PD CEN/TR 16674:2014

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 16674:2014.

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 83899 6
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 16674

June 2014

ICS 35.240.60

English Version

Information technology - RFID privacy impact assessment analysis for specific sectors

Technologies de l'information - Analyse des méthodes d'évaluation de l'impact sur la vie privée adaptées à la RFID

Informationstechnik - Analyse der RFID-Datenschutzfolgenabschätzung 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 16674:2014) 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

— 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 16673, *Information technology — RFID privacy impact assessment analysis for specific sectors*

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 to reduce barriers to adoption 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 standardization work program identified in the first phase.

This Technical Report is one of eleven deliverables for M/436 Phase 2. From a content point of view, and despite their name, most Privacy Impact Assessments in the world have a narrow focus, namely data protection rather than privacy protection. The result is that many PIAs are restricted to legal compliance checks and do not include societal aspects. That is reflected in the form of some PIAs, which are limited to checklists. Increasingly, however, PIA methodologies include narrative descriptions of the systems assessed and the environments in which they will operate, which help to understand better the potential privacy and data protection risks.

Also most PIAs are limited to risk assessment and do not include risk management. Thus, they can be used to identify and assess privacy and data protection risk without suggesting solutions or mitigation strategies, thereby restricting their usability.

This deliverable will begin with research of methodologies used for wireless technologies and the risks associated at within that part of the wireless system from the data carrier to the communication from the 'interrogator' or data capture device to the application system. The reason for this approach is to understand approaches used by security experts and that are not incorporated into any existing standards. This approach makes sense because it moves from the generic wireless towards the specific RFID issues. The intention is to draw relevant 'lessons' from a range of wireless technologies that can be applied to RFID technologies and applications. Risk management will focus on areas that accept the inherent risks of the given technology.

1 Scope

The scope of this Technical Report (TR) is to identify methodologies that are used for, or have been considered applicable to, wireless technologies. These methodologies are analyzed to identify features that are applicable to RFID.

Based on the Industry RFID PIA Framework endorsed by the Article 29 Data Protection Working Party, the Technical Report focuses on proposing risk analysis methodologies suitable for the data capture area of an RFID system. This includes the RFID tag, the interrogator, the air interface protocol used for communication between them, and the communication from the interrogator to the application.

The Technical Report also proposes risk management features based on the inherent capabilities of a number of RFID technologies that conform to standardized RFID air interface protocols. This should provide enough information to enable the proposed privacy control features to be applied to other RFID technologies including those with proprietary air interface protocols and tag architectures. The risk management features exclude fundamental privacy by design features because these should be the subject of revisions and enhancements to technology standards. The risk management features defined in this Technical Report are considered applicable to current and future implementations of RFID based on existing technology. As such, this Technical Report is considered as input into a standard procedure for undertaking an RFID Privacy Impact Assessment.

2 Terms and definitions

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

2.1
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
identified natural person or 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 specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

2.3
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

2.4
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

2.5
PIA process
process based on a privacy and data protection risk management approach focusing mainly on the implementation of the EU RFID Recommendation and consistent with the EU legal framework and best practices

2.6

privacy
the claim of individuals (...) to determine for themselves when, how and to what extent information about them is communicated to others" and as a mean "(...) for achieving individual goals of self-realisation

2.7
privacy impact assessment
methodology (a systematic process) for assessing the impacts on privacy of a project, policy, program, service, product or other initiative that involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative privacy impacts

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

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

2.10
accountability
responsibility of an organization for personal information in its possession or custody, including information that has been transferred to a third party for processing

2.11
wireless network
any type of computer network that is not connected by cables of any kind

3 Symbols and abbreviations

CEN Comité Européen de Normalisation

COBIT Control Objectives for Information and related Technology

DPD Directive Personal Data

NOTE 1 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

DPIA Data Protection Impact Assessment

DPR General Data Protection

NOTE 2 Regulation on the Protection of Individuals with regard to the processing of personal data and on the free movement of Such Data

ECHR European Convention on Human Rights EU: European Union

ECtHR European Court of on Human Rights

ENISA European Network and Information Security Agency

GDPR General Data Protection Regulation

ITIL Information Technology Infrastructure Library

NFC Near Field Communication

NIST National Institute of Standards and Technology

OECD Organization for Economic Co-operation and Development

PBD Privacy by Design

NOTE 3 Related to Data Protection.

PCC Privacy Commissioner of Canada

PIA Privacy Impact Assessment

PLD Personal Locating Device

RTLS Real Time Location Systems

SDLC System Development Life Cycle

TAS3 Trusted Architecture for Securely Shared Services

NOTE 4 EU research project Trusted Architecture for Securely Shared Services, Privacy Requirements, v.2.0, 2009

TDOA Time Difference Of Arrival

TRA Threat and Risk Assessment

Tri Triangulation

WAP Wireless Access Point

WiFi Wireless Ethernet

4 Risk analysis for wireless RFID communications and RFID devices

4.1 Introduction

As stated in the scope, the TR is to identify methodologies that are used for, or have been considered applicable to, wireless technologies. These methodologies are analyzed to identify features that are applicable to RFID. Furthermore, based on the Industry RFID PIA Framework endorsed by the Article 29 Data Protection Working Party, the TR focuses on proposing risk analysis methodologies suitable for the data capture area of an RFID system. This includes the RFID tag, the interrogator, the air interface protocol used for communication between them, and the communication from the interrogator to the application.

The RFID PIA framework is based on Opinion 9/2011 on “The Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications”. Opinion 9/2011 has been influenced by the requirements mentioned in the analysis of ENISA Position on the *Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [of March 31, 2010]* July 2010

The title of Recommendation (2009/387/EC) makes it very clear that the Commission has an objective to see the implementation of privacy and data protection principles in RFID applications, and for this to be partly achieved by RFID operators undertaking a privacy impact assessment (PIA). Much of the work approved under Mandate M436 Phase 2 extends this principle into more practical processes.

Unfortunately there is no evidence of a standards-based procedure for undertaking a PIA for applications using RFID technology. The TR therefore focuses on three strands of research:

— principles that are appropriate to RFID based on the research undertaken to prepare this TR;

— analysis of PIAs that are relevant to the RFID PIA, but not directly associated with RFID, from five countries (Australia, Canada, New Zealand, UK and USA) and discussed more fully in Clause 7;

— comparison between the intended approach and some European interim developments.

4.2 RFID technologies

The Recommendation, provides the following definition of RFID in Paragraph 3 (a):

'Radio frequency identification (RFID)' means the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag

This means that RFID applies to all RFID technologies specified by the ISO/IEC 18000 series of standards plus what some experts consider to be a different technology: smart cards. Thus, ISO/IEC 14443, ISO/IEC 15693, ISO/IEC 18092, ISO/IEC 21481, and the Japanese FeliCa (JIS X6319-4) all fall within the scope of the Recommendation. In fact any standardized or proprietary radio frequency technology operating within the regulated ranges, as listed here, fall within the scope of the Recommendation:

— <125 kHz to 134 kHz

— 13,56 MHz

— 433 MHz

— 860 MHz to 960 MHz

— 2,45 GHz

— 5,8 GHz (although there are no standards in the ISO/IEC 18000 series that address this yet.

NOTE Further details of the RFID privacy capabilities are provided in CEN/TR 16672 Information technology - Privacy capability features of current RFID technologies.

4.3 The RFID system architecture

Each RFID air interface protocol has different characteristics; the most obvious is the frequency at which the protocol operates. This impacts on power capabilities and read range. Even at a given frequency there are often multiple protocols, each of which offers the RFID application particular features. Currently the ability to have interoperable protocols is low. Interoperability between frequencies is rare, because the laws of physics vary according to frequency particularly between low frequency (125kHz to 133 kHz) and high frequency (13,56 MHz) on one hand and all the other higher frequencies.

Each specific air interface protocol defines the communication rules between the RFID interrogator (or reader) and the RFID tag. There are no explicit standards for the interrogator and the tag; instead products are required to conform to mandatory components of the protocol, and may support some of the optional features. Such optional features include the size of memory, even whether some defined areas of memory are supported. The optional features also include a number of commands, e.g. the support for sensors but also more basic features. For a given air interface protocol, tags have more optional (i.e. opt-out) features than interrogators; but this does not mean that interrogators are required to support all the features of a protocol. Generally an RFID application is built around a particular air interface protocol, and there can be many variants in the capabilities of tags that are available. In true open systems the RFID operator is dependent on the RFID tags (and hence their capabilities) provided by others in the value chain. Although not a truism, a rule of thumb is that tags with increasing capabilities tend to be more expensive; so the purchaser of the tags will tend not to over-specify requirements for capabilities. Until the Recommendation was published, few RFID operators consider privacy requirements, and CEN/TR 16672 clearly identifies that potential privacy enhancing features are not available in many RFID technologies.

Some of the protocols are considered fairly stable with little or no developments over recent years. Others, particularly ISO/IEC 18000-63, are under continual development with more features added with each revision. This adds to the complexity, because whereas tags with new features can be implemented reasonably quickly, changing the interrogator infrastructure involves longer-term investment decisions. But even if some advanced tags are introduced, not all tags in an application will change. This is particularly the case where the RFID tag or smart card has a viable life of many years.

The air interface is based on wireless communications, and as such is vulnerable to noise, which interferes with the communication, and to various threats. Because the interface is wireless, most protocols have no

means of restricting additional reads of the tag. In fact, in open systems it is essential that the tag remains readable to any authorised reader. Conversely this can also be exploited, as indicated by CEN/TR 16672. Additionally other mechanisms can be used to read data, such as eavesdropping. As RFID is a read / write technology, it is also possible to change data on the tag again for legitimate reasons (e.g. a chain of custody) and less legitimate reasons.

Besides the tag, the air interface protocol and the interrogator, there are other components to the RFID system. The interrogator needs to communicate with the application to receive instructions that are converted to air interface commands, and to send back responses from the tag e.g. the data read form the tag. The air interface transmits bits of data that need to be created (commands) and interpreted (responses). Device interface protocols and data encoding and decoding rules are needed to perform some of these functions. Not all air interface protocols and applications use standardized rules for this, although this is increasing – and essential in open system applications. Some specific standards are discussed in CEN/TR 16673: *Information technology - RFID privacy impact assessment analysis for specific sectors.*

In some cases the communication between interrogator and application is carried out over wired networks, but this requires readers to be in fixed locations. Wireless communications are also, and increasingly used, particularly with RFID enabled smart-phones and tablet computers. A particular case is with the use of near field communication (NFC). This can bring additional opportunities to the individual smart-phone owner. Where these are designed applications authorised by the RFID operator, this enhanced functionality adds to the application. But the other side of the coin is that making millions of smart-phones as RFID readers does have potential negative implications discussed below.

