PD CEN/TR 16673:2014

BSI Standards Publication

Information technology — RFID privacy impact assessment analysis for specific sectors

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 16673:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/34, Automatic identification and data capture techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 83898 9
ICS 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 June 2014.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16673

June 2014

ICS 35.240.60

English Version

Information technology - RFID privacy impact assessment analysis for specific sectors

Technologies de l'information - Évaluation d'impact sur la vie privée des applications RFID dans des secteurs spécifiques

Informationstechnik - Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID für spezifische Sektoren

This Technical Report was approved by CEN on 20 January 2014. It has been drawn up by the Technical Committee CEN/TC 225.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (CEN/TR 16673:2014) has been prepared by Technical Committee CEN/TC 225 “AIDC Technologies”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This Technical Report is one of a series of related deliverables, which comprise mandate 436 Phase 2. The other deliverables are:

— EN 16570, *Information technology — Notification of RFID — The information sign and additional information to be provided by operators of RFID application systems*

— EN 16571, *Information technology — RFID privacy impact assessment process*

— EN 16656, *Information technology - Radio frequency identification for item management - RFID Emblem (*ISO/IEC 29160:2012*, modified)*

— CEN/TR 16684, *Information technology — Notification of RFID — Additional information to be provided by operators*

— CEN/TS 16685, *Information technology — Notification of RFID — The information sign to be displayed in areas where RFID interrogators are deployed*

— CEN/TR 16669, *Information technology — Device interface to support* ISO/IEC 18000-3 *Mode 1*

— CEN/TR 16670, *Information technology — RFID threat and vulnerability analysis*

— CEN/TR 16671, *Information technology — Authorisation of mobile phones when used as RFID interrogators*

— CEN/TR 16672, *Information technology — Privacy capability features of current RFID technologies*

— CEN/TR 16674, *Information technology — Analysis of privacy impact assessment methodologies relevant to RFID*

Introduction

In response to the growing deployment of RFID systems in Europe, the European Commission published in 2007 the Communication COM(2007) 96 ‘RFID in Europe: steps towards a policy framework’. This Communication proposed steps which needed to be taken for a wider take up of RFID whilst respecting the basic legal framework safeguarding fundamental values such as health, environment, data protection, privacy and security.

In December 2008, the European Commission addressed Mandate M/436 to CEN, CENELEC and ETSI in the field of ICT as applied to RFID systems. The Mandate M/436 was accepted by the ESOs in the first months of 2009. The Mandate addresses the data protection, privacy and information aspects of RFID, and is being executed in two phases. Phase 1, completed in May 2011, identified the work needed to produce a complete framework of future RFID standards. The Phase 1 results are contained in the ETSI Technical Report TR 187 020, which was published in May 2011.

Phase 2 is concerned with the execution of the standardisation work programme identified in the first phase.

This Technical Report is one of eleven deliverables for M/436 Phase 2. Its focus is on four major sectors that have a number of implementations of RFID that currently impact European society. Using these as detailed case studies will assist in addressing the development of the standard on the Privacy Impact Assessment. For the purpose of this work, the definitions of "RFID Operator" and "RFID Application" will be those provided in the EC RFID Recommendation of 2009-05-12.

1 Scope

The scope of this Technical Report is to use the RFID PIA Framework as the basis for exploring issues with four major sectors involved with RFID:

— libraries;

— retail;

— e-Ticketing, toll roads, fee collection, events management;

— banking and financial services.

After specific sector research and consolidation of the results of industry workshops and seminars that take place in several EU Member States, this Technical Report will identify the characteristics that need to be taken into consideration by operators of RFID systems in the example sectors. In addition it will provide advice to operators in the sector on significant variants both in terms of technology and application data. This will enable the appropriate risk factors to be taken into account.

Based on the synthesis of the applications in the chosen sectors, this Technical Report will also identify a set of factors relevant to specific RFID technologies and features that will need to be taken into account in preparing a Privacy and Data Protection Impact Assessment for many RFID applications.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE Definitions are derived from EU Recommendation C(2009) 3200 final, EU Directive 95/46/EC, ISO/IEC 19762 (all parts)

2.1
data controller
controller
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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law

2.2
data subject's consent
any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed

2.3
identified or identifiable person
person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

2.4
individual
natural person who interacts with or is otherwise involved with one or more components of an RFID application (e.g., back-end system, communications infrastructure, RFID tag), but who does not operate an RFID application or exercise one of its functions. In this respect, an individual is different from a user. An individual may not be directly involved with the functionality of the RFID application, but rather, for example, may merely possess an item that has an RFID tag

2.5

information security
preservation of the confidentiality, integrity and availability of information

2.6
monitoring
any activity carried out for the purpose of detecting, observing, copying or recording the location, movement, activities or state of an individual

2.7
personal data
any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

2.8
processing of personal data
any operation or set of operations which is performed upon personal data, whether or not by automatic data means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

2.9
data processor
processor
natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

2.10
recipient
natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients

2.11
radio frequency identification
RFID
use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it

2.12
RFID application
application that processes data through the use of tags and readers, and which is supported by a back-end system and a networked communication infrastructure

2.13
RFID application operator
RFID operator
natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an application, including controllers of personal data using an RFID application

2.14
RFID reader or writer
Reader
fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags

Note 1 to entry: The term interrogator is often used in the context of RFID item management applications, and the term 'Proximity coupling device' and ' Vicinity coupling device' in the context of card applications. They perform the same functions for any given air interface protocol.

2.15
RFID tag
RF tag
Tag
RFID device having the ability to produce a radio signal or a RFID device which re-couples, back- scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer

Note 1 to entry: The most accurate term is technically "transponder". The most common and preferred term is ‘tag’ or ‘RFID tag’ in the context of RFID item management applications and 'Proximity integrated circuit card' or 'Vicinity integrated circuit card' in the context of card applications.

2.16
third party
any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data

2.17
threat
physical, hardware, or software mechanism with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data and / or denial of service

2.18
vulnerability
weakness of an asset or group of assets that can be exploited by one or more threats

3 Symbols and abbreviations

AFI Application Family Identifier

CICO Check-In-Check-Out

CSC Card Security Code

CVC Card Verification Code

CVV Card Verification Value

DPA Data Protection Authority

EPC Electronic Product Code

ERP Enterprise Resource Planning

FMCG Fast Moving Consumer Goods

EMV Europay International, MasterCard, Visa

GDPR General Data Protection Regulation

GS1 Global Standards One

HF High Frequency (3-30 MHz)

IFMS Interoperable Fare Management Systems

IOPTA InterOperable Public Transport Applications for smart cards

ISIL International Standard Identifier for Libraries and Related Organisations

IT Information Technology

LF	Low Frequency
LMS	Library Management System
NEC	National Entitlement Card
NFC	Near Field Communication
PCI	Payment Card Industry
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
POS	Point of Sale
RF	Radio Frequency
RFID	Radio Frequency Identification
UHF	Ultra High Frequency (300 MHz – 3 GHz)
UII	Unique Item Identifier

4 Brief description of an RFID system

4.1 Infrastructure of an RFID system

RFID technology allows for the contactless transmission of data via electromagnetic fields and/or radio waves. An RFID infrastructure contains at least one RFID tag, an RFID reader or writer) and an IT backend system. In order to enable the exchange of data between the transponder and the reader, communication standards define the necessary features for the air interfaces, which have to be supported by both, transponder and reader.

4.2 Components of an RFID system

4.2.1 Transponder/Tag

The transponder or tag has a tiny computer chip which contains radio processing, data storage and data processing capabilities. This chip is attached to an antenna to create a tag. This is incorporated into a particular form factor, e. g. integrated into a self-adhesive label or into a contactless card. The information that can be stored on the tag depends on the memory and influences the speed of the data capture process. The tag generally contains a code, which points to information stored in a data base.

Depending on the application, the choice between different characteristics of tags can be made:

— Energy supply: The energy supply is not directly correlated to the communication modes. Passive tags reflect, backscatter or use the load modulation of an incoming wave from the reader in order to communicate. Active tags have their own transmitter on board to send information or answer to a reader's commands. With today's technology, the link budget requires the use of a battery for the active tags whereas for passive tags, the incoming wave can be used to supply the tag's chip with energy. Nevertheless, even for passive tags, batteries can be used to supply the tag's chip or peripherals like sensors. In that case, we speak of Battery Assisted Passive tags which communicate with the readers through backscattering or load modulation of an incident wave but use the battery to supply energy to the chip and/or embedded sensors.

— The form factor of a tag depends on the purpose of its use and the environment it is used in. Tags can be attached to or integrated into a product, and therefore appear in multiple variations. Examples of tags include, but are not limited to: hard-tags, woven- in tags, glass capsule tags, foil tags, smart labels, personal identification cards (e. g. access cards or library cards), transport cards, contactless payment cards.

— The frequency at which a tag operates is defined by its antenna and the chip design. The choice for Low Frequency (LF), High Frequency (HF) or Ultra High Frequency (UHF) depends on the application and the environment the tags are used in.

— The reading distance depends e.g. on the frequency used, the energy consumption and the environmental circumstances in which the tag is used. Thus, the read range varies from few centimetres up to several meters. The purpose of the use of an RFID application determines the read range to choose (e. g. large distance reading for inventory, short distance reading for contactless cards).

— The chip memory varies from a few bits to several hundred Kbytes, Furthermore, the distinction can be made between read only tags (information on tag stored by tag producer), write-once-read-multiple, write-and-read-multiple (reusable) tags. Contactless cards and active tags might be equipped with a microprocessor that supports the management of data files in a flexible way.

4.2.2 RFID reader or writer

Depending on the application, an RFID reader or writer activates, reads or writes information from or on a tag. It sends or receives the information to or from the tag via its antenna and processes the data on to a backend system. The reader can add information such as time of reading or its own ID to the data read from the tag and transfers it to the software in the backend system. Readers can capture data from several tags in very short time (bulk reading) when these get into its operation field.

The purpose of use of the RFID application defines the type of readers that might be used:

— Mobile readers such as handhelds (e. g. used for inventory in shops, warehouses, hospitals)

— Semi-mobile readers such as on forklifts (e. g. used in large warehouse management systems)

— Fixed readers such as gates or tunnel readers (e. g. used in goods entry or exit area of a warehouse, transit points within a warehouse, access points in public transport systems, access to buildings)

For certain applications additional security features are part of the reader. Secure readers are used e. g. for contactless payment cards or NFC applications. They are equipped with a protected key and data storage and security functions in order to support secure communication with contactless smartcards, the back office system and the key management system.

4.2.3 Backend system

The information captured from an RFID tag is transferred to and stored in the backend system. It is in the backend system where the linking of the identification number from the tag and the corresponding information is done. The information can only be processed where access is provided for the user of the system, ideally in combination with automated systems of authorisation and authentication.

