herausforderung für den Datenschutz*, *DuD 31 (2007)*, S. 107-112 (109).

[17] Legal IST, D.15: *Legal issues of RFID technology*, 13.03.2006, available online at: http://193.72.209.176/projects/P1507/D15%20Report%20on%20Additional%20Legal%20Issues%20-%20final%20version.pdf

[18] Art. 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP131, 15 February 2007, Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf

[19] *Universal Declaration of Human Rights*, United Nations General Assembly resolution 217 A (III), 1948, Art. 12, http://www.unhchr.ch/udhr/lang/eng.htm

[20] Jiang, X. (2002). *Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social*, Privacy Workshop September 29, 2002, University of California, Berkeley. Berkeley, available at: http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/jiang-privacyworkshop.pdf

[21] Hildebrandt M. and Gutwirth S. (eds.), *Profiling the European Citizen – Cross-disciplinary perspectives*, FIDIS deliverable 7.5, Springer, 2008.

[22] Ateniese G., Camenisch J., de Medeiros B., *Untraceable RFID tags via insubvertible encryption,* in: *Proceedings of the 12th ACM Conference on Computer and Communications Security CCS '05,* ACM Press, p. 92-101, 2005

[23] Wood D. M. (ed.), *A Report on the Surveillance Society – For the Information Commissioner by the Surveillance Studies Network*, http://www.privacyconference2006.co.uk/index.asp?PageID=10

[24] EPTA European Parliamentary Technology Assessment network, *ICT and Privacy in Europe – Experiences from technology assessment of ICT and Privacy in seven different European countries*, 2006, http://epub.oeaw.ac.at/ita/ita-projektberichte/e2-2a44.pdf

[25] Bizer J., Spiekermann S., Günther O. (eds.), *TAUCIS Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung*, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, 2006, http://www.taucis.hu-berlin.de/_download/TAUCIS_Studie.pdf (12/28/06).

[26] Bird S. J. and Spier R. (eds.), *Report on the Budapest Meeting 2005 – Intensified Networking on Ethics of Science*, Science and Engineering Ethics, vol. 12(4), p. 731-793, 2006.

[27] Berleur J. and Brunnstein K. (eds.), *Ethics of Computing – Codes, spaces for discussion and law*, Chapman & Hall, London UK, 1996.

[28] Berleur J. and d'Udekem-Gevers M., *Codes of Ethics Within IFIP and Other Computer Societies*, in: *Ethics of Computing – Codes, spaces for discussion and law*, Berleur J. and Brunnstein K. (eds.), Chapman & Hall, London UK, 1996

[29] Association for Computing Machinery ACM, *ACM Code of Ethics and Professional Conduct*, (Adopted by ACM Council 10/16/92), http://www.acm.org/constitution/code.html

[30] The British Computer Society, *British Computer Society Code of Conduct*, 2001, http://www.bcs.org/upload/pdf/conduct.pdf

[31] Lee J. A. N. and Berleur J. *Progress towards a World-Wide Code of Conduct*. In: *Ethics in the Computer Age – Proceedings of the conference on Ethics in the computer age*, ACM press, p. 100-104, 1994, http://portal.acm.org/ft_gateway.cfm?id=199594&type=pdf

[32] Fawcett E., *The Toronto Resolution*, Accountability in Research, vol 3, p 69-72, 1994.

[33] acatech - Konvent für Technikwissenschaften der Union der deutschen Akademien der Wissenschaften e.V.: *RFID wird erwachsen. Deutschland sollte die Potenziale der elektronischen Identifikation nutzen*, acatech BEZIEHT POSITION, issue 1, 2006, Fraunhofer IRB Verlag

[34] FIDIS deliverable 3.6: *Study on ID Documents*, M. Meints, M. Hansen (eds.)

[35] Capgemini: *RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business.* 2005. URL: http://www.us.capgemini.com/DownloadLibrary/requestfile.asp?ID=450, published 9th February 2005.

[36] News release: *World's smallest and thinnest 0.15 x 0.15 mm, 7.5µm thick RFID IC chip*. Hitachi, Ltd., http://www.hitachi.com/New/cnews/060206.html, February 6, 2006.

[37] Spiekermann, S., Rothensee, M., *Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing*, Humboldt-Universität, Berlin, July 2005. Available at: http://interval.huberlin.de/downloads/rfid/neuste%20forschungsergebnisse/SocioPsychofak.pdf

[38] Juels A., Rivest R. L., and Szydlo M.: *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*. In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pp. 103-111. ACM Press. 2003

[39] Garfinkle S. and Rosenberg B. (eds) , *RFID: Applications, Security and Privacy*, Pearson Education Inc, July, 2005, ISBN-0-321-29096-8.