4.4 The challenge of having millions of readers in the hands of individuals

It is fairly easy to create an RFID reader, by using in-built features of NFC-enabled smart-phones. Originally focused on one air interface protocol dealing with smart cards, there are concerns that there is technology creep and these phones are able to read (and write) to tags compliant with other HF protocols. Some RFID operators are extending their applications to make use of the fact that RFID readers are increasingly present. The positives are addressed, but less so the negative aspects. These fall into two broad categories:

— The capability to change data on the tag, which can lead to disruptions of the intended application e.g. even to render the tag unreadable. This is predominantly a security issue for the application, but does have privacy implications too.

— The capability to read data from the tag beyond the scope of the application and beyond the domain of the RFID operator.

There have been developments for smart-phones to support the UHF-based protocols, particularly from Korea, but development has been slower than expected. However, it is feasible. Furthermore, there are many readers for most of the popular readers that can be connected to a USB port, some looking little different than a memory stick.

All of this means that individuals holding RFID tags or smart cards are probably unaware that tags and cards that they are holding can be read beyond the boundary of a particular RFID application. Some evidence has been presented in CEN/TR 16673; one example is of the recent capability to change data on RFID tags in the library sector, another is the capability to read data from some contactless payment cards.

Thus, intruders can launch denial of service attacks, steal identities, violate the privacy of legitimate users, insert viruses or malicious code, and disable operations.

The draft version of CEN/TR 16674: *Information technology - RFID privacy impact assessment analysis for specific sectors* identifies a number of threats that have been recorded in literature and shown to be possible. As a protocol reaches a critical mass of tags or cards in circulation, combined with low cost reading devices capable of reading the tags, this type of issue will spread. A properly structured PIA process can identify the risks and countermeasures that might be implemented.

4.5 Lessons from the risk environment concerning wireless networks

All computer systems are subject to different forms of threat, but wireless networks can suffer from additional threats because of the fact that there are various means of intercepting a wireless transmission that are not possible with a wired network. For RFID this applies to the air interface and wireless communication between the interrogator and the application. The US-based National Institute of Standards and Technology (NIST) recommends that before establishing wireless networks and using handheld devices, organizations should use risk management processes to assess the risks involved, to take steps to reduce the risks to an acceptable level, and to maintain that acceptable level of risk. Using risk management processes, managers can protect systems and information in a cost-effective manner by balancing the operational and economic costs of needed protective measures with the gains in mission capability to be achieved through the application of new technology.

The following is an abstract from NIST's report "Security for Wireless Networks and Devices". Apart from some details, this information is considered highly relevant to RFID.

NIST points out that each new development will present new security risks, which shall be addressed to ensure that critical assets remain protected. Actions that organizations should take to protect the confidentiality, integrity, and availability of all systems and information include:

a) Assess risks, test and evaluate system security controls for wireless networks more frequently than for other networks and systems. Maintaining secure wireless networks is an ongoing process that requires greater effort than that required for other networks and systems.

   The following steps that can be taken to improve the management of wireless networks include:

   — Maintain a full understanding of the topology of the wireless network.

   — Label and keep inventories of the fielded wireless and handheld devices.

   — Create backups of data frequently.

   — Perform periodic security testing and assessment of the wireless network.

   — Perform ongoing, randomly timed security audits to monitor and track wireless and handheld devices.

   — Apply patches and security enhancements.

   — Monitor the wireless industry for changes to standards that enhance security features and for the release of new products.

   — Monitor wireless technology for new threats and vulnerabilities.

b) Perform a risk assessment; develop a security policy and determine security requirements before purchasing wireless technologies.

   The risks associated with the use of wireless technologies are considerable, and many products provide inadequate protection. Organizations should plan to protect their essential operations before they adopt wireless technologies. Common administration problems include installing equipment with "factory default" settings, failing to control or inventory access points, not implementing the security capabilities provided, and not developing or installing security architectures that are suitable to the wireless environment. The use of firewalls between wired and wireless systems should be considered. Other good practices are to block unneeded services and ports, and to use strong cryptography. Often the risks can be addressed, but the tradeoffs between technical solutions and costs shall be considered as well. Organizations may want to postpone the installation of wireless networks until more robust, open, and secure products are available.

Organizations should perform security assessments prior to implementation of wireless technologies to determine the specific threats and vulnerabilities that wireless networks will introduce in their environments. In performing the assessment, they should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, the life-cycle costs of security measures, and technical requirements. Once the risk assessment is complete, the organization can begin planning and implementing the measures that it will put in place to safeguard its systems and lower its security risks to a manageable level. The organization should periodically reassess the policies and measures that it puts in place because computer technologies and malicious threats are continually changing.

c) Effective risk management should be integrated into the System Development Life Cycle (SDLC) of an IT system. The SDLC includes five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. NIST has issued recommendations for conducting the risk management process in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. This document is available online at http://csrc.nist.gov/publications/nistpubs/index.html.

d) Maintain an awareness of the technical and security implications of wireless and handheld device technologies.

   Wireless technologies present unique security challenges due in part to the relative immaturity of the technology, incomplete security standards, flawed implementations, limited user awareness, and lax security and administrative practices. In a wireless environment, data is broadcast using radio frequencies. As a result, data may be captured when it is broadcast. The distances needed to prevent eavesdropping vary considerably because of differences in building construction, wireless frequencies and attenuation, and the capabilities of high-gain antennas. The safe distance can vary up to kilometers, even when the nominal or claimed operating range of the wireless device is less than a hundred meters.

e) Carefully plan for the installation of wireless technologies.

   The security of wireless networks and devices should be considered from the initial planning stage because it is much more difficult to address security once deployment and implementation have occurred. A detailed, well-designed plan can point the way to better security decisions about configuring wireless devices and network infrastructure. The plan will support decisions concerning the tradeoffs between usability, performance, and risk. It is necessary to apply security management practices and controls to maintain and operate secure wireless networks.

f) Organizations should identify their information system assets, and develop, document and implement policies, standards, procedures, and guidelines to ensure confidentiality, integrity, and availability of information system resources. NIST recommends the following steps:

   — The information system security policy should directly address the use of 802.11, Bluetooth, and other wireless technologies.

   — Configuration/change control and management practices should ensure that all equipment has the latest software release, including security feature enhancements and patches for discovered vulnerabilities.

   — Standardized configurations should be employed to reflect the security policy, and to ensure change of default values and consistency of operations.

   — Security training is essential to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies.

   — Robust cryptography is essential to protect data transmitted over the radio channel, and theft of equipment is a major concern.

g) Physical controls should be implemented to protect wireless systems and information.

Adequate physical security measures include barriers, access control systems, and guards. Physical countermeasures can lessen risks such as theft of equipment and insertion of rogue access points or wireless network monitoring devices. The small size, relatively low cost, and constant mobility of handheld devices make them more likely to be stolen, misplaced, or lost, and the physical security controls that protect desktop computers do not offer the same protection for handheld devices.

h) NIST recommends to enable, to use and routinely to test the inherent security features, such as authentication and encryption methods that are available in wireless technologies. Firewalls and other appropriate protection mechanisms should also be employed.

Wireless technologies generally come with some embedded security features, although frequently many of the features are disabled by default. The security features available in wireless networks and devices may not be as comprehensive or robust as necessary. The security features provided in some wireless products may be weak; therefore, robust, well-developed, and properly implemented cryptography should be used to attain the highest levels of integrity, authentication, and confidentiality.

The built-in security features of Bluetooth and 802.11 networks can include data link level encryption and authentication protocols, and these features should be used as part of an overall defense-in-depth strategy. Although these protection mechanisms may have weaknesses, they can provide a degree of protection against unauthorised disclosure, unauthorised network access, and other active probing attacks.

The data link level wireless protocol protects only the wireless sub-network. Where traffic traverses other network segments, including wired segments or the organization’s backbone network, other end-to-end cryptographic protection may be required. Since there is still a residual risk when cryptography and other security countermeasures are used, it may also be necessary to provide strategically located access points, firewall filtering, and antivirus software.

4.6 Conclusion and a way forward

The recommendations of NIST can be used *mutatis mutandis* for the RFID applications. It should be noted that NIST recommendations are for wireless networks and hence applicable when an application read operation is undertaken within the application domain. However RFID identifiable items in the possession of individuals pass beyond the application boundary and are potentially subject to conditions and attacks that are outside the control of the main network and so the protective capability of the RFID tag is the main focus for assessment for such situations.

The approach calls for a formal risk assessment procedure taking into account threats and vulnerabilities. There are no international standards that address RFID and its associated privacy risk assessment. However, ISO/IEC 27005 provides some methodologies for carrying out risk assessments and these have also been adopted and adapted by ENISA, but not explicitly for RFID.

Three metrics are required:

— A valuation of assets in the application. For RFID and privacy this needs to be based on the "value" of explicit personal data or identifiable data encoded on the RFID tag. This would include unique chip identifiers that are present in most RFID technologies. ISO/IEC 27005 score assets in a range from 0 (no value) to 4. Given the early stages of developing an RFID PIA this level of granularity seems reasonable.

— Threats associated with the technology need to be considered. There is sufficient literature on RFID threats for these to be identified and taken into consideration. In ISO/IEC 27005 threats are defined as low, medium or high.

— Vulnerabilities identify the opportunities to exploit a threat. Again ISO/IEC 27005 has a simple metric of low, medium and high.

How these are applied is discussed in CEN/TR 16674, which will be the subject of public review, so describing details is probably not appropriate in this Technical Report. Table 1 shows the approach to providing metrics to risk assessment.

Table 1 — ISO/IEC 27005-matrix approach to determine a risk value

	Likelihood of Threat	Low			Medium			High		
	Ease of Exploitation - Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

The overall risk score is between 0 to 8. Initially the difference between one value and the next for assets, threats and vulnerabilities could be arbitrary. For consistency, CEN/TR 16674 will need to provide some meaningful guideline that can be understood by RFID operators, particularly SME operators. The long-term temptation might be to expand the range of assets, threats and vulnerabilities. This should be avoided for two reasons:

— The Recommendation calls for the information to be provided about the application to include " the likely privacy risks, if any, relating to the use of tags in the application and the measures that individuals can take to mitigate these risks." This risk scoring is detailed enough to be understood by most citizens.

— Changing the scoring system will result in an old and new risk scoring being operated simultaneously.

Instead what is proposed is that as more knowledge is acquired more sophisticated methods could be developed to correctly assign the component scores.

NOTE The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) provides alerts about IT vulnerabilities. These are presented as high, medium, or low; but behind these is a100 point scale, which in turn has complex algorithms to determine the score. Most users focus on the simpler score of high, medium, or low and the software or hardware that has the vulnerability.