Additionally, the backend system can also provide functions for card- or key management systems as an additional or required security feature of the specific application. This could be relevant in applications using contactless cards, e. g. payment cards or multi-application cards for public institutions or transport systems.

4.3 Characteristics of RFID technology compared to other data capture techniques

Where other data capture technology requires optical (1- or 2-dimensional barcodes) or physical contact (magnetic stripe) between data carrier and reader, RFID-based applications do not need this. Additionally, the possibility of reading several data carriers sequentially in a very short time with the long distance read range of one reader accelerates data capture processes considerably.

While adding or changing information on optical or physical contact data carriers would require the reproduction of the carrier, tags provide for the possibility of changing or adding information on the same data carrier. In return, this requires managing access authorisations as content on the data carrier should only be

changed when wanted respectively intended by the involved parties. Data, and where applicable additional functionalities, on the tag can support improving quality of products and services for both, application operator and consumer.

Examples of improvements through RFID technology include, but are not exhaustive:

— improved accuracy and traceability;

— improved processes in terms of speed and quality;

— reliable and automated quality control features of an object or service;

— reliable and automated anti-counterfeiting and antitheft mechanisms;

— reduction of out-of-stock situations;

— improvement services and processes with regard to speed and quality.

5 Privacy concept in RFID-based applications

5.1 Interaction between data protection, data security and privacy

The characteristics of an RFID-based application as described in 4.3 can be appreciated as benefits for the parties involved. Due to the nature of RFID not needing visual or physical contact between reader and data carrier, the technology is sometimes looked at sceptical and perceived as a threat to data protection and privacy. This results from the reading process, which is not necessarily noticed by an individual.

It is the more important to provide for transparency and ensure the safeguarding of privacy. In order to understand how privacy of the individual can be provided for, it is important to look at three aspects, the interaction of which leads to an effective privacy concept.

NOTE Transparency is to be understood in the sense Cf clauses 7 and 8 of Recommendation C(2009) 3200 final.

In order to safeguard the privacy rights of an individual, the three aspects: data protection, data security and privacy shall be taken into consideration when setting up a RFID-based application.

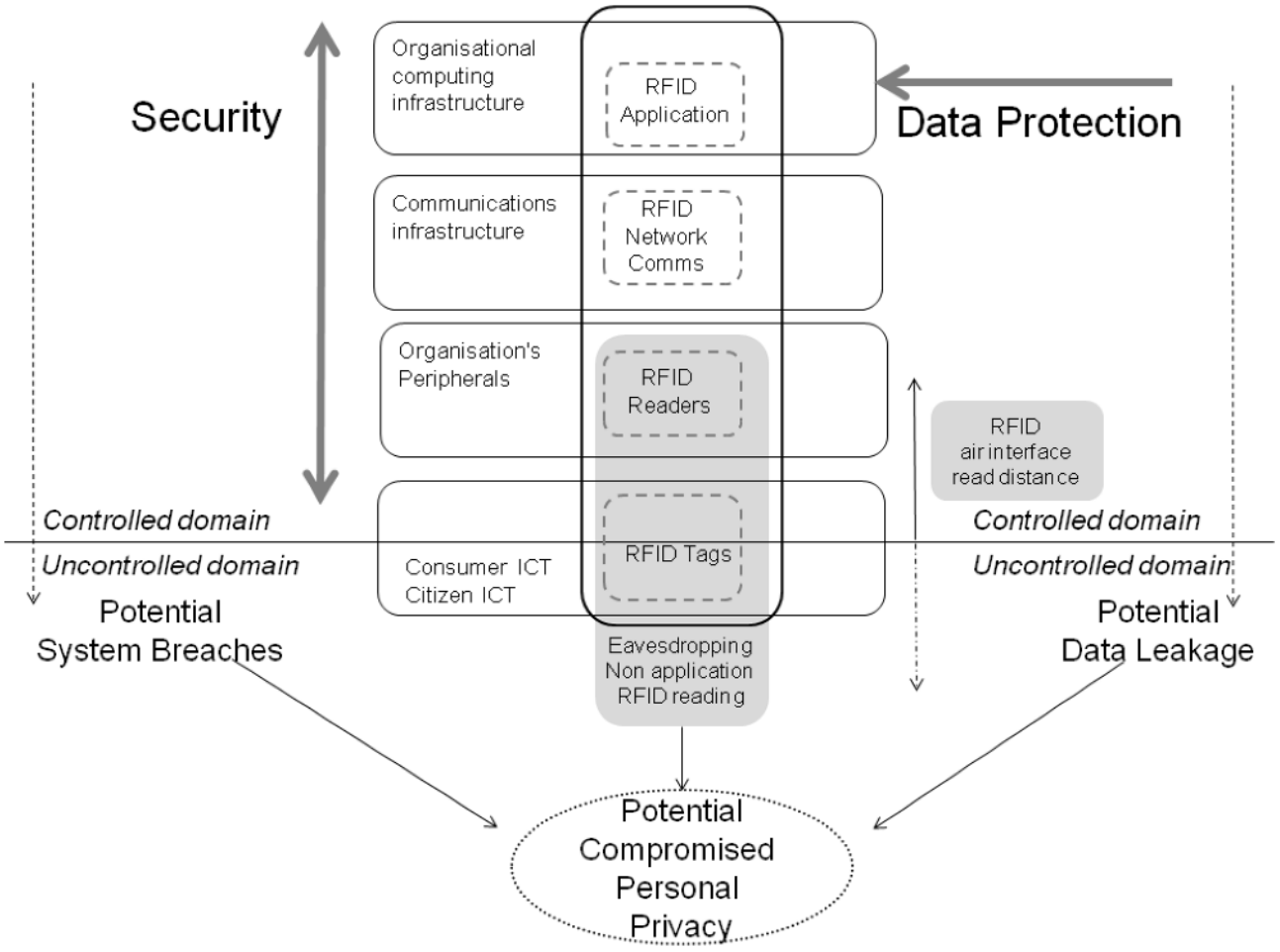

Figure 1 — Relationship of data protection, data security and privacy

Data protection comprises all processing of data such as collection of data, accuracy of data and use of data. Most importantly, it is addressed by legal requirement for compliance as set out in Directive 95/46/EC. Security of data is additionally protected by the implementation of security procedures for protection computer systems, using procedures defined e.g. in the ISO/IEC 270xx series. There is no legal requirement to implement such system, but some breaches of computer security can be the direct cause of infringement of data protection. While privacy is the individual's right to determine the use of any information about him, from an RFID perspective this presents a challenge between data protection, data security and privacy: some of the privacy risks can occur beyond the boundary of a legitimate RFID application, which does place some but not the entire responsibility on the RFID operator. With the ongoing development and spreading of RFID technology into a wider range of use there will be a need to address review of current legislation with regard to illicit use of RFID technology by individuals.

5.2 Data protection

Current legislation and probably the upcoming General Data Protection Regulation (GDPR) deal with aspects of data protection and data security. Legislators intended to cover as many areas as possible in the area of processing of personal data and thus tried to be as generic as possible. They emphasise the importance of adequate security measures, both on technological as well as on organizational level. These need to be implemented wherever personal data is processed. Adequate security measures (either technologically or organizationally) have to be implemented.

The current understanding of the upcoming GDPR is that it will take up the contents of the data protection Directive 95/46/EC: the data controller is responsible for the quality and security of the data he holds. He shall

provide for protection of personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and unintended and unlawful forms of processing. This becomes even more relevant where the processing of data also involves transmission of data to third parties via a network.

Any measures taken to provide for data protection should be appropriate with regard to the technology used, the cost and effort for implementation and the risks emerging from data processing with a given technology at given cost and probable risks.

The General Data Protection Regulation takes up the existing regulation from Directive 95/46/EC, which holds the data processor as liable as the data controller.

This part of the privacy concept refers to how (personal) data is collected and then dealt with in an organization's database, independent of the means of collection, i. e. manual or automatic data capture.

5.3 Data security

Data security is referred to as the protection of data from unauthorised - accidental or intentional - modification, destruction, loss or disclosure. In the context of this TR, data security is primarily concerned with the implementation of security risk assessment and implementation techniques that organizations adopt as a means of protecting their computer systems from external and internal threats. The objective is focussed on protecting the assets of the organization, but in doing so this does provide the protection of data from unauthorized - accidental or intentional - modification, destruction, loss or disclosure.

Various methodologies are used to assess, and therefore keep under control, the security risks to an organization. The internationally recognised reference is the ISO/IEC 270xx series of standards, although other organizations have prepared useful references.

5.4 Privacy

There are many privacy definitions available. The most used is the definition of Westin: “the claim of individuals (...) to determine for themselves when, how and to what extent information about them is communicated to others” and as a means “(...) for achieving individual goals of self-realisation.”[1] This also includes the right to determine whether and to whom personal information is to be revealed.

Privacy therefore can also be referred to as the individual's right on (informational) self-determination. One substantial aspect of this is the transparency to the individual about the use of data, including the purpose and the persons using the data. This includes the explicit consent of the individual to the processing of his data. Furthermore, the General Data Protection Regulation strengthens the individual's rights by requiring e. g. the reporting of privacy breaches to the individual, the individual's access to his own data and the possibility to control the data quality, the transferability of his data or the individual's "right to be forgotten", i. e. the deleting of data at the wish of the data subject.

5.5 General privacy risks

The more personal information about an individual that is available, the greater is the risk of harm to an individual's privacy. Such harm can go from gathering data without having explicit consent of the data subject about his behaviour to provide him with customised offers up to identity theft by malicious persons, who appropriate and use personal data in order to pretend being the individual they stole the personal information from and use this for fraud and other illegal activities.

Figure 2 shows the different areas where privacy issues might arise.

[1] Westin A.F., Privacy and Freedom, New York 1967 p. 39

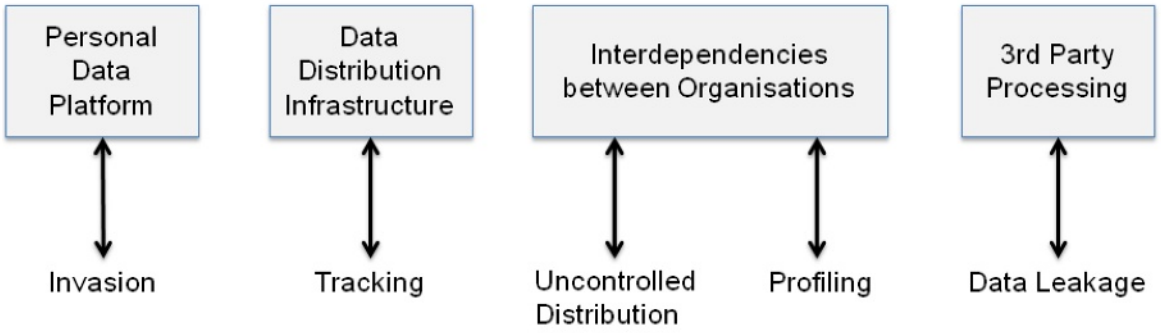

Figure 2 — Incidence of privacy issues

Figure 2 contains four columns. The first concerns applications and related devices on which data and possibly personal data are stored, from which they can be collected and/or processed. Examples of such devices could be smart cards, mobile phones, tablet computers, RFID-tagged items such as clothing and more. This is where breaches in the privacy sphere might take place for the first time in the chain of processing data. The second column relates to the infrastructure through which personal data are and distributed via public and private networks, including of course the Internet. Within this infrastructure, it becomes possible to follow the related personal data of persons. This may have been the original intention to facilitate data processing, but might also be subject to privacy breaches when used without the consent of the data subject. The third column represents the interdependencies between different organizations. Data processing is undertaken by many different types of organizations, for example private and public sector, utilities, health, voluntary. At the same time, the data processing is undertaken by many different applications such as risk analysis, logistics, insurance, law enforcement, transaction processing etc. The interrelationships between such organizations might, if not well controlled and protected, bring about uncontrolled distribution of personal data and profiling. The fourth column makes visible the potential of data leakage arising from the activities of others through, for example, click streams, other web bugs, multiple storage of the same data in different databases and use of 3rd party infrastructure services.