[40] Punie Y., Delaitre S., Maghiros I. & Wright D. (eds), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities,* Safeguards in a World of Ambient Intelligence (SWAMI) Deliverable D2, January, 2006.

[41] Juels A. *RFID Security and Privacy: A Research Survey*, RSA Laboratories, September, 2005

[42] ICAO_NTWG, PKI Task Force, *PKI for Machine Readable Travel Documents offering ICC Read-Only Access*, Technical Report, Version 1.1, October, 2004.

[43] Newitz A. *The RFID Hacking Underground* , WIRED, http://www.wired.com/wired/archive/14.05/rfid_pr.html

[44] Reid S., *'Safest ever' passport is not fit for purpose*, Daily Mail, http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=440069&in_page_id=1770

[45] Juels A. *Minimalist cryptography for low-cost RFID tags*. In Blundo C. and Cimato S., (eds), The Fourth International Conference on Security in Communication Networks – SCN 2004, volume 3352 of Lecture Notes in Computer Science, pages 149–164. Springer-Verlag, 2004.

[46] Rieback M. Crispo B. Tanenbaum A., *Is your cat infected with a Computer Virus*?, Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06) - Volume 00, pp169 – 179, 2006

[47] Sarma S. E., *Towards the five-cent tag*, Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org

[48] Hennig, J; Ladkin, P; Sieker, B: *Privacy Enhancing Technology Concepts for RFID Technology Scrutinised*, 2004, RVS Group, University of Bielefeld, Bielefeld, Germany, RVS-RR-04-02, available through http://www.rvs.uni-bielefeld.de → Publications → Research Reports.

[49] PRIME project leaflet, May 2005, https://www.prime-project.eu/press_room/leaflets/PRIME-flyer-20040518.pdf

[50] Garfinkel S. *An RFID Bill of Rights*. Technology Review, page 35, October 2002.

[51] Sieker B, Ladkin P. B, Hennig J. E. RVS Group, University of Bielefeld in cooperation with FoeBuD e.V. and Causalis Limited: *Privacy Checklist for Privacy Enhancing Technology Concepts for RFID Technology Revisited*, 13 October 2005

[52] Ohkubo M., Suzuki K., and Kinoshita S. *Cryptographic approach to a privacy friendly tag.* In RFID Privacy Workshop, MIT, 2003.

[53] Molnar D., Soppera A., and Wagner D. *Privacy for RFID through trusted computing* (short paper). In De Capitani di Vimercati S. and Dingledine R., (eds), Workshop on Privacy in the Electronic Society (WPES), 2005.

[54] Sarma S. E., Weis S. A., and Engels D. W.. *RFID systems, security and privacy implications.* Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT, 2002.

[55] Weis S., Sarma S., Rivest R., and Engels D.. *Security and privacy aspects of low-cost radio frequency identification systems*. In Hutter D., Müller G., Stephan W., and Ullmann M., (eds), International Conference on Security in Pervasive Computing – SPC 2003, volume 2802 of Lecture Notes in Computer Science, pages 454–469. Springer-Verlag, 2003.

[56] Ateniese G., Camenisch J., and de Madeiros B. *Untraceable RFID tags via insubvertible encryption.* In 12th ACM Conference on Computer and Communication Security, 2005

[57] Juels A. *'Yoking-proofs' for RFID tags*. In Sandhu R. and Thomas R., (eds), Workshop on Pervasive Computing and Communications Security – PerSec 2004, pages 138–143. IEEE Computer Society, 2004.

[58] Avoine G. and Oechslin Ph. *RFID traceability: A multilayer problem*. In Financial Cryptography -- FC'05, LNCS, Springer, 2005

[59] Juels A. and Brainard J. *Soft blocking: Flexible blocker tags on the cheap*. In De Capitani di Vimercati S. and Syverson P., (eds), Workshop on Privacy in the Electronic Society – WPES, pages 1–7. ACM, ACM Press, 2004.

[60] Müller G., Rannenberg K. (eds.): *Multilateral Security in Communications*; Addison-Wesley-Longman; München *et al.* 1999; ISBN-3-8273-1360-0

[61] Sotto L. J., *An RFID Code of Conduct*, RFID journal http://www.rfidjournal.com/article/view/1624/ 2005.

[62] UK RFID Council, *A UK code of practice for the use of radio frequency identification (RFID) in retail outlets*, release 1.0, 2006

[63] Heise Online News, *Data protectionists call for RFID code of conduct* http://www.heise.de/english/newsticker/news/75263 2006

[64] Heise Online News, *Neue Vorstöße zur RFID Selbstregulierung der Industrie* http://www.heise.de/newsticker/meldung/73621 2006

[65] European Expert Group for IT-Security (EICAR), *Task force on RFID "Leitfaden: RFID und Datenschutz"*, http://www.eicar.org/rfid/infomaterial/RFID_Leitfaden-100406.pdf

[66] Münzberg H, *Aufklärung der Konsumenten wird der Knackpunkt für RFID*, Capgemini http://www.de.capgemini.com/presse/pressemitteilungen/archiv_2005/rfid/ 2005

[67] Bungard D. *et al. Orientierungshilfe «Datenschutzgerechter Einsatz von RFID»*, Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 2006.