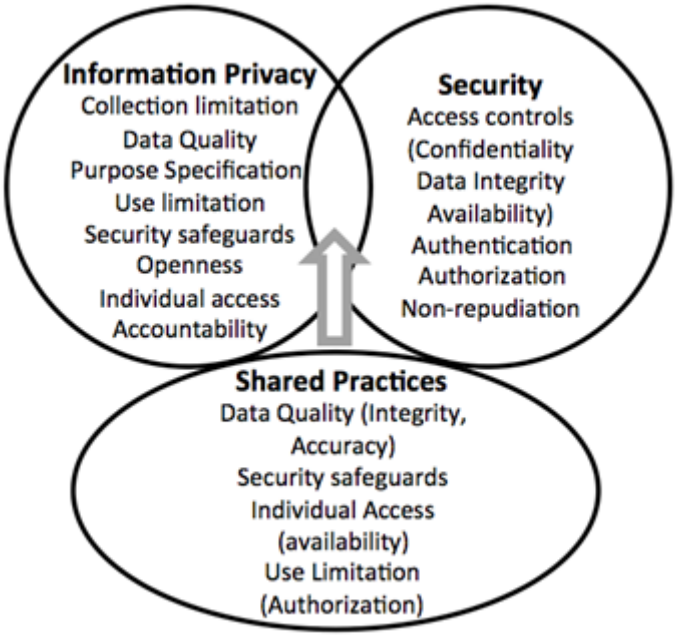
5 The relationship of the RFID PIA process and methodologies standards to the privacy law

5.1 Privacy requirements

The Directives 95/46/EC and 2002/58/EC (privacy directives) are applicable only when the processing of personal data is taking place. The controller as defined in the Directives is responsible that the processing of personal data is performed in compliance with the privacy directives. Although the wording in the privacy directives is generic and isn't explicit on RFIDs, at the moment RFID tags, (smart) cards, RFID readers/interrogators and connected back end systems are processing personal data the EU data protection legislation in all its rigor is applicable.

Article 17 of 95/46/EC and Article 4 of 2002/58/EC obliges the controller to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. The measures shall

ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Recital 46 of Directive 95/46/EC stipulates that the controller is responsible for appropriate technical and organizational measures to be taken, at the time of the design of the processing system as well. According to Article 17 of the Data Protection Directive 95/46/EC personal information/data shall be protected in a manner commensurate with its sensitivity. The sensitivity of information may vary according to context. Security safeguards shall protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use or modification. Personal information that is no longer required for the identified purposes shall be disposed of in a secure manner. Privacy protection and information security overlap each other but are not similar as can be concluded from Figure 1.



Source: Cavoukian 2002

Figure 1 — Shared areas of privacy protection and information security

Based on 95/46/EC the following eight basic threats can be discerned that are relevant for PIA:

1. secret possession of personal data [files];
2. secret processing of personal data;
3. out of bounds processing;
4. out of law processing;
5. out of jurisdiction processing;
6. irresponsiveness to discontent of the data subject by the controller;
7. personal data deterioration.
8. Violation by the data controller.
9. Personally owned products where individuals undertake their own processing using purchased apps (for example smart-phone apps)

10. Personally owned products that can be accessed by others even if there is no organizational application relevant to the accessible product (examples: wireless printers, RFID tagged books that have been purchased and tags may be kept enabled for personal inventory and library use or tags that haven't been killed after the delivery of the goods

The provisions of the European Directives 95/46/EC and 2002/58/EC have been transposed into the legislation of all EU Member States and is applicable to all controllers (see definition) and processors (see definition) within the EU.

The European Commission issued a Recommendation dated 12 May 2009 on the implementation of privacy and data protection principles in Applications supported by Radio Frequency Identification ("RFID Recommendation"). In that Recommendation, the Commission established a requirement for the endorsement by the Article 29 Data Protection Working Party of an industry-prepared framework for Personal Data and Privacy impact assessments of RFID Applications. These assessments are commonly referred to as privacy impact assessments, or PIAs. This RFID Application PIA Framework ("the Framework") addresses that requirement.

The Art. 29 Working Party has endorsed the RFID PIA Framework, developed by industry, in February 2011 in its Opinion 9/2011. On 25 January 2012 the European Commission published the final version of the proposal for the General Data Protection Regulation on the Protection of Individuals with regard to the processing of personal data and on the free movement of Such Data (DPR) as the successor to the Data Protection Directive 95/46/EC (DPD).

In the upcoming (2013) General Data Protection Regulation (GDPR) Article 30 obliges the controller and the processor to implement appropriate measures for the security of processing, based on Article 17(1) of Directive 95/46/EC, extending that obligation to processors, irrespective of the contract with the controller.

Articles 31 and 32 introduce an obligation to notify personal data breaches, building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC.

In Article 33 data protection impact assessment (DPIA) are being mandated for data controllers and processors whose processing presents specific risks to the rights and freedoms of data subjects.

The DPIA has been described in general terms as ”an assessment of the impact of the envisaged processing operations on the protection of personal data.”

Under discussion is whether a ‘privacy impact assessment’ has a broader meaning than a ‘data protection impact assessment’. The reason for this is that the term ‘privacy’ is considered to be much wider than ‘data processing of personal data’. Unknown yet is whether a data protection impact assessment will become a tool for simply checking the legal requirements spelled out in the European data protection framework (compliance check with a restricted scope compared to a PIA).

As in the EU Commission Recommendation C (2009) 3200 has been stated in the scope that it provides guidance on “design and operation of RFID applications in a lawful, ethical and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data”, apparently the use of both terms indicate that a broader concept than data protection has to be addressed in a PIA. Therefore a PIA has to cover all aspects of privacy: physical (bodily) privacy, privacy of personal behavior, privacy of personal communications, informational privacy and spatial privacy.

5.2 Definitions

5.2.1 General

It remains to this day difficult to find a meaning of privacy that is not significantly bound to a particular subjective or cultural perspective. For example, privacy in some Asian cultures, which tend to focus more on the collective, appears to place great emphasis on the preservation of reputation rather than on individual rights as such. In Clause 2 is a definition of privacy that has been generally accepted by most privacy experts.

Westin's definition of privacy is commonly used: "the claim of individuals (...) to determine for themselves when, how and to what extent information about them is communicated to others" and as a mean "(...) for achieving individual goals of self-realisation"

One of the reasons why privacy creates conceptual problems is that different aspects of privacy are belonging to the different sectors as can be concluded from Figure 2.

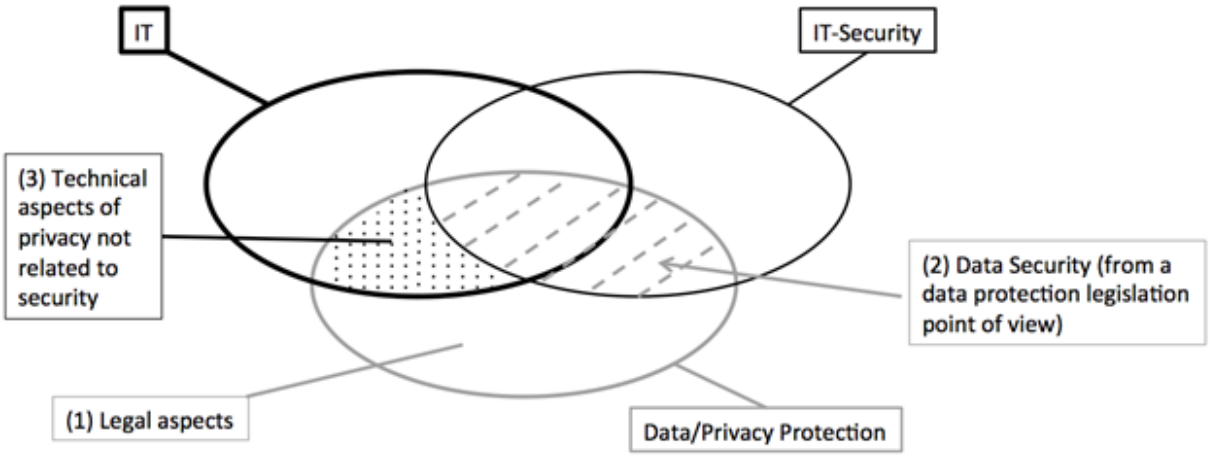


Figure 2 — Correlation of IT, IT Security and Privacy Protection

5.2.2 Five types of privacy

Amongst privacy experts it is generally accepted to that privacy can be discerned into five types of privacy. These types of privacy are covered by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms covers privacy i.e. the right to respect private life, family life, home, correspondence and communications.

1. Physical privacy. This is to ensure the integrity of the body of the individual. Problems that can occur include: mandatory immunisation, blood transfusion without consent, compulsory surrender of body fluids, hair and skin, and compulsory sterilisation;

2. Privacy with respect to personal behaviour. This affects all aspects of behaviour, inclusive intimate, sexual behaviour, both in private and in public spaces, also called as 'media privacy';

3. The privacy of personal communications. For individuals, it is important that they are using a variety of media to communicate without their communications being watched by other persons or organizations. This form of privacy is also known as 'interception privacy';

4. The privacy with respect to personal information. Individuals claim that data about themselves, not necessarily should be automatically available for other individuals and organizations, and that, even though others obtain such data, the individual himself shall be capable to exercise a considerable degree of control over that data and the use of these data. This is often referred to as "data privacy" or "informational privacy"

5. The spatial privacy as a shield of its own territory.

The following principles are applicable with regard to the protection of privacy according to The European Court of on Human Rights (ECtHR): The technology, i.e. RFID, should be used in accordance with and as provided by the law; The technology or processing should serve a legitimate aim; The technology should not violate the core aspects of the privacy right; The technology should be necessary in a democratic society; The technology should not have or give unfettered discretion; The technology should be appropriate, least

intrusive and proportionate; The technology should not only respect privacy requirements but also be consistent with other human rights. (Wright & De Hert, 2012, p.45-76)

At the moment personal data is processed within the fields of the above mentioned types of privacy the Directive 95/46/EC (DPD) and the e-Privacy Directive 2002/58/EC are applicable.

5.2.3 Personal data

Notwithstanding the lack of a worldwide-accepted definition of privacy, the governmental authorities charged with the enforcement of privacy rights needed to concur on what data required protection. Within the EU and specifically under the Directives mentioned under 5.1, personal data has been defined as stated under the terms and definitions 2.4.

While this definition appears to be relatively straightforward, its application to more contemporary technologies like RFID has introduced significant challenges. The Article 29 Working Party has provided guidance in its opinion 4/2007 on the scope of on the concept of personal data.

5.2.4 Processing

“Processing” of personal data under the Directive is understood as stated under the terms and definitions 2.8.

The definition of processing is important to consider because the list of examples of what may constitute a processing activity provides a substantial breadth of the types of activity to which the Directive may apply.

5.2.5 Processor

The next logical term to define is that of “processor” which in the Directive is defined as stated under the terms and definitions 2.9.

5.2.6 Controller

This is a somewhat circular definition, as it refers to undertaking any of the acts defined as processing on behalf of an entity called a controller. A “controller” under the Directive is defined stated under the terms and definitions 2.1.