5.6 Challenges for a privacy concept in context with RFID

RFID technology provides a lot of benefits to its users (see 4.3), independent of the business they deal with or the role they have within a supply chain, a functional entity or other. But its characteristic of reading without needing any physical or visual contact between reader and the data carrier may cause concerns with regard to the unnoticed reading process and its possible abuse, such as e. g. unauthorised interference with the normal process of reading.

Therefore, the pursuance of data protection and data security are crucial elements to provide for privacy within the organization operating RFID-based applications. Additionally, the fact that an RFID tag as data carrier might also be read beyond the boundaries of an organization, needs attention. An RFID operator should consider at least:

— What kind of objects are tagged?

— What kind of data is on the tag?

— To what extent is the tagged object exposed in a public environment?

— Is there an impact from the data on the tag on privacy related issues?

— If so what harm could the information cause if used by unauthorised persons?

These considerations are made on a very general basis and are thus relevant for any kind of RFID application and its operators. The detailed analysis of these question though depends on the application, the parties

involved and the industry or sector the technology is used in. This TR analyses four, sectors and its specific characteristics. In the following subclauses the TR shows the necessity of different templates, depending on various aspects of each sector.

5.7 Need for transparency

The nature of risks arising from RFID applications is not fully understandable by the individual. Therefore transparency and extensive information of consumers is necessary to achieve acceptance for RFID technology. Consumers shall be put into a position to at least get a basic knowledge of the technology integrated or attached to the items or objects they buy. It is then up to the consumer to decide for or against a tag on or in the item.

The Recommendation 2009/387/EC requires for transparency by applying a common European sign to indicate that an RFID tag is present on or in the item. An additional valuable information for the consumer is the knowledge of where the tag is placed. With regard to different categories of tagged items, the placement probably provides the solution with regard to privacy aspects:

— Where the tag is in the packaging of an item, it is very likely that the tag is removed with the item packaging.

— Tags may also be attached to the item itself. When the tag is easily removable, the individual can decide whether or not he wants to remove the tag.

— Tags may be included into an item. Depending on the functionality of the tag, the consumer needs to decide whether he wants the tag to be disabled or not. This may be wanted when the tag is not part of the item function itself. However, deactivation would be counterproductive where the RFID tag is the core element of the tagged item (e. g. smart transport cards).

6 Library sector overview

6.1 Aspects of the library sector

The library sector was an early adopter of RFID, with pre-implementation discussions in the 1980s. The first implementations were in Singapore (September 1998) and Rockefeller University in New York (February 1999). An earlier implementation at a Canadian University in 1991 is also cited. Since then, the number of library implementations around the world has increased at a steady rate.

There is some uncertainty about the number of libraries using RFID technology, depending on the metrics used for counting. One measure uses a library authority, and another metric is the number of individual locations.

Thus, estimations vary from around 2500 to 5000 library sites world-wide, which use RFID technology, taking into consideration the statements of 3 major solution providers claiming to have installed RFID solutions in libraries. New sites are being implemented on a daily basis across Europe and elsewhere in the world. Both the library and RFID for libraries have reasonable futures. Although outside Europe, here are some recent developments (mentioned for their scale):

— Ottawa Public library in Canada has started a 5-year implementation programme to introduce RFID to 34 locations, with a collection of 2.3 million items.

— The Qater National Library, due to open in 2014 will house a collection of 1.2 million items in one on the largest libraries in the world.

— The University of Technology Sydney, Australia will have a sophisticated underground automated storage and retrieval system when it opens in 2016.

The vast majority of libraries around the world have been using bar code technology for circulation control, both on loan items and on the membership card for many years. Most of this operation involves library staff undertaking the loan transaction.

The conversion to RFID focuses on a self-service system for checkout and returns. From the customer's (or patron's) point of view, this reduces queuing and releases staff to provide more information to members of the library. Another, and less declared, benefit to the library is that RFID can combine circulation control with security to avoid the theft of books. Standardised and proprietary features are built into an RFID tag to make this possible. Although the primary focus is on self-service for self-issue and self-return, there have been a number of additional functions added which increase the benefits of RFID for the library and its customers. Most of these functions do not directly impact on the patron, such as the use of RFID-enabled returns sortation systems and systems for inter-library loans.

In Europe, the types of library implementing the technology include both public and academic libraries, even libraries in teaching hospitals. There are also a few implementations in higher education colleges (including the UK public school, Eton). In Australia there is a large crossover between public library services and school libraries, particularly in smaller communities. There are some unusual high profile implementations such as the Vatican library.

6.2 RFID technology overview

With respect to RFID technology, there are three separate considerations that need to be taken into account for libraries. The first is with the RFID technology used for loan items, the second is the RF technology used for any membership cards and the third being the data which can be stored on the RFID tag.

In the first category of RFID tagged items, the following technologies are used:

— 13.56MHz based on ISO/IEC 18000-3 Mode 1 (which, in turn, uses the inherent air interface protocol of ISO/IEC 15693);

— Some long-established library systems still use proprietary technology operating at 13.56MHz, although most library installations in recent years use standardised solutions;

— Within the past two or three years, there has been interest in the use of UHF technology, and a number of implementations using ISO/IEC 18000-63 tags have taken place. Within Europe, some installations have taken place in Spain and others in some of the member states that joined the European Union during, and following, the 2004 enlargement. The St Petersburg public library in Russia has nearly 100 branch libraries using UHF technology.

In RFID-enabled membership cards, the following technologies are used:

— 13.56MHz based on ISO/IEC 15693;

— 13.56MHz based on ISO/IEC 14443;

— 125 kHz using proprietary technology.

There are no standards in the library community for the encoding of membership cards. This is partly because in addition to the three RFID-enabled membership cards listed above, membership cards can be based on bar code data carriers and Wiegand technology. In addition, library cards used by local authorities are often multi-function cards provided by the local authority, so the library management has no control over the choice of technology or the data encoded on the tag. A similar situation applies to membership cards for university libraries, which can also be used for many other functions within the university.

The HF RFID tag contains the following data, which is now specified in ISO 28560; but similar data applies to proprietary schemes too:

— A permanent 64-bit unique chip identifier that is encoded in a read only part of the memory.

— An AFI that indicates that this is a library book. The AFI is registered under ISO/IEC 15961-2. If the library does not toggle between two AFI codes, then the code equivalent to the "on loan" code is used, and in this case it recommended that this is locked.

— A unique loan item code that is only unique within the library authority. This is recommended to be locked. In the UK this is one city, county, or university. In The Netherlands this is a national code.

— Additional data is encoded on an optional basis. Migration is to a flexible structure defined in ISO 28560-2, or a fixed memory structure defined in ISO 28560-3. A code - International Standard Identifier for Libraries (ISIL) - may be used to identify the library on a global basis using a code defined in ISO 15511. If encoded, the ISIL is recommended to be locked. The combination of ISIL and unique loan item provides assurance to the library that it owns the book. As such it is evidence of ownership in the case of theft.

Developments for UHF are at an early stage of development. All the current implementations use proprietary encoding rules, often paying little attention to established standards from GS1 EPCglobal and ISO. A new standard, ISO/TS 28560-4 has been approved to develop a standard solution for using the ISO/IEC 18000-63 tag. This requires a unique item identifier (UII) to be encoded. Two options are being offered:

a) The UII based on the existing library accession code (or primary item identifier). This is unique within the library domain (as is the current code used for HF tags.

b) The UII based on the ISIL plus the library accession code. This UII will make all library books uniquely identifiable and distinguishable from all other items encoded using the UHF tag.

The library community recognises the balance that it has to address. Option (a) appears to provide more privacy; option (b) provides a link to the Internet of Things, given that there is already a global repository[2)] of 1,920,476,243 bibliographic holdings.

6.3 Applications and parties involved

There are a number of different applications that a library management is introducing, but currently only two interface with the customer (or member or patron): self-service checkout and returns. In the near future customers might be provided with search facilities, but there are some technical challenges because of the closeness of books and that fact that many are displayed spine out. For simplicity, only books will be discussed, but this also applies to CD, DVD, BlueRay and other media when these are part of the self-service system.

After a collection of books has been selected, the customer takes them to a self-service check out. The borrowing procedure is as follows: the borrower is identified by scanning his or her library membership card. This card can use bar code, RFID, or smart card (using ISO/IEC 15693 or 14443 technology). The books to be loaned are placed on the reading panel. The tags in the articles are read automatically. If the membership card uses RFID or smart card technology this can be read at the same time. For security and privacy PIN numbers are often required as part of the "sign-in" procedure so that only the patron's information is displayed on the check-in / check-out kiosk screen. The membership cards sometimes have additional functions, especially if a local government or university authority is responsible for issuing the cards.

Libraries use different anti-theft mechanisms. The RFID based mechanisms are:

a) Changing the AFI code from the code for "in stock" to the code for "on loan"

b) Using a proprietary security feature on the tag that is deactivated

2) http://www.oclc.org/worldcat/statistics/default.htm and click the "watch it grow" link

c) Writing the unique chip id to a log

NOTE Recent changes to NFC specifications are now beginning to pose a threat to option (a), and increased use of standards will eventually result in option (b) being used less.

The security gates then use one of the security features to ensure that all books that leave the library have been properly loaned, and not removed by accident or stolen. Library security gate systems also use separate EAS technology at 8.2 MHz or 10.5MHz frequencies.

The customer leaves the library with the RFID tags still in a readable state; so too is any RFID or smart card membership card. At a later date, the customer returns the books that had been borrowed. In some libraries the returns, or check-in, system is very similar to the check-out system. In other libraries there is a book drop system that enables books to be returned at any time of the day or night.