[68] Rodotà S., Capurro R., *Ethical Aspects of ICT Implants in the Human Body*, Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, 2005

[69] Pitkänen O. and Niemelä M, *Privacy and data protection in Emerging RFID Applications*, paper presented at the EU RFID Forum 2007, RFID Academic Convocation, 14 March 2007, available online at http://www.rfidconvocation.eu/Papers%20presented/Business/Privacy%20and%20Data%20Protection%20in%20Emerging%20RFID Applications.pdf

[70] Kardasiadou Z. and Talidou Z, *Legal issues of RFID technology*, Legal-IST, IST-2-004252-SSA, D15, 2006

[71] Müller J, *Ist das Auslesen von RFID Tags zulässig?*, *DuD (28) 2004*,p. 215

[72] Bygrave L, *Data Protection Law – Approaching its Rationale, Logic and Limits*, Kluwer International, 2002

[73] Dutch Ministry of Justice, *Personal Data Protection Act: Guidelines for Personal Data Processors* (2001)

[74] Commission of the European Communities, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the committee of the regions – *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, COM(2007)96 final.

[75] EU Press Release, *Commission proposes a European policy strategy for smart radio tags*, IP/07/332, Brussels/Hannover, 15 March 2007

[76] PRIME Project, Deliverable D14.0.a, Framework V0, Chapter 5.0 '*The Legal and Regulatory Framework for PRIME*' (Anna Buchta, Jos Dumortier, Henry Krasemann)

[77] Carey P, *E-Privacy and Online Data Protection*, Butterworths, 2002

[78] Schmidt A. *IT and the judiciary in the Netherlands - A state of affairs*. Computer Law & Security Reports 23 (3): 1-8, 2007

[79] Agre, P. E. and M. Rotenberg, (eds). *Technology and Privacy: The New Landscape.* Cambridge, Massachusetts, MIT, 2001

[80] Barth, A., A. Datta, *et al. Privacy and Contextual Integrity: Framework and Applications*. Sp, 2006

[81] Bygrave L. *Minding the Machine. Art.15 and the EC Data Protection Directive and automated profiling.* Computer Law & Security Report. 17: 17-24

[82] Custers, B. *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Nijmegen*, Wolf Legal Publishers

[83] Dötzer, F. *Privacy Issues in Vehicular Ad Hoc Networks*. Workshop on Privacy Enhancing Technologies. Dubrovnik, available at: http://www13.informatik.tu-muenchen.de/personen/doetzer/publications/Doetzer-05-PrivacyIssuesVANETs.pdf

[84] Fayyad, U. M., G. Piatetsky-Shapiro, *et al.*, (eds). *Advances in Knowledge Discovery and Data Mining*. Meno Park, California - Cambridge, Mass. - London England, AAAI Press / MIT Press

[85] Flanagan, M., D. Howe, *et al. Values in Design: Theory and Practice*. Information Technology and Moral Philosophy. Van den Hoven J.and Weckert J. Cambridge, Cambridge University Press

[86] Jiang, X. *Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social*. Privacy Workshop September 29, 2002, University of California, Berkeley. Berkeley, available at: http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/jiang-privacyworkshop.pdf

[87] Nissenbaum, H. *Privacy as Contextual Integrity*. Washington Law Review 79: 101-140

[88] Rip, A., T. Misa, J., *et al. Managing Technology in Society: The Approach of Constructive Technology Assessment*, Pinter Publishers

[89] Roussos, G., D. Peterson, *et al. Mobile Identity Management: An Enacted View.* International Journal of Electronic Commerce 8 (1): 81-100

[90] Art. 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

[91] Hsi, S., Fait, H., *RFID enhances visitors' museum experience at the Exploratorium*, Communications of the ACM, Vol. 48, No. 9, Assn. For Computing Machinery, New York, September 2005, pp 60 -65.

[92] Fleck, M. *et al.*, *From Informing to Remembering: Ubiquitous Systems in Interactive Museums*, IEEE Pervasive Computing, Vol.1, No. 2, IEEE Computer Society, April 2002, pp. 13-21.

[93] Engberg S., Harning M., and Damsgaard Jensen C. *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

[94] Juels A., Weis S. A. *Defining Strong Privacy for RFID,* Extended abstract in Fifth IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07), 2007 pp. 342-347. Full paper available at http://eprint.iacr.org/2006/137.pdf.