TAS3 comments that “Read in conjunction, the controller is the party deciding on the means or purposes of the processing. A number of issues are raised with these terms and their applicability to modern business transactions and information flows, like outsourcing. It is often difficult to determine in practice that party is the controller and which is the processor, although it is a fundamental issue. The Data Protection Directive (EC/95/46) characterises the test of a controller in terms of the degree of discretion or decision-making authority exercisable by that party in relation to the data it processes. The party that decides the purposes and means of the processing will be the controller.

The difficulty many organizations face in practice is that their business operations are dynamic. Businesses operate in an increasingly collaborative manner and the nature of relationships changes over time. A party that was once merely a processor might, over a period, assume a greater degree of responsibility in relation to the data. This might occur as a result of additional services being added or new technology being deployed. More subtly, as the relationship develops, the processor may simply be entrusted with greater discretion in relation to the data.” (Alhadeff J., Van Alsenoy B, 2009,p.9)

5.2.7 Data security

5.2.7.1 General

As pointed out under 4.1 data protection legislation obliges the controller and the RFID operator to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful

destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

5.2.7.2 Data Security at the periphery

RFID privacy assessment has to be addressed for tags used in data subjects' day-to-day lives where 99 % of the time they will be open to threats not under formal data protection controls implemented by the RFID operator. In other words, the issue is about the periphery of the application or activities beyond the accepted system boundaries. This places the burden of privacy protection on the protective capabilities of the tags and in turn the protective capabilities that are used are frequently determined by the readers.

5.2.7.3 Data security for central databases

The security of centralised databases is also of great concern with loss or theft being a frequent occurrence in many industries. Furthermore SMEs suffer from data base security threats disproportionately compared to large corporations. It is essential that PIA process addresses the needs of SMEs who should not be discouraged from taking up the technology due to the burdens of assessing and implementing privacy and security for their applications. Significant privacy threats could emerge if RFID tag personally linkable data that is lost or stolen.

5.2.8 Data minimization

Data minimization is one of the most important principles in the data protection theory and practice.

The principle encompasses:

a) The collection and further processing of personal data shall be adequate, relevant and non-excessive in relation to the purpose for which they are collected/processed and the data should be kept in a form that permit identification of data subjects for no longer than necessary for the purposes for which they were collected/processed. The possibility of identification of the data subject, i.e. linking personal data with an individual should be removed as long as it is no longer indispensable. This may be achieved through anonymisation or pseudonymisation of personal data. Data which is no longer needed for the purpose(s) for which it was collected/processed should be erased; for certain categories of data, such as traffic data) this requirement is specified in relevant legal instruments.

   Mechanisms to limit collection could include screening out transmissions from non-targeted tags. Specifically, rather than issuing indiscriminate read commands and then filtering to retain the tags of interest, reader queries could target only relevant tags. It is advised to delete data immediately that it was not necessary to collect in the first place.

   Organizations could configure the technology to recognize distinct collection practices. For example:

— Anonymous Monitoring: This allows for the collection of information without the need to know the unique ID of any given tag. Floerkemeier uses the examples of sensor applications such as automatic door openers or the counting of the number of items in a given area.

— Local Identification: This is used to identify the presence of a certain item in a particular area, but does not show where it has come from. Revealing the past locations of an item would not be permitted without an appropriately strong justification, such as a criminal investigation. A declaration of use only for local identification would provide the employee with some assurance that his or her movements would not be tracked across different locations.

— Item Tracking: This practice goes beyond local identification and involves the tracking of items as they move from one location to another. This has the potential to enable the tracking of employees through association of the employee with the unique identifier in the RFID tag.

— Person Tracking: A workplace system might be designed to collect information about an employee's location or movements. This might be done, for example, through RFID tags in uniforms or RF-enabled ID cards. It is also possible that such information can be gleaned from item tracking, if the item in question can be associated with an identifiable individual. If item tracking is also used to track persons, this additional purpose for collection shall be identified. Person tracking will almost certainly raise more substantial privacy issues than item tracking.

These collection declarations can be used to selectively allow tags to remain anonymous, whenever possible.

Whenever possible, anonymous monitoring should be used instead of monitoring that could identify the employee. Anonymous replies are already part of some RFID protocols.

The greater the amount of identifiable data held on the tag, the more likely it is that some sort of privacy could be placed at threat outside the application's operational domain.

b) Collection Limitation: Personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. In other words, in lack of a legitimate basis for processing (such as one of those listed in Article 7 DPD), personal data may not be collected/processed and the individual concerned shall remain anonymous.

The system, network and related processes shall install appropriate limits on personal data collection to what is needed for legitimate, identified and notified business purpose. The system shall be supplemented by explicit policies that limit employee access to data based on business need.

c) Response to attribute requests: Technical policy enforcement mechanisms shall have the ability to respond to data requests with only that information that the requesting entity is authorised to receive (sufficient level of granularity).

Selective attribute/personal data disclosure during authentication: Authentication protocols shall be designed in a way which ensures that no more attributes/personal data than needed for the processing are verified or propagated (e.g. avoid unnecessary leaking of identifiers).

Storage limitation: Procedures shall be in place to ensure destruction or anonymisation of personal data once the purpose for which it was collected and/or further processed has been completed

Prior to initiating any processing operation upon personal data, the storage duration of each data element shall be specified, either individually or by category, for every entity that is involved in the processing. This should be done as part of the service/process definition.

5.2.9 Purpose binding

The purpose binding principle requires organizations to identify the purposes for which personal information is collected at or before the time the information is collected. In the employment context, this can be done through personnel manuals, policy statements or other such documents, providing they are made easily available to employees. More importantly, however, the components of all RFID systems should be identified and marked to make their use clearly evident and transparent.

Users shall be notified of the purposes for which personal information is collected using RFID technology. It is a good practice to break down and identify as specifically as possible the purposes for the use, collection and disclosure of information gathered through the use of RFID tags.

RFID technology could be designed to address the identification of purposes. Building Privacy Principles, embedded in the data protection directives, into technology is required, like into the communication between RFID readers and tags. For example, separate purpose "declarations" could be used for different reader queries to identify the specific purposes for which a tag is being read, for example: "Access control" ("Tag IDs are scanned for the purpose of access control, e.g., by identifying a pass holder or by authorising the validity of an access key."), "Anti- theft", "Asset management" (where "tags are read to provide a picture of the

whereabouts of assets."), and "Emergency services" ("The system is monitoring tags to provide rescue workers with occupancy information.").

However it is accomplished, all purposes for which personal information is collected shall be identified. Collecting information about the location of an item for the purpose of monitoring its movements potentially enables the tracking of people through association with the unique identifier in the RFID tag. For example, the tracking of a piece of equipment within the workplace may indirectly provide the employer with information about the activities or whereabouts of the employee who is authorised to use that equipment. If the tracking can be justified as reasonable, then this purpose for the collection of personal information shall be separately identified (see "Limiting Collection").

Other important privacy requirements are Openness and Individual access.

5.2.10 Openness

It is essential for organizations that make use of RFID systems to devote adequate time and resources to educating users (ANEC's research, and that of others, has shown that consumer education is a very weak mechanism and should only be applied when privacy-by-design and usability are poor) and employees about how the technology functions, where the RFID tags and readers are located, what information will be collected and how that information will be used. Users and employees shall be told about the presence of all RFID tags on items in their environment (such as products and packaging, tools and other assets) and the presence of all readers.

Employees should also be given a demonstration of how the information is gathered in the workplace. For example, employees should know that RFID tags broadcast information without the employee taking any action.

Employees shall be told whether the RFID-related information will be linked with other personal information and whether the information will be made available to third parties.

Data Management: Data shall be managed according to a data life cycle that describes its management from collection to deletion, and all processes in between, including which events trigger which processes.

There shall be no **hidden** RFID tags or readers. A notice saying that an RFID tag is being read can be placed close to the reader, or by having the reader emit a tone or flash a light when a reading takes place. Experts doubt that the notice requirement will be practical in the consumer environment.

5.2.11 Individual Access

Users are entitled to have access to their personal information that is collected by the organization that uses the readers and/or are processing the personal data into the back office systems. Users (consumers, employees) to fully exercise this right of access, shall know the scope of the collection that is taking place. There shall be no hidden RFID tags or readers. Thus, all RFID readers shall be identifiable so that users can request access to the personal information that has been collected and question whether the data that has been gathered has been used for a purpose for which they have not granted consent.

For example, an employee could request all the data that is associated with his RFID-enabled employee card.

The location of all tags and readers is also important, as it may be possible that RFID systems could interfere with active implantable medical devices.

5.2.12 Consent

Also of significant relevance, both within the Directive and towards the RFID applications is the concept of "consent". As defined in the Directive, consent has the meaning stated under the terms and definitions 2.3.

The Directive 95/46/EC explicitly lists the cases in which personal data may be processed. This means that for each processing of personal data – collection, recording, storage, adaptation, alteration, retrieval, consultation, disclosure, dissemination, etc. - the controller has to verify if the processing falls under one of the criteria for making data processing legitimate, i.e.:

— the data subject has given his unambiguous consent for processing;

— the data processing is necessary for the performance of a contract to which the data subject is party or in order to take pre-contractual steps which are necessary to conclude a contract at the data subject's request;

— the data processing is necessary to comply with a legal obligation to which the controller is subject;

— the data processing is necessary to protect the vital interest of the data subject;

— the data processing is necessary for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except where the interests or the fundamental rights and freedoms of the data subject, in particular the right to protection of the private life, prevail.

The privacy directives and the DPR require both the knowledge and consent of the user for the collection, use or disclosure of personal information. The controller has to inform the users about how the information being collected by the RFIDs would be used, The organization has to develop and make available a policy document on the use of the RFIDs, for example in a leaflet attached to the product or on its website.

Because RFID systems are a relatively new phenomenon, many users will be unfamiliar with the technology, how it operates and how data is collected, used and stored. Organizations implementing an RFID system should educate their employees about the privacy aspects and that an organization needs to make an effort to help individuals understand their privacy rights. The DPD rules that organizations have primary responsibility to inform individuals about the primary and any secondary purposes motivating a collection, use or disclosure of any personal information, as well as their options in a particular information bargain, including any ability to opt out of a particular collection, use or disclosure of personal information.

Under the Directive, consent is a mechanism of central importance, which enables data subjects to exercise their rights. The hallmarks of consent are that it be freely given and informed. The Article 29 Working Party Opinion 15/2011 provides a thorough analysis of the concept of consent as currently used in the Data Protection Directive and in the e-Privacy Directive. The Opinion provides numerous examples of valid and invalid consent, focusing on its key elements such as the meaning of "indication", "freely given", "specific", "unambiguous", "explicit", "informed" etc. The Opinion further clarifies some aspects related to the notion of consent. For example, the timing as to when consent shall be obtained, how the right to object differs from consent, etc.