Many multiple function cards are issued under the ownership of one authority, for example a city or university will offer many functions against the one membership card, although there is a requirement to enrol for the specific functions. The Scottish national entitlement card (NEC) is primarily a transport card for citizens over 60 years old and applies nationwide. However the NEC currently delivers over 30 services, using the same card, depending on which area the citizen lives. One major function is as a library membership card. It is unclear how the RFID operator can be identified, although card issuance is via the local government authority.

6.4 Privacy considerations

6.4.1 Privacy of possession

A prime function for RFID in libraries is to assist with the issuing and return of loan items with patrons. Therefore the loaned items leave the premises with RFID tags in the possession of the public. This might raise concerns about traceability of individuals via the RFID tags on books. However, this would require knowledge about the relation from the proprietary allocation of the unique loan item code as well as being able to singularise an individual to then get the connection from the loaned item to the individual and further information.

Although cited in some literature, librarians are much more concerned about RFID tags being removed to enable the loan item to be stolen. Vulnerable products are CDs and DVDs and these often require security cases and a restriction on self-checkout.

The membership cards present a slightly higher privacy risk, which can be mitigated by minimising the personal data held on the tag, using RFID technologies with reduced read range, and potentially encryption on the more sophisticated cards. Given the different technologies available for these cards, the different card issuers, the difference between single function and multi-function use, and the lack of standards for the encoded data, the extent of privacy risk is highly variable between libraries.

6.4.2 Privacy of personal data in the central system

The central database is generally known as the library management system (LMS). It provides functions such as procurement, bibliographic record compilation and interlibrary loans that are completely separate from the front-end circulation system. There are very few vendors that offer both products, because of the way that the market has evolved. There are about three different protocols used to communicate between the front end RFID (and bar code) circulation kiosk and the LMS. Currently the vulnerability of a privacy leak in this interface is reasonably low simply because of the operational frustration experienced by library management and RFID vendors in getting improvements in the LMS. The majority of LMS vendors are based in the USA, and have seemed slow to respond to requirements for RFID. Open source LMS systems exist giving libraries more control, but seem to be much more popular in North America, Australia and New Zealand. From an operational perspective they provide libraries with greater freedom; but do have the prospective for enhancing privacy.

Like any backend system, the LMS is vulnerable to data protection breaches. The fact that there is no indication to the public what LMS system is operating makes it difficult to attack via the RFID front-end, especially if membership cards need to be supported by a PIN to access the individual's records. Hackers would need to be aware of which of over 25 LMS systems is operating in a library. The bigger risk – and it falls within the scope of security and data protection – is of an "insider" breach.

6.4.3 The impact of NFC-enabled phones

In recent months, it appears to be the case that NFC phones have extended their capability beyond ISO/IEC 14443 to now cover ISO/IEC 15693 protocol. This means that any tags that are using standardised HF technology in libraries will increasingly be susceptible to being read by NFC-enabled phones which will increase the vulnerability of an individual's privacy if library loan items and particularly library membership cards can be read. As the current technology has very little protection for security and privacy, the risks of illicit data capture could increase over the coming years. Libraries themselves need to be concerned about privacy and denial of service, because some of the smart phone devices are as equally capable of writing data to the tag. This presents a greater risk to the library in terms of a denial of service of any tags that are modified. However, there is also a potential risk of being able to clone membership cards and therefore assign loan items to the cloned membership card with the intention of not returning them.

One countermeasure that could help alleviate the problems is for a more widespread introduction of the ISO/IEC 18000-3 Mode 3 tags, which have the potential to incorporate security and privacy features. The Technical Specification (part of M436 / 2 deliverables) for a device interface to support this protocol and ISO/IEC 18000-3 Mode 1 would enable a planned migration to a more secure technology.

6.5 Prospects for PIA templates

At one level the library community is organized in such a way that information can be shared between organizations. Libraries do not really compete with each other. A problem is organizing activities at the correct level. The international level, through ISO TC 46 SC4 works well for global issues, but not all countries have the same issues as Europe about privacy. There are no significant organizations at a pan-European level, but a number that operate nationally.

Vendors of RFID systems for libraries and for the LMS vary from a narrow single or few national markets, to truly international players. The prospects of RFID system vendors and LMS vendors collaborating on privacy, when they do not do so for more basic operational needs, is low.

Libraries should be interested, but until recently have depended on the vendor community, which offers turn key project solutions. Libraries purchase systems on brand, reputation, price and service. It is easier to purchase a "package" than for the library to select products that are best in class for a particular function. Interoperability is only beginning now that standards are in place and some libraries are beginning to explore multiple vendor projects. Until this is more widespread, most libraries will not have the technical knowledge to assess RFID and RFID privacy.

In contrast to this negative picture, the following features suggest that a sector-based template(s) can be developed for and might be supportive with regard to privacy aspects to the library sector:

— The new ISO standards for data encoding provide a common platform to explore other features. Already new protocols are being explored to overcome the limitations of the protocols between the RFID front-end and the LMS back-end functions.

— Most libraries are owned by governments of one level or another or by universities. So being responsible stakeholders is fairly common.

— The NFC threat offers an opportunity to address system security and privacy as two sides of the same coin.

— Although there is no pan-European platform for collaboration, mutual sharing of information is possible between national bodies, and by vendors.

— Competition between vendors, resulted in all the larger companies committing to support the new data encoding standards when these were published in 2011. Something similar could happen with a PIA.

Challenges still exist about how the PIA would address the multiplicity of membership card features. HF and UHF need to be addressed separately, with the HF-based PIA being addressed around established implementations. There should be opportunities to address the UHF-based PIA around the new ISO standard: ISO/TS 28560-4.

7 Retail sector overview

7.1 Aspects of the retail sector

Current technology used in the retail sector is bar code scanning. The fundamental difference for industry between bar code identifiers and RFID identifiers in the retail sector is the difference in the cost of source-marking. For bar code, the cost of source-marking involves the redesign of packaging to incorporate a bar code; thereafter, the cost for each individual bar code is so low as to be almost negligible. In contrast, each RFID tagged item has to bear the cost of the RFID tag and its application. When using rather complex tags (e.g. GS1 EPC Class 1 Gen 2 according to ISO/IEC 18000-63) the cost is such that it adds a few Euro Cents to the cost of each item. Therefore a use of RFID technology with low cost items at the time of writing this TR is not realistic to be applied on medium-term.

The retail sector cannot be looked at as one single sector for which RFID applications are used with the same purpose. The diversity of the retail sector as well as a variety of aspects have to be taken into consideration.

Classification of products can be done according to diverse aspects such as: price (low, high), life cycle (short, long), environment of use (private, public), functionality of the tag (identification, part of functionality), placement of the tag. With regard to privacy and data protection aspects, often more than one criteria have to be looked at. Some examples are listed below, whereas this list is not complete and only shows an extract of the criteria that need to be considered:

— Products with short life cycle, low cost, products which generally are not carried around by persons but brought from store to home, e. g. Fast Moving Consumer Goods (FMCG). These products are taken from store to home and consumed there. Sometimes, they do not even reach a certain destination, they are consumed right after purchase, e. g. beverages. The time of exposure of the tag in a public environment is rather short.

— Products with a long life cycle, higher priced, brought home from the store and not carried around by consumers e. g. electronic equipment such as televisions or washing machines. Tags on such products can have additional function for after sales services such as warranty handling or maintenance. The time of exposure of the tag in a public environment is rather short.

— Products that are generally carried around by people (such as apparel and textile, mobile phones, consumer electronics). Depending on the category of products the functionality of the tag is a crucial element to consider with regard to privacy aspects. The time of exposure of the tag in a public environment can differ, but as these products are regularly carried by an individual, exposure should be classified as long.

— Products where the tag is part of the product and/or provides security aspects such as protection against counterfeiting or monitoring of the product quality, e. g. expiry date on health care products. The time of exposure to public environment may differ depending on the product.

Another important aspect is the placement of the RFID tag on the object. There are different possibilities of placing, which depend on:

— the tag's functionality: object identification, additional functions for the tagged object (e. g. sensor assisted temperature or expiry date control), use for after sales services

— process of applying the tag to the object

— intended reading environment (warehouse logistics, shop logistics, cash register or POS, after sales functionalities)

— level of product hierarchy to which the tag is attached (pallet, case, single item)

Taking these aspects into consideration, the decision will be made whether the RFID tag is integrated into or attached to the product or its packaging. Implementation of RFID technology continuously grows. Nevertheless, implementations in rather higher priced product ranges will be faster than in the FMCG sector. Even if ordered in high volumes, production cost of RFID tags suitable for the above described fields of application still move in price ranges which do not allow to equip low cost products (e. g. yoghurt cups) in the near future with RFID tags.

At the time of writing this TR broadest implementation in the retail sector with the available technology and the benefits of RFID are to be found in the garment and textile sector.

7.2 RFID Technology Overview

As stated above, the largest expected platform for RFID in the retail sector will be based on GS1 EPCglobal standards. However, there will be users of AIDC technology who may choose to use proprietary systems.

The current contender technologies used in retail are:

— UHF technology based on ISO/IEC 18000-63 (previously 6 Type) (GS1 EPC Class 1 Gen 2).

— Possibility of the use of ISO/IEC 18000-3 Mode 3 (GS1 EPC Class 1 HF) operating at 13,56 MHz.

— Closed system retail applications e.g. for retails with a predominant own label product range which can choose a standardised technology but use an in-house product coding scheme. Possible technologies include: ISO/IEC 18000-3 Mode 1, ISO/IEC 18000-62 (previously 6 Type B), and ISO/IEC 18000-64 (previously 6 Type D).

— The use of any proprietary technology, probably operation at HF (13,56 MHz) or UHF (860 to 960 MHz), also in a closed retail system.

7.3 Applications and parties involved

7.3.1 General

The retail sector consists of several steps in the supply chain, starting from the supply of raw material, production and/or assembling, over logistic processes such as stock management, dispatch, order management and product availability up to the selling of products at the point of sale (POS), either in the stationary or online retail shop.

7.3.2 Use of RFID in retail logistics

Processes in production, assembling, order and stock management or dispatch require a high level of quality, as the producer wants to provide good product quality, safety of a product and right delivery at the right time. At the same time companies are interested in avoiding additional cost caused by manual processes. Manual handling and thus involvement of human beings, depending on the complexity of processes, can be extremely work intensive and time-consuming as well as susceptible to errors. RFID technology can provide considerable benefits in such processes. It can enhance speed and quality at the same time. This applies to

internal processes (e. g. RFID-based stock-taking) as well as to processes with external players such as suppliers, service providers or customers (e. g. RFID-based receipt of goods).

Independent of where the tags are attached (shipping unit, packaging unit or single item), the individual as a consumer does not get in to contact with the technology in the logistic context (shipping, stock-taking, picking of goods, goods receipt, stock transfer, filling of shelves in the shop). However, RFID applications in the logistic context can also be used to help prevent theft of high-priced products, control of optimal stock conditions in terms of climatic conditions or control of piecework and therefore have a relevance to the individual in his position as an employee.

The parties using the information from the RFID tag need this to trace their shipments, control their stock and enhance these processes by efficient means of automatic data capture techniques. They read the encoded number, e. g. Electronic Product Code (EPC) from the tag which is then forwarded via air interfaces to the backend system. It is only with access to the backend system or a central product database that the identification number can be put into context with the tagged object.

The interaction between the different players in the supply chain is important for its optimal functioning, both regarding the flow of goods as well as the data flow. RFID technology in combination with data standards (e. g. GS1 EPCglobal Standards) can improve the supply chain by enhancing quality, speed and transparency. In return, agreements on accessibility of data and rights for processing data need to be fixed and regarded from all partners in the supply chain. Usually, the supply chain partners are also the RFID application operators as defined by the EU Recommendation 2009/387/EC.

7.3.3 The role of the solution provider

Solution providers and/or system integrators offer their services and/or products to the application operators. They provide the infrastructure for the RFID application, including data flows, according to their customers' needs. Setting up an application and/or integrating this into an Enterprise Resource Planning (ERP) system they should consider possible technical features of the RFID system, which can help designing the system in a way that it is compliant to requirements of data protection and privacy. The so-called "privacy by design" approach can support both, the data security related as well as the organizational aspects of an RFID system.

7.3.4 Impact of RFID technology for the consumer

The consumer who buys goods in a shop represents the end of the supply chain. Current single items which pass the POS are barcoded for quick check-out processes. At the time of writing this TR also customer loyalty programs are most commonly based on bar-coded loyalty cards.

Despite developments in recent years RFID technology today is far from being as widespread as barcode technology. Current use on the basis of single item identification can be found in the rather high-priced product categories. More and more implementations can be found in the garment and fashion retail environment where the benefits of the RFID technology support logistic processes, stock management, inventory and replenishment, which are special due to the diversity of the products offered to the customer. Another reason is that the cost of RFID tags is only marginally more than pure EAS tags; and with the right system design the EAS functionality can be built into to contribute to anti0theft control.

RFID technology not only supports the retail company with efficient handling and management, but also the individual profits by the advantages as described in 4.3. From the individual's point of view, benefits can be:

— Improvement of optimal shelf availability and/or helping to avoid out-of-stock situations makes products available when looked for by the consumer.

— Supporting anti-counterfeiting helps the seller to maintain the image of his brand whereas the consumer can rely on his preferred brand to be genuine and keep the promises made for the product.

— Supporting intelligent shop systems by RFID technology. This helps the seller to improve his service towards the customers and the consumer to better find the products or special product offers he is looking for.

— Improving after-sales services, e. g. paperless handling of warranty, maintenance, goods return or replacement etc.

7.4 Privacy considerations

Concerns about threats to an individual's privacy mostly come from the circumstance of not necessarily noticing the reading process when RFID technology is used. As for retail applications, UHF is the common frequency used, which enables reading from distances up to several metres. This might increase concerns about malicious use of the technology. As RFID identifiable items leaving the premises of a retailer in the possession of consumers and members of the public, this brings with it concerns about eventual tracking and tracing via tagged items, especially if these items relate to sensitive details such as personal bodily details, e. g. medicine relating to serious diseases.

However, RFID is a complex technology and there are many aspects to take into consideration to give a complete picture of eventual threats and appropriate mitigation measures.

The intended function of tag can differ from mere identification of a product over use for supporting quality control, easier product maintenance or warranty handling up to being a part of the product as a component of the product's functionality. In connection with this the tag placement will differ as well. Where it contains functional elements of the product the tag might well be included into the product. This might be different for a tag containing product identification which might be placed on the packaging and would be discarded at the use of the product. Therefore the functionality of a tag and its placement are bound with the possibility of removing a tag from the product it is attached to.

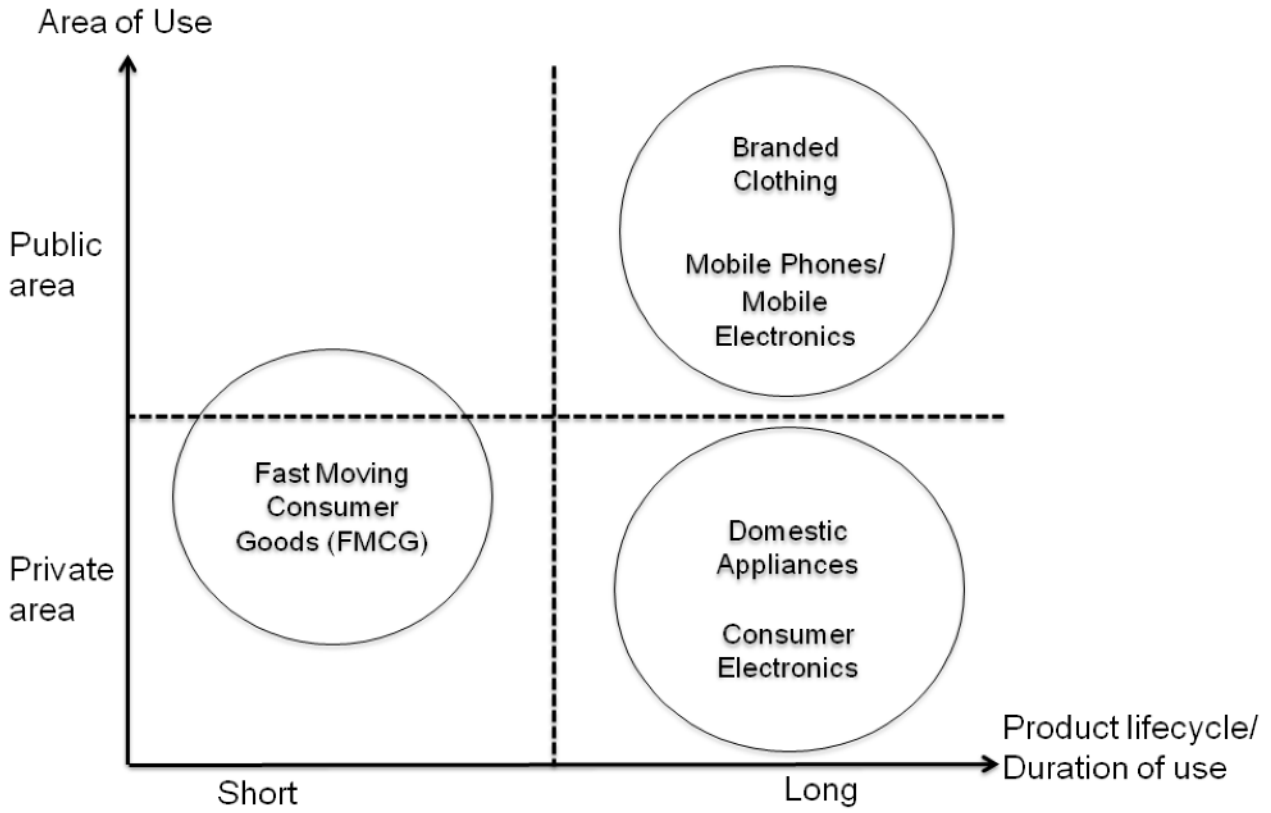

Figure 3 — Products categorised according to their area of use and their lifecycle

Figure 3 shows different categories of products with regard to where they are typically used and how long the duration of use is. This is directly related to the exposure of a tag to an environment outside the boundaries of the application operator. Goods with a short product life cycle used in the private area are very little likely to harm privacy whereas products carried by an individual also in the public area are more likely to be subject to privacy attacks.

Finally the data on the tag and its ability to be linked to an individual needs to be considered. According to Directive. 95/46/EC any information relating to an identified or identifiable person (data subject) is personal data. And an identifiable person is defined as a "person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". The upcoming GDPR however defines an identifiable individual as "... a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors..." The decisive term is "reasonably likely". Whether an identifier should be supposed to be regarded as "personal information" depends on the entire situation and includes the application operator, intended purpose of the application, nature of the tagged object, data encoded on the RFID tag and the data subject or individual. With RFID technology another aspect is important: when a number of tags are present in the possession of a number of individuals within read range then a read or eavesdropping activity cannot be sure which individual possesses which tag. Therefore, an individual can only be traced when it can be separated from others.

The great variety of levels within the retail supply chain as well as the diversity of products to be found at today's POS requires detailed analysis of the different categories of products. This is why PIA cannot be done on a generic level but should refer to a sector or may even need to be more detailed than this.

7.5 Technological prospects for privacy enhancements

A new generation of ISO/IEC 18000-63 tags is currently being standardised by ISO and GS1 EPCglobal with a more sophisticated air interface protocol. Tags and readers that are conformant with the new protocol will be available in the coming years. There will a number of additional optional features in this new generation that will provide support for enhanced privacy ("privacy by design" approach). However, RFID application operators need to be aware of the fact, that these additional features are supported in new technology (readers, tags), but that for other tags circulating different approaches to provide for data protection and privacy might apply.

8 Transport sector overview

8.1 Aspects of the transport sector

In order to use public transport a passenger requires an entitlement, otherwise known as a ticket. Such entitlements are traditionally issued to passengers in the form of paper tickets which the passenger may have to validate (stamps) before beginning of the journey, and which may be checked by an inspector in the vehicle or on the platform.

In many parts of the world electro-mechanical access equipment has been introduced in public transport. In such applications, access to the platform through gates or other access barriers requires the presentation of a valid entitlement. Simple techniques were used at first such as tokens (e.g. New York) and magnetic stripe cards (Singapore, London).

Nowadays, many of these initial implementations in public transport have been replaced by contactless proximity chip technology. Other important references have emerged such as London, Copenhagen, Peking, Seoul, Moscow, Paris, Warsaw and Oslo. The contactless chip technology available today can provide for reliable, powerful and cost-efficient solution for mass applications in public transport.

Currently, almost all large-scale international implementations in public transport utilise relatively inexpensive chip cards with simple contactless memory chips. Many of these projects are the sole responsibility of a single transport company. If more than one transport company is involved, then there is a contractually regulated relationship between the providers, and on that basis there is an organizational collaboration governing in detail aspects such as products, fares and clearing.

The increasing use of NFC-enabled mobile devices on one hand introduces new form factors different from the standard smart card and on the other hand offers enhanced options to combine different applications in one NFC mobile device.

The last generation of implementations are the so-called Interoperable Fare Management Systems (IFMS). These intend to improve the attractiveness of public transport for the customer by introducing features such as interoperable customer medium for the use with any participating transport company or automatic fare calculation on the basis of the transport services used. Additionally, they strengthen the transport industry by counteracting counterfeit fraud, helping to apportion revenues among the participating companies or increasing competition by creating an interoperable service platform offering the companies flexibility in their fare policies.

8.2 RFID Technology Overview

At the time of writing this TR, most RFID-based applications in the public transport sector use the international air interface standard ISO/IEC 14443. This standard is applicable to various types of chips, such as low-cost memory chips, secure memory chips or others with additional features.