The consent may at a later time be withdrawn. If there is no freedom of expression, then any consent invalid, so void and / or voidable. Since the permission should be given with respect to a specific processing and target-specific data, a generic authorisation (consent) is not valid. The consent shall be given in principle every time. The more sensitive personal data (for example medical data) is, the greater the requirements for permission.

Any collection, use or disclosure of personal information shall meet the test of what the reasonable person would consider appropriate in the circumstances. (Test of reasonableness). Under the privacy directives and DPR there are several situations where personal information can be collected, used or disclosed without the individual’s consent. Article 13 of 95/46/EC contains exceptions and limitations thereto.

These exceptions may prove to be important in the context of RFID technology, as RFID creates the potential for organizations to collect unprecedented amounts of personal information.

5.2.13 Limiting Use, Disclosure and Retention

Organizations shall not use or disclose personal information for purposes other than those for which it was collected, unless the individual consents or the law requires it. In cases where information has already been collected and the organization wants to use or disclose the information for a new purpose, employee consent is required. For example, if an employer has collected information using RFIDs for the purpose of tracking equipment, then linking this information to employee personal information and using it for disciplinary purposes would be beyond the scope of the original collection.

Information that is inadvertently collected should be immediately disposed of in a secure manner. Organizations shall retain personal information only for as long as necessary to achieve the purposes for which it was collected. When the information is no longer required, it shall be disposed of immediately, in a secure fashion, taking into consideration requirements for employees' right of access.

5.2.14 Accuracy

Personal information needs to be as accurate, complete and up-to-date as necessary for the purposes for which it is to be used.

Organizations may encounter a scenario where users contest the accuracy of the information gathered using an RFID system. For example, a user may challenge their registration on a reader that they claim not to have experienced. It is possible that other individuals might use uniforms, badges or other items embedded with RFID tags containing information pertaining to an employee, with or without the employee's consent. As well, whether a tag can be hacked and the data altered will be of major concern for organizations, unions and employees. For example, an RFID- enabled badge of an employee in an airport or nuclear facility might be an attractive target for an unauthorised person seeking access to a secured area.

RFID Operators should provide users and employees with **a risk analysis** of the accuracy of information their RFID system will provide, based on the particular applications. With this information, users and employees will know the perceived limits of a particular RFID system and be in a better position to know when to challenge conclusions derived from it.

5.2.15 Unique identifiers

New Zealand has formulated an extra privacy principle or requirement concerning unique identifiers, such as IRD numbers, bank customer numbers, driver's license and passport numbers. These unique identifiers shall not be assigned to individuals unless this is necessary for the organization concerned to carry out its functions efficiently. The identifiers shall be truly unique to each individual (except in some tax related circumstances), and the identity of individuals shall be clearly established. No one is required to disclose their unique identifier unless it is for, or related to, one of the purposes for which the identifier was assigned. The Government is not allowed to give people one personal number to use in all their dealings with government agencies.

Addressing the uniqueness of the data elements that may be linkable to individuals is an important aspect of privacy analysis. However it should be noted that the New Zealand approach does not address RFID technology where tags can incorporate unique chip identifiers that can be accessible to others beyond the application operator's control.

5.2.16 Accountability

In light of the growing realisation that the notice and consent model has limitations in the Information Society, the concept of accountability has been developed. WP 29 has elaborated on the principle of accountability in Opinion 3/2010. The proposed General Data Protection Regulation on the Protection of Individuals with regard to the processing of personal data and on the free movement of Such Data (DPR) has implemented the concept of accountability for controllers in article 22. It clearest articulation has been made in PIPEDA (the Canadian privacy law) as stated under the terms and definitions 2.10.

Someone within the organization thus shall be accountable for the use of RFID systems. The EU privacy directives and the Data Protection Regulation also consider someone responsible when personal data are processed, i.e. the Controller.

The controller can appoint the individual accountable for privacy compliance by. This will be the privacy officer. He should be involved in the design of any RFID system and should complete a Privacy Impact Assessment on its application in advance of deployment. By addressing privacy at the design stage, organizations can help ensure that their RFID- related activities comply with EU's privacy laws and meet their users' reasonable privacy expectations.

The controller shall be aware of all collections of personal information by the RFID system and all subsequent uses, disclosures and the retention period. This may include procedures for approving new and unanticipated uses of information gathered by RFID systems and ongoing PIAs. This might also extend to preparing procedures for dealing with unauthorised uses of access control records.

Any data from the RFID system that is transferred to a third party for processing (the processor) shall be protected by a contract that provides comparable protection while it is being processed.

The components of an RFID system shall be labelled or coded with the identity of the organization that is responsible for them. Without knowledge about the device that is collecting data, it would be difficult to satisfy the principles of Openness and Accountability.

5.2.17 RFID operator

The EU Commission's Recommendation makes clear that all RFID operators should assess the impact of their RFID operations on privacy and data protection. Article 3 (e) of the Recommendation stipulates: " '*RFID application operator' or 'operator' means the 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*". Note that also a **natural person** not being a commercial organization may be obliged to execute a PIA

5.3 Accountable Technology

Technology assuring privacy in the information society is becoming increasingly important. In defining what technical architectures should look like, the major requirements are related to policy-aware tools, including transactions logs, language frameworks and perhaps most importantly policy-reasoning tools.

The increased level of identified transactions, which occur on-line across all aspects of life, and the rise of identity theft and other similar crimes have also heightened concerns of accountability across information flows. Personal data breaches have become a common part of the lexicon and are now defined in the revised e-Privacy Directive as:

"*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community".*

5.4 Applying Data Protection Concepts in practice

A workflow approach to privacy and security requirements first starts at the moment an individual enters a system/ecosystem.

The first introduction of a person to a system may be in person, on the phone, via documents, RFID chips or online. In all cases, the individual has a right to know certain things:

— Who is controlling the collection of information;

— What personal information is being collected (both in the event of directly and indirect collection);

— For what purpose is the information is being collected;

— How the information will be used;

— Who the information will be shared with;

— That the information will be appropriately secured;

— How to request access to the information for correction/review;

— The information will only be retained (in identifiable form) for a period of time relevant to the purposes of collection.

A number of these questions are essential to allowing an individual to determine whether they wish to consent to the collection and use of the information. In considering these questions, it is essential to understand all the possible purposes of collection and uses of information by both the collecting entity and any downstream/ecosystem entity with which the information may need to be shared. The consent of the data subject to the collection and use of information is limited to those purposes specified. Thus, if an enterprise only specifies the limited uses of information that it currently engages in, but then desires to share the information with other parties, or use the information for other purposes, a new notice and consent would be required.

5.5 Technical/business considerations

There is a need to develop a notice strategy across all channels of communication and to explore short-form notice options to address form factor issues. The understanding of what personal data elements are going to be needed is important. One has to identify the persons/organizations that may get access to the information Developer and user have to consider how the various data elements will be used by the system and the ecosystem.

Developers and controllers have to address intrusion detection, virus protection firewalls, encryption at rest and in motion, authentication/ID management systems, authorisation, access control, audit/logging, data retention/deletion, separation of duties and security policies.

6 RFID and personal information

6.1 DPD

EU privacy Directive 95/46/EC (DPD) states that the principles of data protection shall apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person. Data rendered anonymous in such a way that the data subject is no longer identifiable means that the Directive is not applicable.

6.2 Personal information written in a tag

If the microchip in the RFID tag contains personal information of an individual stored in a given memory bank, then it is considered as repository of personal information. This could include, for example, the person's name and address, an identifier uniquely linked to a person, or biometric information, such as a fingerprint stored in digital form.

6.3 Unique identifier

An RFID tag containing a unique identifier has the potential to become a "proxy" for an individual when it becomes associated with that individual. In such circumstances, it will become personal information. This

would be the case with an RFID-enabled identification badge or uniform. Location data gathered by scanning tags associated with individuals is also considered to be personal information.

6.4 Tracking and profiling

Information about possessions (internet of things) that can be manipulated or processed to form a profile is personal information. This is the case whether the information is gathered through multiple visits to a facility or organization, or through access to a database recording activities of certain tags that were manipulated by an individual. A database could record information like the item's location, who moves or possesses it, and whether the movement is authorised or not. It may have the purpose of triggering an alarm if the movement is not permitted. All of this information would contribute to building a profile of an individual's activities.

6.5 Proportionality of wearable RFID tags

Without exaggerating, the capabilities and privacy risks associated with RFID tags worn by individuals (and certainly human implantable microchips (HIMs) or tags with sensors that are used or placed inside devices that are themselves implanted), are significant. Currently the far broader use is with tags that are worn by individuals but implantable microchips are marketed. Therefore we address tags that can be worn, in one form or another, which in some cases could result in tags being implanted. Application examples include:

— Access control tags, often worn on lanyards, carried by employees that have functions that are beyond general access to the workplace and are used for access control and monitoring of the employee's location within the workplace.

— Tags using active RFID protocols worn in certain occupations (firefighters, miners, others in safety-critical environments) where it is important to have a precise or last known location for rescue in an emergency.

— Tags (often active tags) worn by patients in medical institutions (e.g. new born babies as protection against kidnapping, mentally ill patients to provide them with freedom within the institution but to minimize the risk of escape and personal harm outside).

— Tags in uniforms and personal clothing with a prime function for control of laundry, but with systems creep could be used for monitoring the individual.

— Tags carried, or bracelets worn, by children in schools for access, registration and monitoring purposes. Notwithstanding the privacy issues within the application domain, if such tags remain readable beyond the application boundary then the privacy issues are greater.

— Bracelet tags worn by children in amusement parks with a prime function of addressing 'lost and found' situations, and also to monitor load distribution in the park.

— Although not worn by individuals, pets are often injected with RFID tags. As there is often a limited number of humans associated with a given pet, this can be considered as making the person identifiable.

In these examples there is some established infrastructure to be able to read the RFID tags in a manner specified for the application. In some cases (new born babies, children in amusement parks, firefighters and miners) the track and trace capability can often end at the physical exit or end of a duty shift. Other applications are more open-ended, like the use of employee badges and cards, which are generally taken out of the workplace to re-enter on another day.

There are applications where RFID tags are implanted in the human body. Increasingly artificial limbs are carrying AIDC technology, including RFID tags, for track and trace purposes when the patient requires an operation years later. There has long been talk of RFID chips being implanted in people purely for identification purposes. PositiveID (previously VeriChip), and its competitors, are much more focussed on developing RFID solutions for implantable RFID chips linked to sensors, for example to continually monitor glucose levels for diabetic patients. Such applications require an external RFID reader, and the RF component is to read data wirelessly from within the body.