Furthermore, several categories of carrier media, also referred to as customer media can be identified:

— Contactless smart ticket, which is a multi-layered paper ticket with conventional memory chip with contactless proximity interface as defined in ISO/IEC 14443

— Contactless secure chip card with a secure, flexible memory chip with contactless proximity air interface as defined in ISO/IEC 14443

— Contactless secure multi-application card, with a secure controller chip with a programmable operating system and application software with contactless proximity air interface as defined in ISO/IEC 14443

— Secure NFC mobile device.

IFMS implementations as described in 8.1 are based on three standards:

— The functional system architecture and the application scenarios of IFM systems are described in EN ISO 24014-1.

— The EN 1545 standard describes the data elements and EN 15320 describes the data structuring (IOPTA, InterOperable Public Transport Application).

Furthermore, there are some proprietary e-ticketing concepts. BeIn-BeOut systems e.g. employ proprietary wireless technology for the communication between an active user medium (having its own energy source) and the on-board systems (acceptance terminals) to automatically detect the presence of users without them having to consciously trigger a capture process. Some other ticketing schemes are based on the EMV standard.

8.3 Applications and parties involved

8.3.1 General

This clause focuses on current applications, types of tickets (including entitlements) and sales processes as they are in use in public transport in Europe at the time of writing this TR. However, emphasis will be placed on the check-in/check-out (CICO) variant since this is the most highly developed, powerful and flexible of the InterOperable Public Transport Applications for smart cards (IOPTA) application scenarios. In a CICO-system passengers actively register with the system at the start and at the end of the journey by using their electronic customer media.

8.3.2 Types of tickets, features and characteristics

Customers are provided with services by public transport companies, and the following kinds of tickets or entitlements are offered in that relation:

— Electronic ticket valid for a defined time (day, month, year) and network (regional, over-regional, long distance).

— Multi-journey entitlements.

— Upgrading with additional entitlements.

— Subscription entitlements (e.g. a so-called automatic fare entitlement for use in a CiCo system or an electronic ticket subscription contract).

These types of entitlements differ in various features and characteristics:

A distinction is made between interoperable or non-interoperable usage, whereas interoperability is defined as the acceptance of an entitlement/product (acceptance terminal interfaces have to be standardised), its

calculation of the use of services and apportioning of revenues between two or more public transport companies. From the customer's point of view interoperability means that they can use their media and entitlements to travel with different service providers.

Increasingly, public transport companies are accepting contactless payment cards from other providers.

The value of the entitlement depends on the validity of a defined time frame and zone in which the entitlement is used and the type of service that can be obtained by the entitlement. Values can vary between about one Euro and several thousand Euro.

The criteria about tickets being transferable personalised, non-transferable personalised or anonymous has an impact on the privacy issues of such an entitlement. In some cases, these aspects can correlate with the type of ticket and/ or from the chosen sales channel.

Validity in terms of time and region / non-regulated entitlements.

Finally, there are different ways of how the fare calculation is done and how it is charged to the customer.

8.3.3 Characteristics of automatic fare calculation

All automatic fare calculation requires a check-in at the start of the journey and a check-out at the end, and this in turn requires a CICO (check-in/check-out) infrastructure. The transactions generated in the process serve as conformation for billing systems that use access barriers and can use these for checking in and out. In systems without access barriers, a CICO infrastructure comprising check-in and check-out terminals shall be installed on the platforms and in the vehicles of public transport, such as trains, trams, busses and similar.

In case the customer medium is also an active device, e.g. a mobile telephone, the CICO infrastructure supplied by the public transport operator may consist of passive tags. Another possibility is that position information are captured with the help of the active device, e.g. GPS, and used to generate check-in and check-out transactions.

The automatic fare entitlement defines the general conditions for use of the service, the calculation of prices and the method of billing and payment. Aside from its use in CiCo systems the automatic fare entitlement can be used as a method of payment for public transport services (e.g. for the payment of electronic tickets).

There are three forms of automatic fare entitlement as payment method:

A postpaid entitlement is billed by the issuing retailer for a service after it has been used. This requires the customer to register with a method of payment (e.g. bank account, credit card) before using the service.

The procedure of prepaid entitlements is essentially the same as for a postpaid entitlement except that a certain amount is paid by the customer in advance (e.g. by direct debit of the customer's account).

When a prepaid amount is loaded on the user medium and reduced accordingly during usage the services is called stored value entitlement. This payment method can be anonymous.

8.3.4 Sales channels and their impact on the products

8.3.4.1 General

The products for public transport can be provided either directly by the product provider (e. g. customer service centres, local point of sale, internet) or by retailers (e. g. travel agencies, hotels, internet). With both suppliers, the customer has several means to buy the entitlements needed.

8.3.4.2 Sale by personnel

Sales through customer service centres, local points of sale, conductors or drivers require a direct interaction between the customer and the personnel of the product provider. The personnel can identify the customer (e.g. by checking the customer's identity card). Several payment methods may be used in a flexible way.

Initialising customer media requires online access to the relevant background systems and the availability of the necessary equipment on site. For this reason at the time of writing this TR, customer media are often ordered at customer service centres and points of sale and then delivered by post. Alternatively, the finished customer medium can be picked up at a customer service centre. Loading entitlements onto existing personalised and non-personalised media requires direct communication between the customer medium and the sales system via a suitable reader. This is currently supported in customer service centres and local points of sales for personalised and non-personalised products.

In the future there will be methods for loading applications and personalising in customer service centres and also via the Internet using home readers, and over-the-air using NFC mobile devices.

8.3.4.3 Sale by fixed and mobile vending machines

Vending machines are nowadays very widespread. There are fixed installations in railway stations or at bus stops as well as mobile readers used in vehicles.

Fixed vending machines can be connected to sales and management systems via an online link. This means that vending machines could even be used to initialise and personalise customer media. In contrast sustained online links are not generally available in vehicles.

Currently customers do not have the option of performing a personal registration at vending machines, since a reliable means of identification does not exist. This also means that customer accounts cannot be set up and personalised media cannot be applied for.

For this reason vending machines only sell products anonymously at present. Loading entitlements onto existing customer media is technically possible if the vending machine is equipped with an appropriate reader and SAM.

Soon customers will be able to enjoy secure, convenient methods of identification and authentication using – for example – electronic identity cards. This can also enable registration at vending machines.

8.3.4.4 Sale by internet

The customer submits personal details, the order, and payment information to a service centre via the Internet (web page). The availability of the product and, where applicable, seat reservations can normally be dealt with straight away when ordering on the Internet. Payment is by credit card, direct debit or other established means of payment. Products and customer media are delivered by post or can be made available for pick up at a customer service centre.

Personal information (e.g. address) submitted through a web page cannot generally be considered trustworthy. Checking this information reliably involves considerable extra effort. Normally it is checked solely against a current address database and a credit check is performed.

In the future there may be other ways for customers to register and place orders by internet using card readers/ over-the-air and secure proof of identity (e.g. by an eID).

It will involve the customer submitting the order and payment information to a service centre via the Internet (web page). Personal data relating to the customer (where necessary) will be identified and transmitted online by means of direct communication between the ticket issuer's application server and a secure identity card (electronic identity card, eID).

The availability of the product and, where applicable, seat reservations can normally be dealt with straight away when ordering on the Internet. Payment is by credit card, direct debit or other established means of

payment. Products and customer media are delivered by post or can be made available for pick up (at a customer service centre, point of sales or vending machine).

The personal information received by communicating with the eID are to be considered trustworthy and reliable. Additional checking is not required.

Anonymous use of public transport can also be offered via this sales channel, in which case an anonymous medium is used and a non-personalised entitlement loaded onto it. The service is paid for by means of credits stored on the medium. These credits can be purchased through the sales infrastructure using anonymous payment methods.

8.4 Privacy considerations

As described in 7.3 there are various possibilities to use electronic tickets or entitlements.

Where personalised tickets or entitlements are sold, public transport system implementations are normally processing personal data and consequently have to obey to corresponding national or European legislation for data protection (e. g. Dir. 95/46/EC), independent of the technology used. Anonymous tickets are not in the same extend exposed to privacy risks as these types of tickets are not directly related to a person. However, safety features should be provided to avoid illicit reading and theft of the financial value of such tickets.

Current RFID-applications used in public transport are based on proximity RFID-technology using personal contactless media (contactless cards, mobile devices). As personalised contactless transport cards contain personal information, they need to be supplied with appropriate security figures such as encryption and authorisation mechanisms for reading. Relevant threats related to the use of RFID in public transport can be encountered by appropriate safeguards within the system. However, additional advice should be provided to consumers how they can additionally protect the card physically from unauthorised access.

Additional assets to be protected and privacy targets are very much depending on the particular system setup concerning products, control schemes and sales processes. Individual assessments involving data protection officials and other stakeholders proved to be the best practice. The following example shows typical privacy targets and assets that need to be covered by dedicated measures:

1) Protection of personal data that is generated by the CICO process;

2) Protection against illicit access, manipulation of personal data on the customer media or the backend systems;

3) Protection against cloning of customer media.

There are two aspects to be considered: On the one hand, the strength of the safeguards which have to be put in place depends on the financial value of the assets to be protected. E.g. a season ticket with a value of > 3000€ requires a high security customer media that provides strong access control, protection against eavesdropping and other attacks. On the other hand, the personal information stored on public transport cards always has to be protected by strong safeguards. Advice should be provided to consumers how they can additionally protect the card physically from unauthorised access.

8.5 Other applications not covered in detail

8.5.1 General

This clause has a narrower focus than that defined in the scope. The RFID-related issues concerning e-ticketing are by far the more significant, because of the numbers of citizens that are impacted. Therefore this is the focus of the clause of the TR.

8.5.2 Toll roads and fee collection using RFID

Toll roads and fee collection associated with RFID generally require a number of features that have a lesser impact on privacy, as follows:

Tolling involves communication from a passive or active tag to a reader. The reader is located at generally six meters high (about the height of a highway overhead sign). Tags shall communicate at an angle up to the reader and at speed (~80-150 km/h).

Due to the geometry, any illegal eavesdropping of the communication at speed is difficult.

However, it might be possible to read some tags illicitly, when the vehicle is stationary.

Identifier(s) exchanged are application specific; they do not link to any services other than fee collection and cannot be used in other means or in other contexts. Access to data stored on the tag, in accordance to the applicable standards, may be protected against unauthorised access by cryptographic means. Information associated with the account holder is stored only in secure back-office systems.

8.5.3 Event management using RFID

Event management using RFID is in its very beginnings of development with proprietary solutions, different RFID air interface protocols being used and a truly transient nature of data capture associated with the specific event. There are generally two main applications within event ticketing.

— One application is for simple access control, e.g. to a sports event, where the prime purpose is to prove that the RFID enabled ticket is valid and to define access zones.

— The other application is for exhibitions where visitors are equipped with an RFID tag or badge, which can be read to capture data about the individual. This information can then be used to provide customised offers to visitors depending on the price of their ticket and/or forwarded for information to the exhibitors, providing that the individual has given his consent for the latter.

Both these types of application (toll roads and event management) do need to be the subject of a PIA process, but are, due to constraints with regard to time and manpower, not further analysed in this TR.

9 Banking and financial services sector overview

9.1 Aspects of the finance sector

This Technical Report focuses on the financial sector using RFID as it has been defined by the European Commission. Therefore contactless payment cards are the main topic that is dealt with in Clause 9.

Current methods for effecting payments are various. The European Payments Council has recorded that although there is a significant growth in cashless payment methods in Europe, cash payments are still the predominant payment method in Europe. However, the trend towards cashless payment - especially the use of payment cards - is going to continue, combined with increases in electronic and automated processing of payments more generally. The use of internet banking and internet shopping has also increased considerably, allowing payers to make payments regardless of location or time and using payment cards as means of remote transactions (card-not-present).

At the time of writing this TR, the methods of cashless payment defined as general-purpose instruments are:

a) Credit transfers are instructions sent by a payer to its bank requesting that a defined amount of funds be transferred to the account of a payee. Credit transfers may be submitted to the payer’s bank in either paper or electronic form, but as a rule further processing occurs in electronic form.

b) Direct debits are payment instruments authorising the debiting of the payer’s bank account. These are initiated by the payee on the basis of authorisation given by the payer.

c) A cheque is a written order from one party (the drawer) to another (the drawee; normally a credit institution) requiring the drawee to pay a specified sum on demand to the drawer or a third party specified by the drawer. However, as a paper-based instrument, cheques are the most costly non-cash payment instrument to process and settle. As a result, payment service providers are seeking ways of promoting the use of other cashless payment instruments, particularly card payments.

d) Debit cards are linked to a bank account and allow cardholders to charge purchases or ATM withdrawals directly and individually to this account. Consequently, when a cardholder uses a debit card, the amount is typically debited from the account either immediately or within a few days and there is no postponement of payment. Debit cards are also referred to as bank or cheque cards.

e) Credit cards provide cardholders with a credit facility and the possibility of delaying payment. The size and duration of the credit facility are the subject of an agreement between the cardholder and the card issuer. Another type of credit cards are those cards that behave as debit cards, where the cardholders account is directly debited. Both types are used in relation with the 16-digit card number to effect payment.

This Technical Report focuses on cashless payment methods that require the use of a payment card described in (d) and (e). Various technologies are used to achieve a payment transaction between the card holder and the product or service provider:

a) Magnetic stripe (mag stripe) payment cards contain a magnetic stripe on the back on which the information on the card holder and the card itself (number, validity date) is stored. When being read, the magstripe card is swiped through the reader, the processing of the data happens later. Signatures are often required as additional verification.

b) Payments cards with a microchip on their card face contain or generate the data required for transaction routing and card authentication (e.g. Primary Account Number (PAN), Application Cryptogram). Compared to mag stripe cards, they are more secure in terms of storing and processing data. Chip cards need to remain in contact inserted into the reader during the payment process. Many transactions require the use of a cardholder verification method, such as Personal Identification Number (PIN), commonly used for debit, or signature to verify the cardholder, commonly used for credit within Europe.

c) Cashless payments can be effected by contactless payment cards which use RF communication protocols or a smart phone with integrated NFC technology. Compared to the contact payment methods mentioned before, RFID minimises the time needed for reading the card. No PIN or signature is required for low value transactions by the merchant. Above a certain threshold, PIN is required. For high value transactions smart phones may require the use of personal codes entered on the phone.

d) "Virtual" payment transactions on the Internet or over the telephone, also known as "card not present payments" where the card details are provided, but where a physical transaction between the merchant (supplier) cannot use a physical card reading device. For added protection against fraud a 3-digit code on the back of the card in the signature block is generally, but not always required. This code is known by various names: card verification code (CVC), card security code (CSC), card verification value (CVV), and other variant names. Services such as those based on the 3D-Secure protocol are commonly used for cardholder verification.

Although the prime subject of this TR is contactless payment using RF communication protocols as described in this section under c), there is relevance in also taking the other technologies into account.

9.2 RFID Technology Overview

9.2.1 General

The current RFID technologies used for contactless payment systems can be divided into two major categories: contactless payment cards and NFC based payment by mobile phones, the characteristics of which are explained hereafter.

9.2.2 Contactless payment cards

Contactless payment cards use secure microprocessors, flexible chip memory and use the contactless proximity air interface as defined by ISO/IEC 14443, using high frequency with only very limited read range. Contactless payment cards have the ability, once in a secure state, to perform cryptographic processing and generate fresh dynamic authentication values for each transaction:

— Contactless secure chip card;

— Contactless secure multi-application card.

9.2.3 NFC based payment by mobile phones

Mobile devices such as smart phones can be used to effect contactless payments in different ways, taking either the functionality of an RFID tag (passive mode) or of an RFID reader (active mode). Using a mobile phone as a proximity and vicinity device requires active involvement of the owner of the device. For the purpose of this TR however, the focus will be on mobile devices taking the functionality of a tag (passive mode).

When mobile devices are supposed to act like an RFID tag, they are based on NFC technology, which again uses the specifications as defined by ISO/IEC 14443. This includes short reading distances (maximum 3 to 4 centimetres). Furthermore, NFC based devices contain additional security features such as encryption, authorisation and verification in the air interface. These are specified in ISO/IEC 18092 (NF C IP1), ISO/IEC 21481 (NF C IP2) and the Japanese standard JIS X6319-x (FeliCa).

When the NFC-based function is in a smart phone, it can act as an RFID tag or contactless payment card. The smart phone uses exactly the same air interface protocol as that for a contactless payment card. However, application details may be different based on the capability of a smart phone.

9.2.4 Micro-tags or stick-on-tags

Because of the time to market of NFC payment technology, the card issuers have created what is effectively a self-adhesive plastic label ("micro-tag" or "stick-on-tag"), which can be affixed to any telephone or other common item carried by the individual and used for contactless payment. These stick-on-tags have no interaction with the processing on the mobile phone. It is effectively a contactless payment card in a different form factor. Other form factors exist such as key fobs.

9.3 Applications and parties involved

Due to the nature of payment cards to be used as flexible as possible by the cardholder, the same is supposed to be expected from contactless payment cards. This requires card issuers to be aware of the multi-application use of contactless payment cards and also include merchants into their considerations about the application itself as well as security aspects. There are already contactless cards that can be used as multi-application card for entitlements on prepaid or post-paid basis in public transport as described in 7.3.3. as well as for payment in retail stores. However, at the time of writing this TR, transaction values for contactless payments are limited in value.

Although many financial transactions can be 'agnostic' in terms of the products or services being purchased there are some where the RFID operator needs to consider the application. Some public transport systems are known to apply different rules for contactless payment from a banking card to those of a contactless transport card. There are also different levels of privacy associated with the different methods of contactless payment. In 8.4 we also consider some of the potential risks of the mechanisms being available globally.

9.4 Privacy considerations

9.4.1 General

Irrespective of the payment method chosen by an individual, the details on a payment card are always closely related to personal data. Information stored on a payment device directly refers to key financial account data of the individual. This can cause direct harm to the cardholder in terms of financial loss. At the same time, the cardholder will pay increased attention to the card as he is well aware of the threats related to abuse.

It is important to distinguish between privacy and data protection aspects of payment cards.

With the exception of some pre-paid cards, the PAN of a payment card is closely related to a personal account at a financial institution. This data is subject to the principles of data protection legislation such as 95/46/EC.

Privacy issues need to be considered during any contactless reading process, as all air interface protocols require a means of selecting particular tags for communication purposes using some form of chip identifier.

As for payment cards, the individual might be afraid of the financial loss due to a fraud risk, card holders will to pay increased attention to the card to avoid the threats related to abuse.

9.4.2 Security of contactless payment cards

The contactless payment cards are protected by security methods that are different from those used for mag stripe and chip and PIN cards. Additionally this distinguishes the method and process of payment. There are two security codes, and the card issuer (e.g. the bank or store) may choose which code structure to use:

— Static CVC3, which is a different authentication code to the mag stripe CVC1 code.

— Dynamic CVC3 generates a discrete authentication code for each transaction based on a challenge-response technique, where the challenge is issued by the terminal to the card. CVC3 uses the triple DES algorithm with a 112-bit key.

NOTE The static CVC3 is being phased out as scheme rules no longer allow its use on newly issued cards. In the meantime both operate in parallel.

9.4.3 Organizations

9.4.3.1 General

Being aware of the sensitivity of banking and financial transactions, there are two major organizations (see 9.4.3.2 and 9.4.3.3) that deal with security and data protection issues. In addition to the two umbrella organizations, there are over 650 members in the categories

— Financial institutions;

— Payment processors (e.g., for internet payment, other payment gateways);

— Merchants (e.g. retailers, airlines);

— Technology providers.

Either through rules defined by the organizations described below or through rules defined by the payment companies (e.g. MasterCard, Visa) products are tested to rigorous levels and certified. But the focus is on security and fraud detection and prevention, not on privacy. Understandably the payment companies and card issuers do not want to discuss how fraud can be committed.

9.4.3.2 Payment Card Industry (PCI)

The Payment Card Industry (PCI) has developed rules for providing data security, referred to as PCI Data Security Standard (DSS). These can be applied to both variants, contactless and contact payments. PCI's

founders were the global payment brands -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. PCI DSS defines a set of 12 requirements for the protection of cardholder data and then describes the steps necessary to implement a security assessment. Two PCI documents that have some relevance to Mandate M436 / 2 are:

— PCI DSS Wireless Guideline version 1.2 published in July 2009, dealing with wireless communication from the terminal to the application.

— PCI DSS Risk Assessment Guidelines version 1.0 published in November 2012, dealing with risk assessment of the system including data protection with some reference to ISO/IEC 27005.

In addition, the PCI self-assessment questionnaires (SAQ) could provide a model for some RFID PIA templates. The PCI SAQs could – probably should – be extended to address privacy.

9.4.3.3 EMV Co.

EMV Co. has been created as a limited liability company in 1999 by Europay International (today: MasterCard Europe), MasterCard and Visa. JCB and American Express joined as owners in 2004 and 2009 respectively. This consortium has established specifications to facilitate interoperability between chip cards and terminals for credit and debit payment. They have expanded their specifications to security and data protection aspects, also for contactless payment cards.

9.4.4 Impact of privacy in the banking and finance sector

Contactless payment products based on ISO/IEC 14443 (like contactless cards) does not need physical or visual contact between reader and data carrier. This enhances reading processes, but at the time is perceived as a potential threat to data protection and privacy because reading of information is not necessarily noticed by an individual. This aspect becomes the more important, as the data on payment cards are always closely related to an individual and contains information about key financial account data. The loss of such data may not only mean a breach of privacy but may additionally be related with financial loss for the individual and in return may cause higher criminal willingness for those intending fraud.