Requiring employees, and others, to wear RFID tags may be only permitted if the reasons for doing so are legitimate and proportionate in a democratic and free society. Implanting employees with RFID tags against their will is unacceptable. If a less intrusive alternative to HIMs is available, which accomplishes similar objectives and provides similar security benefits, then that alternative should be used instead. Such activity raises fundamental human rights concerns, including bodily integrity. Employment should never be made contingent on a willingness to be implanted with an RFID tag.

Klitou (Klitou, 2012) argues that the quantity and scope of the location information collected and any other personal data associated with HIMs, or any other PLD or location-aware device for that matter, should be in line with the objectives and purposes for which the data was collected in the first place, as specified, for example, in a HIM purpose declaration attached to a standard or tailor-made service provider agreement. No more data than is required to fulfill the specified purposed should be collected and/or linked to the HIM, in accordance with both the principles of proportionality and data minimization.

6.6 Technical issues with unknown legal consequences

The potential privacy invasiveness of RFID applications with RFID tags and readers can be particularly serious, when significant infrastructural requirements have been realised like a dense network of RFID readers linked to databases in the back offices of organizations that deploy RFID applications.

As pointed out under 4.4, RFID data can be processed outside the application domain of the RFID operator by other operators.

The consequence is an RFID enabled item from one operator A being processed by another operator B without operator A's agreement, without the consent and knowledge of the data subject concerned and without the PIA assessment of operator B. An example of this is the social networking with the London Oyster card being used as an identifier. The eavesdropping of tags stimulated by readers that are compatible with the tag but not of the tag's application is another “spin-off”, as well the processing of data by non legitimate readers (e.g. RFID card skimming). Personal RFID apps create another class of problems. For example: scan the item and do a cheapest source search where the app has been purchased by the consumer or do this on home inventory apps.

The widespread deployment of RFID-enabled mobile phones with the capability of reading tags will increase the number of RFID readers in the global society with connections in the cloud. This creates two serious problems First, the information on the tags carried by the individual, can be read by any smart phone of which the bearer has no authority to do so. The second problem is that this capability creates an unforeseen legal (systemic) problem. The reader collects personal data from individuals and by doing so each user of this RFID reader enabled smart phone is no longer only a data subject but might become also a controller with all its legal obligations, for example to conduct a PIA and apply privacy by design.

This is an unforeseen problem and so far no solution has been presented by the legislators to cope with this problem.

7 Standards organizations and risk management standards

7.1 Standards organizations

Standards organizations have no legislative power. They are not part of government and don’t make laws or regulations. The legislative authority belongs to legislator being either the Parliament or, when delegated, to the State or the Crown. A standard is not a legal document (irrespectively of their rigor) and is not a law. Standards are voluntary consensus documents that are developed by agreement. Anyone can use such a standard, and its use is voluntary. A standard only becomes mandatory if it is referred to in laws or regulations. The legislator may stipulate conformity with a specific standard. In general, references to standards in laws and regulations may relieve the state and private parties of the responsibility for developing detailed technical specifications. Standards are one tool in a regulatory spectrum that may be applied by governments to provide a solution to a problem.

It becomes legally binding between parties if the standard has been a part of (mentioned in) an agreement between these parties. A CEN RFID PIA Standard may play a significant role in the jurisprudence. The judge may accept the CEN PIA standard as a particularisation of the general wording of the article or paragraph in the data protection legislation dealing with a PIA. The judge may also assume that the party using the CEN RFID PIA standard a prima facie shows due diligence. This may reverse the burden of proof of the party using this standard. The CEN RFID PIA standard may prevent legal disputes because it sets out unambiguous specifications and may provide legal certainty. Even where a CEN RFID PIA Standard is not expressly named in a contractual agreement, it can be used to settle legal disputes, especially when there isn't jurisprudence on RFID PIAs.

Contrary to consumer protection under the General Product Safety Directive 2001/95/EC where product safety standards support levels of acceptable risks balancing the practicalities of implementation with adequate levels of consumer protection, the privacy directives and the data protection regulation (DPR) don't recognise a level of acceptable risks for privacy violations or intrusion. The risks that are associated with the processing of personal data have to be avoided or when occurring have to be cured. The DPR therefore requires a data protection impact assessment (DPIA), Data Protection by Design and Data protection by default. In the Opinion 168 on *The Future of Privacy* of WP 29 is stated that "*The application of such principle (PBD) would emphasise the need to implement privacy enhancing technologies (PETs), privacy by default settings and the necessary tools to enable users to better protect their personal data (e.g. access controls, encryption).*"[1]

Why do standards matter? Because they matter for risk reduction by providing: (ii) persistent technical base with stable versioning for unstable business and technical requirements, (ii) evolving and converging standards for new and emerging business requirements, (iii) interoperable standards for diversity of business partners and technologies, and (iv) reliable, fixed terms of availability for the need for long term support [Gannon 2005]. Standards are living documents that reflect progress in science, technology and systems.

ISF [ISF 2007] states that organizations can use security standards to improve their information security policies, standards and procedures, measure the effectiveness of information security across the organization, raise awareness of information security enterprise-wide, develop or improve information security controls, comply with internal and external information security requirements, and undertake information risk analysis of important applications and systems.

Xiaolin et al. [Xiaolin 2008] state that in order to understand the present and future system risks, access the security threats and the degree of influence probably engendered from these risks, and provide the basis for security strategy identification, establishment and safe operation of the information system, many countries and organizations have established the risk assessment audit standards such as CC, SSE, CMM, ISO/IEC 1799, BS 7799, ISO 13335, IATF, and GB/T. Audit methodologies, especially within IT environments, and related governance and quality standards include ISA, CobiT, ITIL, ISO 9000, and ISAE 3402, while standards for internal audit and external assessments against adopted standards include ISAE 3402, ISAE 3000, CobiT, and ISO 9001.

7.2 Risk management standards

7.2.1 General

In the scope 1 of this document states: "The TR also proposes risk management control features based on the inherent capabilities of a number of RFID technologies that conform to standardized RFID air interface protocols".

There are already in existence standards for the management of information security, which are commonly accepted and publicly available specifications. From the variety of risk management and process improvement frameworks and standards to create an information security and privacy program that is sufficiently comprehensive and effective that are abound, prevalent standards in use at this time are briefly described in

[1] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

the ensuing subsections. Some of these standards have been used in the PIA to be discussed below, can be used in the PIA RFID process, and conform to standardized RFID air interface protocols.

7.2.2 AS/NZS 4360

The joint Australian/New Zealand AS/NZS 4360:1999 Risk management standard provides a generic framework for establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risk. It originated as AS/NZS 4360:1995, with Second edition 1999, and Third edition 2004. Detailed information about this joint Australian/New Zealand Standard can be found from the Standards Web site at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz. The AS/NZS 4360 risk management process has the following steps [ASNZS 1999]: 1) Establish the context, 2) Risk identification, 3) Risk analysis, 4) Risk evaluation, 5) Risk treatment, 6) Monitoring and review, and 7) Communication and consultation.

7.2.3 BS 7799 (ISO17799)

The BS 7799 (British Standard 7799: Code of Practice for information Security Management), evolved into ISO 17799:— The Information Security Standard. BS 7799 Part 1 became ISO 17799, then ISO 27002, while BS 7799 Part 2 remains a British Standard only and "forms the basis for an assessment of the Information Security Management System (ISMS) of the whole, or part, of an organization (http://www.itgovernance.co.uk/bs7799.aspx). BS 7799 (BS 7799-2:2005), which now has the international number ISO 27001:2005, is the international best practice information security management standard, defining and guiding Information Security Management System (ISMS) development.

7.2.4 NIST SP 800-30

The NIST SP 800-30 (Special Publications Risk management Guide for Information Technology Systems) provides practitioners with practical guidance for carrying out each of the three steps in the risk assessment process (i.e., prepare for the assessment, conduct the assessment, and maintain the assessment) and how risk assessments and other organizational risk management processes complement and inform each other. It also provides guidance on identifying risk factors to monitor on an ongoing basis, so that organizations can determine whether levels of risk have increased to unacceptable levels (i.e., exceeding organizational risk tolerance) and different courses of action should be taken. NIST (National Institute of Standards and technology) is a non-regulatory federal agency within the US Department of Commerce.

There are 9 steps for risk analysis in the NIST800-30: (1) system characterisation, (2) threat identification, (3) vulnerability identification, (4) control analysis, (5) likelihood determination, (6) impact analysis, (7) risk determination, (8) control recommendations, and (9) results documentation.

7.2.5 RFRM

The RFRM (Risk Filtering, Ranking, and Management Framework) [Haimes 2001] is, what the authors called a philosophical approach rather than a mechanical methodology, a framework to identify, prioritise, assess, and manage risk scenarios of large-scale system. The authors further explain qualitative screening of scenarios and classes of scenarios is appropriate initially, while quantitative assessments may be applied once the set of all scenarios has been prioritised in several phases. It has the following eight-phases [Haimes 2001]:

— ***Phase I, Scenario Identification*** - a hierarchal holographic model to describe the system as planned or success scenario.

— ***Phase II, Scenario filtering*** - filtering the risk scenarios according to responsibilities and interests of the current system user.

— ***Phase III, Bi-Criteria Filtering and ranking*** - filtering at the level of sub topics and moving closer to a quantitative treatment where the joint contributions of two different types of information - the likelihood of what can go wrong and associated consequences - are estimated on the basis of the available evidence.

— ***Phase IV, Multi-Criteria Evaluation*** - reflecting on the ability of each scenario to defeat three defensive properties of the underlying system, namely, resilience, robustness and redundancy using a set of 11 criteria.

— ***Phase V, Quantitative Ranking*** - filtering and ranking scenarios based on quantitative and qualitative matrix scales of likelihood and consequences, and ordinal response to system resilience, robustness, redundancy.

— ***Phase VI, Risk Management*** - performing identification of management options for dealing with the filtered scenarios and estimating the cost, performance benefits and risk reduction of each.

— ***Phase VII, Safeguarding against missing critical items*** - examining the performance of the options selected in Phase VI against the scenarios previously filtered out during Phases II to V.

— ***Phase VIII, Operational feedback*** - using the experience and information gained during application to refine the scenario filtering and decision processes in earlier phases.

7.2.6 COBIT

COBIT (Control Objectives for Information and Related Technology) IT control framework, created by the Information System Audit and Control Association (ISACA) (http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx). COBIT is a major information security governance model that provides a set of generally accepted measures, indicators, processes, and best practices for the use, governance, and control of information technology[2].

Wikipedia describes COBIT as process focus of COBIT is illustrated by a process model that subdivides IT into four domains (Plan and Organise, Acquire and Implement, Deliver and Support and Monitor and Evaluate) and 34 processes in line with the responsibility areas of plan, build, run and monitor, and has been aligned and harmonised with other, more detailed IT standards and good practices such as COSO, ITIL, ISO 27000, CMMI, TOGAF and PMBOK.