Gathering an individual's card details can be done without the cardholder being aware via any mode of operation (contact, visual, online, and in RFID mode). As this information could be used to make fraudulent transactions it is important for application developers to create safeguards that minimise the use of any data that can be captured, which reduces the interest of criminals to capture such information.

9.4.5 Vulnerabilities

There are vulnerabilities which can be exploited as threats to an individual when using payment cards. However, due to the nature of contactless payment cards there are some vulnerabilities which need to be addressed, additional to the general ones.

— The fact that two completely different levels of CVC3 (static and dynamic) are available, with one obviously weaker than the other is of basic concern. Furthermore, there is no way for the ordinary card user to know whether the bank card he is using has of the more or lesser secure version of CVC3.

NOTE 1 The static CVC3 is being phased out as scheme rules no longer allow its use on newly issued cards. In the meantime both operate in parallel.

— Data can be extracted from contactless cards using apps on smartphones. Whereas contact cards such as mag stripe need physical handling, contactless cards allow exploiting even the normal read range of 3 to 4 cm with standard equipment, without the victim being aware. Longer read ranges are possible with more specialist equipment to eavesdrop on transmissions.

NOTE 2 Penetration tests from PT-D show that read ranges can be increased by at least a factor of 2 for different frequencies (see FprCEN/TR 16670).

— Cloning of payment cards and their use causes direct financial harm to the card holder. The possibility of unnoticed reading of a contactless card and using the captured data increases the risk of creating a mag stripe clone of such a card. Unlike other cloning, the victim of electronic eavesdropping could be completely unaware of such risks. In contrast individuals are aware of letting a card leave their sight in any transaction requiring the card being inserted into a terminal or swiped.

— A similar consequence of cloning is possible with 'card not present payments' it is also possible to create a fraudulent "virtual" clone of the payment card. Although the 3-digit CVC, which is common practice at the time of writing this TR, is required not all those operating the cards for payment call for this - even though in breach of the PCI and / or EMV rules. Even when required, the code can be hacked through a "brute force" attack.

— There are vulnerabilities in the contactless communication between the payment terminals accepting various payment methods: while the transaction message is encrypted, the message identifier is not encrypted but is required to be unique and non-repeatable. Where pseudo-random generators are used for these transaction identifiers, these can be predicted and used for fraud.

Although the security aspects are beyond the scope of any RFID PIA, what needs to be stressed is these have the potential to impact on two aspects of personal privacy. The first is that the same attack methods, which can be used to exploit some of the vulnerabilities listed above, can be applied as part of identity theft. The second is if the vulnerabilities are in the system, the bank could be considered to be financially responsible for the fraud. It is therefore crucial to make bank customers aware of the technology used, inform them about the vulnerabilities and provide them with the appropriate know-how to decide for or against a contactless payment card.

9.4.6 Transparency, consumer information, commercial confidentiality and security

Payment cards are a privacy-sensitive issue for each individual. As new technology such as contactless cards also cause new malicious potential, individuals need to be informed about new technologies, their possibilities, the weaknesses and the individual's possibilities to decide for or against accepting such new technologies. Therefore, the cooperation of payment card industry, banks, card issuers, processors and the data protection authorities is crucial: it can at the same time enhance new technologies, the acceptance of which in the public can only be achieved when transparency on the product, its functionality and security features provided are clearly communicated.

It is appreciated that from the financial industry perspective the details of their security design, assessments and mitigations are highly confidential and commercially sensitive. However, the identified fraud and privacy weaknesses come from the poor take up of security/privacy options and need improvement taking into consideration the characteristics of RFID technology. The objective of data protection and privacy should be to address the weakest link in the chain, especially with regard to the threat of financial loss.

Given the widespread distribution and increasing use of contactless payment cards, there is concern that there need to be mechanisms whereby stakeholder participation and concurrence with the PIA process can occur and be shown to have been addressed. Any suitable mechanisms are not likely to include open information disclosure and the possibility of involving trusted stakeholder (including consumer) representatives may need to be considered as one approach. Another approach might be through the DPAs, some of which in Europe have expressed some concern about the privacy aspects of contactless cards and the need to address these. However, the individual needs advice on how to protect against fraud and to protect their own privacy (e. g. shielded wallets to protect contactless cards from unnoticed reading). The payment card industry's marketing may not only contain the benefits of the technology, but shall also provide potential card holders with information of all the consequences, adequate countermeasures to be taken by the individual as well as the choice to decide for a contact payment card.

9.4.7 Implications for the PIA

With the financial industry structure the core expertise that designs the technology and best understands the threats and vulnerabilities lays with a few organizations while there are world-wide millions of application

operators, many of whom are small businesses with no expertise to carry out their RFID PIA responsibilities. This situation would seem to confirm:

— The benefits of a PIA process that facilitates ‘reusable analysis’ should be considered so that core expertise can pass outwards to end operators thereby reducing burdens, through the use of templates and other tools. The PCI self-assessment questionnaire would appear to be a good starting point.

— The need for the PIA process to establish where consumer privacy information is needed and what public information is to be provided.

— The need for continual enhancements of the PCI and EMV rules and procedures, not just for security and fraud protection as at present, but also for privacy purposes.

Given the dependence of the application operators on core expertise, that there will be a need for scrutiny and checks to provide confidence to retailers and end operators as well as the public. This might be a role for DPAs.

10 Conclusion and recommendations

10.1 Diversity of RFID based applications

RFID technology is used in a variety of market sectors for very different purposes. Examples are numerous; this TR is restricted to Retail, Libraries, Public Transport and Banking and Financial services. Each sector hosts at least one RFID-application such as EPC, Identification and Access Control, eTicketing or contactless payment. Some sectors (e. g. retail, supra-regional transport systems) use open systems, which are adopted by a lot of users and benefit from large number of users. Other applications (e. g. employee cards, regional transport systems) are conceived for closed systems with a limited number of users.

Anyhow, the before-mentioned applications require specific functions and features of the air interface. In general, RFID components and air interfaces are following the specific requirements of a defined application, the business processes and legal rules that have to be obeyed. Privacy aspects need to be looked at in the given context and cannot be addressed generally.

A large variety of contactless communication interfaces using different frequencies, protocols and data models are specified in international standards and introduced into the market. All these technologies are summarised by the generic term “RFID”. The closer the relationship between the information on the RFID tag and personal data becomes, the more analysis of the individual situation is required to comply with privacy requirements appropriately in the defined context.

10.2 Benefits of and recommendation for sector or application specific templates

The European Commission has addressed the data protection and privacy issue in RFID based applications by its Recommendation dated May 12, 2009 (2009/387/EC). The objective was to support the introduction and enhancement of RFID technology by providing at the same time approaches to solutions for the safeguarding of data protection and privacy. One outcome of this Recommendation is the setting up of Privacy Impact Assessments (PIA), the process of which has been defined in the PIA Framework which was adopted in April 2011.

This concept is a feasible basis for the introduction of PIA to any sector and application because it provides the necessary flexibility to cope with the specific characteristics of any implementation. The process and methodology of how to conduct a PIA, based on the privacy principles as defined in the Data Protection Directive 95/46/EC, defines the boundaries. The details need to be covered in the sector or application specific context, due to the multiple possibilities which RFID can provide.

EXAMPLE The retail sector deals with a supply chain which starts with the provision of raw material, goes to production, transport and logistics, warehouse management, shelf availability and sales to the consumer. A RFID application intended to be used in logistics and/ or warehouse management (e. g. tagging of logistic units but no consumer

units) is completely different to one which also comprises the sale of products to a customer (single units passing the point of sale). Another distinction needs to be made depending on the kind of product (FMCG, textile, consumer electronics).

The results of a PIA will most probably differ from sector to sector and from one application to another. Requirements regarding privacy, likely threats and appropriate mitigation measures may be defined for a specific application, and derived from this for a group of similar applications. Nevertheless, a generic PIA for one or even more sectors will not be able to cover all relevant aspects needed to comply with the requirements for privacy. Depending on the purpose of use within one sector, there might even be the necessity for more than one PIA, e. g. when tagged goods pass the point of sale for settling the bill, and payment is effected with a contactless payment card, then two different applications need to be addressed.

The preparation of templates brings significant benefits for all stakeholders and supports the introduction of privacy compliant RFID applications:

— The alignment between stakeholders can be done once per application by involving e.g. customer representatives, RFID operators, suppliers solution providers and data protection officials during creation of the template.

— Operators can use templates as a reference for the implementation of privacy compliant applications and processes. They can use these to comply with the concept of "privacy by design" on the one hand and conducting a PIA by themselves without external support.

— All risks, the mitigation measures undertaken by the operator for a defined RFID-based application as well as advice for measures the individual can take additionally are documented in the PIA and can thus be made transparent to the public.

10.3 Recommendation for a general approach to PIA

RFID applications are complex and require a differentiated analysis according to where they are used. However, an overall approach can be done by establishing a common process. This process refers to the necessary steps that need to be considered in order to integrate all relevant aspects of a PIA. The process is described in EN 16571: *AIDC technologies - Information, Privacy and Data Protection Aspects of RFID - RFID privacy impact assessment (PIA) process* and consists of:

— Strategic considerations that an RFID operator needs to take into account before undertaking an RFID PIA. This includes taking responsibility over and above the requirements of the Recommendation.

— Tools and other mechanisms that can be employed to simplify the process of undertaking the PIA. These tools have the additional advantage of providing consistency between similar PIA reports.

— Defined process of undertaking an RFID Privacy Impact Assessment, including the degree of granularity required for a PIA.

— Definition of the lowest level of deliverable from the PIA process, which is an RFID functional statement.

— Definition of necessary details to prepare the description of the RFID application(s). This description covers all aspects from the RFID tag to how the RFID data is held on the application.

— Identifying the risks and undertake the risk assessment itself, including the consideration of appropriate countermeasures.

— Providing a summary of the PIA.

— Consideration of need for document revision control and monitoring.

Bibliography

[1] 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

[2] General Data Protection Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data 2012/0011 (COD)

[3] Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification C(2009) 3200

[4] A. F. Westin (1967), Privacy and Freedom, The first complete and authoritative study of privacy in America

[5] Technical Guideline (TG) 03126-1 of BSI - Federal Office for Information Security, Germany on Technical Guidelines for the Secure Use of RFID, Application area "e-ticketing in public transport" (2009)

[6] EUROPEAN CENTRAL BANK. Editor T. Kokkola (2010), The Payment System, Payments, securities and derivatives, and the role of the Eurosystem

[7] R. Walker (2011), Significant Growth in Cashless Payments in Europe, in European Payment Council (EPC) Newsletter 2011-08-19

[8] Risk Assessment Special Interest Group (SIG) PCI Security Standards Council (2012), PCI Data Security Standards (DSS), Version 1.

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™