7.2.7 HIPAA

HIPAA (Health Insurance Portability and Accountability Act) addresses privacy concerns of health information systems by enforcing data exchange standards. Abu-Nimeh and Mead [Abu-Nimeh 2010] describe the overall objective of a HIPAA risk analysis as the documentation of the potential risks and vulnerabilities of confidentiality, integrity, or availability of electronic protected health information and the determination of the appropriate safeguards to bring the degree of risk to an acceptable and manageable level. There are 7 steps involving in HIPAA risk assessment.

1) Inventory and classify assets

2) Document likely threats to each asset

3) Vulnerability assessment

4) Evaluate current safeguards (administrative, physical or technical)

5) Document risks

6) Recommend appropriate safeguards

7) Create report of results

[2] www.isaca.org/Template.cfm?Section=COBIT6

7.2.8 ITIL

ITIL (The Information Technology infrastructure Library) v.3 service management framework is a set of concepts and techniques for managing information technology infrastructure, development, and operations[3].

7.2.9 ISMS

ISMS (An Information Security Management System) is a set of policies concerned with information security management. It includes mechanisms to design, implement, review, measure, and maintain processes and systems that ensure the confidentiality, integrity, and availability of information assets while striving to minimize information security risks. “ISMS is a proactive approach to continuously and effectively manage, at a high level, information security including people, infrastructure and businesses. The goal is to reduce risks to manageable level, while taking into perspective both business goals and customer expectations.”[4].

7.2.10 ISO/IEC 27001

ISO/IEC 27001: The ISO (International Organization for Standardization)/IEC (International Electrotechnical Commission) 27001 standards is a major information security governance model that outlines the requirements to design and implement ISMS. As with all management processes, an ISMS shall remain effective and efficient in the long term, adapting to changes in the internal organization and external environment. ISO/IEC 27001 therefore incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming cycle, approach: See http://en.wikipedia.org/wiki/Information_security_management_system. Modeling an information security governance program using this standard will provide organizations with an auditable, measurable, and comprehensive framework that promotes strategic planning and continuous improvements.[5]

7.2.11 ISO/IEC 27002

ISO/IEC 27002: ISO 27002 is the common name for a comprehensive set of best practices used in establishing and managing ISMS. The full name is ISO/IEC 27002:2005 – Information technology – Security techniques – Code of practice for information security management. It describes “should do’s,” and establishes guidelines and general principles for initiating The 36 control objectives and 133 controls outlined provide general guidance on the commonly accepted goals of information security management.[6]

7.2.12 ISO/IEC 27005

ISO/IEC 27005 (Information technology -- Security techniques -- Information security risk management) is an International Standard that provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements of ISMS according to ISO/IEC 27001 but does not provide any specific methodology for information security risk management [ISOIEC 2007]. The standard describes the information security risk management process that consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review. The standard also encourages iterative information security risk management process for risk assessment and/or risk treatment activities, which can increase depth and detail of the assessment at each iteration and provide a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that high risks are appropriately assessed.

7.2.13 ISO/TR 13335

ISO/IEC 13335-2: Management of information and communications technology security - Part2: Information security risk management. ISO/IEC IS 13335-2 is an ISO standard describing the complete process of

---

[3] www.itil-officialsite.com

[4] http://www.cccure.org/Documents/ISMS/isms.pdf

[5] www.iso.org/iso/catalogue_detail?csnumber=42103

[6] www.iso.org/iso/catalogue_detail?csnumber=50297

information security Risk Management in a generic manner, and can be viewed at as the basic information Risk Management standard at international level, setting a framework for the definition of the Risk Management process. It supports risk identification, risk analysis and risk evaluation risk assessment phases. The risk management phases include risk assessment, risk treatment, risk acceptance, and risk communication [ENISA 2006].

8 Legal supported PIA methodology

8.1 Background information

In Australia, Canada, New Zealand, The United Kingdom and the United States are principal guidance documents at national level, in some countries since 2000. These countries are the only ones that recognise in the legislation or related regulation PIAs as a tool to safeguard privacy. PIAs are targeted at the government and, with the exception of the US, also to the private sector. Only a few PIAs (approx.20) have been widely published in full with the exception of vulnerable data security information

Each PIA guidance document can be considered as a methodology and fulfills the criteria of a methodology[7)].

— It comprises a number of subsequent steps;

— The result of each of the steps serves a specific goal and will produce well defined results;

— The result of each step can be validated by independent auditors;

— The number of sources used in each steps is limited;

— The expertise necessary to perform each step is homogeneous and requires a limited number of different experts;

— The sequence can be repeated starting from any of the intermediate products to improve the overall result.

In these countries PIAs are mandatory for certain issues. In New Zealand PIAs are mandatory for systems collecting and handling biometric data, in Canada for federal departments and agencies with funding submissions, in the UK for government agencies and in the US for all new or substantially changed systems that collect. Maintain or disseminate personally identifiable information.

In Australia, New Zealand and the UK PIA guidance has been prepared by the privacy commissioner. In Canada the Treasury Board and in US the Office of Management and Budget have prepared the key PIA guidance documents.

PIAs are applicable to all technologies. Only the Privacy Office Official Guidance of the US department for Homeland Security mentions the use of PIAs specifically technologies with privacy implications, i.e. RFID, biometric scans, data mining and geospatial tracking.

The privacy targets of the PIA are based on the privacy principles.

In all countries PIA should be initiated at the early stage of project development before decisions are taken and collaboration of external stakeholders, program managers, technical specialists and privacy and legal advisors. PIAs are considered as a form of risk management and focus on privacy risks involving personally identifiable information also known as informational privacy. The Australian and UK PIA handbook don't rule out other forms of privacy than informational privacy, i.e. physical (bodily) privacy, privacy of personal behavior, privacy of personal communications and spatial privacy.

7)From T.W. Olle et all, Information Systems Methodologies: A Framework for Understanding, Boston1988

Buttin and others have pointed out that PIAs and accountability are considered dual in some sense - PIA occurs before the deployment of a system whereas accountability applies by definition to a running system- and strongly tied, in the sense that PIAs should lead to measures to make accountability possible

Definitions and methodologies for PIAs vary considerably in the countries mentioned above. In all countries the PIA guidance contains a set of privacy principles. In Canada these principles are based on the Code of Fair Information Practices in the Federal Privacy Act and the personal Information and Electronic Documents Act, while in the UK the PIA guidance is based principles derived from on the 95/46/EC and other privacy Directives. For Australia and New Zealand PIA guidance is based on similar privacy principles and privacy legislation. In the US the picture varies either the PIA guidance doesn't mention the privacy principles or it refers to Fair Information Practice Principles. The privacy principles are at the basis of the privacy protection legislation.

Only the US put primarily emphasis on compliance. The other countries mention the importance of compliance with laws, regulations and/or codes of practice, but consider the PIA's primary purpose to identify risks to privacy and ways of dealing with those risks.

Generally speaking the scope of the PIA is to consider all dimensions on the privacy of the individuals, not merely the privacy of personal information (data protection).

The PIA guidance in all mentioned countries contains a template for preparation of the PIA report and provide a set of questions either for consideration during the PIA process. Australia, The UK and US accept that PIAs are scalable i.e. no one size fits all, while in the other countries the template is leading. The PIA policy in Canada and the US provide for review (auditing) by third parties. In Canada government institutions shall ensure that the PIA is sent to the Privacy Commissioner.

Australia and New Zealand advocate publication of the contents and findings of the PIA report, but doesn't require it with the exception of PIAs in relation to the New Zealand immigration Act concerning the processing of biometrics. These PIAs should be published on the website of the Privacy Commissioner.

All countries opinionate that the PIA report may need to be revised and updated or a new PIA process undertaken when system are changed and updated.

The fact that a PIA guidance document has been published and actively supported by the Privacy Commissioner or Data Protection Authority has had considerable influence on the use of PIA within the jurisdiction of that Commissioner.

The PIA process in Canada is from a legal perspective the most elaborate of all PIA methodologies supported by the Privacy Commissioners.

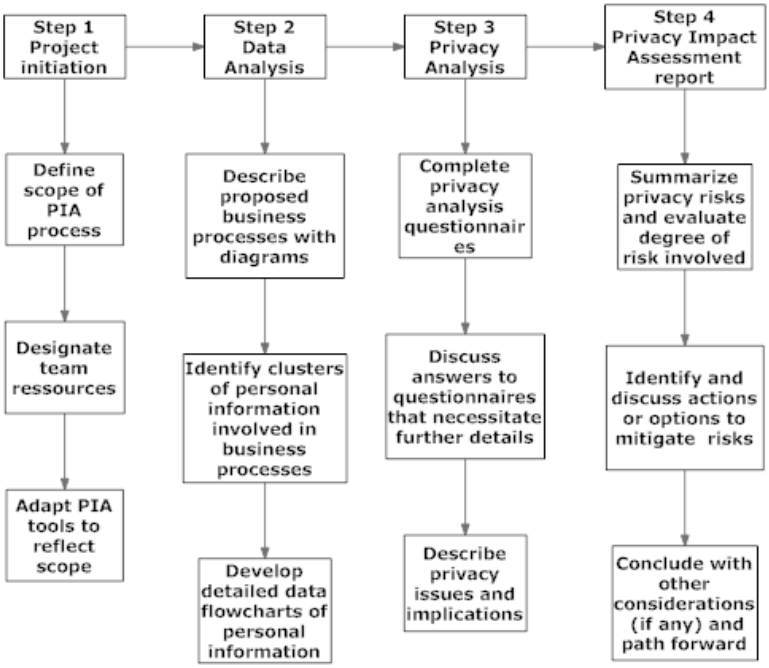


Figure 3 — PIA Process as developed by the Treasury Board of Canada (2007)

8.2 Analysis of five PIAs

In order to get valid results that are repeatable only PIAs that fulfill the criteria of a methodology (Olle 1998) have been analyzed. One time PIAs that follow a process that hasn't been tested over time are considered methodologically not to be stable enough over a longer period and can't be a candidate for using it as a proven approach. Five PIAs have been analyzed:

a) Privacy Impact Assessment on Google's collection of unsecured WiFi payload data in Australia using Street View vehicles;

b) Privacy Impact Assessment on Enhanced Driver's License (EDL) in Canada; A RFID chip has been implemented in the EDL card;

c) Privacy Impact Assessment on the utilisation of license plate readers in USA;

d) Privacy Impact assessment on the Collection and Handling of Biometrics at the Department of Labour in New Zealand;

e) Privacy Impact assessment on the Use of Smart Metering Data by Network Operators in United Kingdom.

f) All of the discussed five PIAs in this Technical Report qualify for a level 3 full scale PIA discussed under 8.1.

8.3 Findings

8.3.1 The application operator perspective

a) With the exception of the Google PIA, All analyzed PIAs offer a prospective identification of privacy risks **before** systems and programs are put in place.

b) All PIAs takes into account the market and societal expectations and values about privacy.

c) All PIAs refer to an entire process of assessment of privacy (and security) risks from begin to end to prevent problems around the weakest link.

d) The scope and depths of the PIAs is dependable on a number of crucial variables, like the sensitivity of the personal data involved, the perceived risks, the intrusiveness of the technology etc.

e) Legal and information technology knowledge is required in order to conduct and produce an adequate PIA.

8.3.2 The consumer and public interest perspective

a) All relevant privacy protection perspectives have been covered in the five PIAs discussed above.

b) The PIA reports follow the Privacy Impact Assessment Guides/Handbooks of the Privacy Commissioners. At least five key stages in the PIA report are of importance: A. Project description: Broadly describe the project, including the aims and whether any personal information will be handled.

   A. Mapping the information flows and privacy framework: Describe and map the project's personal information flows and document all relevant legislative and organizational rules.

   B. Privacy impact analysis: Identify and analyze the project's privacy impact.

   C. Privacy management: Consider how to manage any privacy impact, particularly options that will improve privacy outcomes and still achieve the project’s goals.

   D. Recommendations: Produce a final PIA report covering the above stages and including recommendations.

c) Following the established methodology by the Privacy Commissioner or Data protection Authority, having binding jurisdiction, will create legal certainty for all stakeholders involved.

d) The process (information flows) and the used technology is analyzed *in extenso*, from the start to the end inclusive the processing of the collected data in the backend system.

e) All elements in the process have been considered individually and as a whole assuring the privacy safe handling of data collected, processed, disseminated and stored.

f) All PIAs focus is on privacy protection in the legal sense of the word. Information security is just one of the elements. It is noticeable that processes and used technologies have been analyzed and that measures have formulated to minimize not only legal risks but to address community expectations on privacy and concerns in a positive and constructive manner. The PIAs have a broad scope in relation to the perspectives reflected in the process, taking into account the interests not only of the organization, and of the strategic partners/ stakeholders, but also of the population segments affected by it.

g) The PIAs focused both of problems and of solutions to them. The PIAs have proposed or actually have changed the privacy management structure. In several PIAs training of employees and promotion a privacy oriented communication strategy is considered essential. Involvement and commitment of the employees and stakeholders is considered a necessity.

h) The Google PIA wasn’t anticipatory. It was executed after lots of negative publicity and legal action from the Privacy Commissioner.

i) The analyzed PIAs were time consuming and extensive and required legal and technological expertise.

8.4 Audit report on the use of wireless technologies

Of particular interest is the audit report on the protection of personal information in a wireless environment that the Privacy Commissioner of Canada (PCC) issued in 2010. It shows that a PIA can be subject of a privacy audit by the Data Protection Authorities.

The objective of the audit was to determine whether the selected entities (Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada) had adequate controls – including policies, procedures and processes – to protect personal information transmitted and stored within wireless environments.

PCC examined the security frameworks surrounding wireless networking and the use of portable wireless devices. They found that risks and threats have not been formally assessed, although PIAs had been drafted. What was missing was a Threat and Risk Assessment (TRA) that defined the threat environment, evaluated the associated risks and that recommended mitigating actions to address identified vulnerabilities. The assessment of the PCC also validated that the minimum standards required under Treasury Board policy are appropriate for the type of information being transmitted and stored within a wireless environment.

The criteria used to conduct the audit and assessing the risks were derived from the Canadian Privacy Act, relevant treasury Board policies, generally accepted privacy practices, IT Governance Institute, control objectives for information and related technology (CoBit® 4.1) and the information technology infrastructure library (ITIL) Framework.

9 Proposed methodologies for RFID PIA process

9.1 Initial Decision Tree

The Recommendation of the European Commission dated 12 May 2009 has been followed up by the Privacy and Data Protection Impact Assessment Framework for RFID applications of 12 January 2011. In this Framework the PIA process has been described to provide guidance to RFID Application Operators for conducting PIAs on specific RFID applications. It presents a decision tree on whether and at what level of detail to conduct a PIA.

Some companies are RFID operators in the sense of the Framework but don't need to execute a PIA because they simply don't process RFID data for personal data processing or profiling (De Hert, p.329). For example: a farmer using RFID for tagging his cattle. However when his cattle is going to the slaughterhouse the RFID will be used to track the meat of his cattle to the farmer for health reasons. The key question at start of the analysis is whether the RFID application actually process personal data or whether the RFID application links RFID data to personal data for example through a data sharing network at the back-end.

The 2011 PIA framework supports the use of sector- or application specific guidelines (templates). These guidelines can provide detailed suggestions for applications and sectors (privacy targets, threats, risks, controls).

Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications points out that:

The PIA process is constructed in two phases:

a) A pre-assessment phase that classifies an RFID application according to a 4 level scale, based on a decision tree. The result of this evaluation allows to determine if a PIA is required or not, and to choose between a "Full Scale PIA" and a "Small Scale PIA". Applications that use RFID tags that are likely to be carried by individuals will require at least a "Small Scale PIA" (level 1), while applications which further process personal data will require a "full scale PIA" (level 2 and 3). Conversely, applications that do not use tags that are likely to be carried by individuals and do not further process personnel data are not subject to a PIA (level 0).

b) A risk assessment phase that is broken down into 4 main steps:

1) Characterisation of the application (data types, data flows, RFID technology, data storage and transfers, etc.).

2) Identification of the risks to personal data, by evaluating threats, their likelihood and their impact in terms of privacy and compliance with European legislation.

3) Identification and recommendation of controls, in response to previously identified risks.

4) Documentation of the results of the PIA, establishment of a resolution regarding the conditions of implementation of the RFID application under review, and information concerning residual risks.

Each step in the risk assessment phase is further supported by elements provided in the annexes of the Revised Framework and designed to provide guidance to the reviewer with:

i) A template to describe key characteristics of the RFID application.

ii) A list of 9 privacy targets for the RFID Application, derived from Directive 95/46/EC.

iii) A list of typical privacy risks, with descriptions and examples.

iv) A list of examples of controls and mitigating measures that can be used in response to previously identified risks.

The result of a PIA is formalised by the RFID application operator in a PIA report, which describes the RFID application and documents the details of the 4 risk assessment steps referred above.

9.2 Critique on the initial decision tree

Below is the decision tree from the PIA Framework document, but overlaid with two colored boxes.

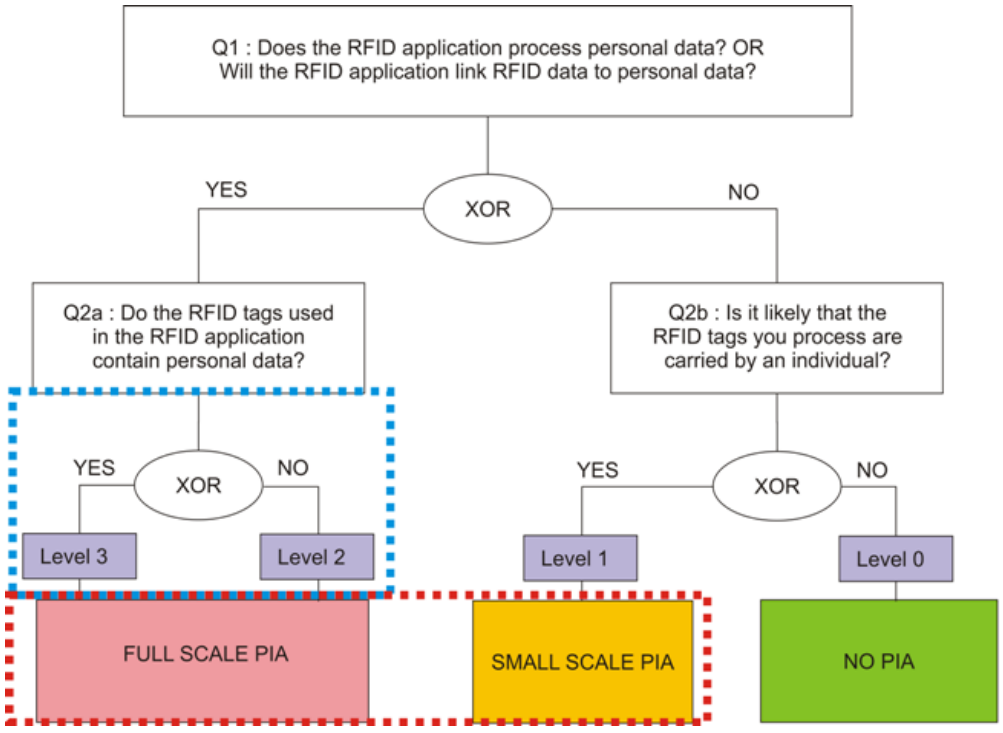


Figure 4 — Initial decision tree on PIA necessity and scope overlaid with two colored boxes

"Personal Data" as defined by the Directive 95/46/EC (Article 2) 'shall mean 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'.

NOTE A"RFID Application" is a system that processes data through the use of tags and readers and which is supported by and part of a back-end system and a networked communication infrastructure.

The box with the blue boundary shows that as both Level 2 and Level 3 point to a full scale PIA that either the XOR decision is not required or that there is some other distinguishing feature between these two levels. This can be found – it is a bit "implied" – in the text about the full scale PIA, which is placed before the decision tree.

Whatever the outcome of the XOR yes/no question at moment personal data directly or indirectly occur in the RFID tag, reader or application the principles of data protection shall apply in full to any information concerning an identified or identifiable person. This also the fact for the question concerning the tag carried by an individual. Therefore a level 1 small scale PIA is very misleading. The law is fully applicable on a level 1 situation. Both require what is in effect a risk assessment of the access to the back-end system. Level three requires a risk assessment of the tag when in the public domain. We have seen a total failure of this with, for example, the contactless payment cards. The box with the red boundary is there to illustrate that the PIA Framework fails to distinguish between what is a small scale and full scale PIA. A full scale PIA is in practice always required.

9.3 Relevance of the 2011 RFID PIA Framework

9.3.1 General

The Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications - Adopted on 11 February 2011 has been identified as a key input to the CEN RFID Privacy Impact Analysis process and methodologies project being undertaken by Project Team C for the Mandate M436 Phase 2.

9.3.2 Framework reviews by others

The Article 29 Data Protection Working Party reviewed the 2011 RFID PIA Framework and passed two significant opinions on the Framework.

— The structure of the qualifying decision tree would lead on many occasions to the miss qualification of applications as level 1 when they should be qualified as level 2 applications in line with their Opinion 10/2010.

— This version of the Framework had addressed a key concern raised about previous versions in that it now requires RFID Operators to evaluate the risks when tags may be used outside the operational perimeter of an RFID application.

9.3.3 Scope of work for the 2011 RFID PIA Framework

9.3.3.1 Data Protection and privacy

The 2011 RFID PIA Framework was focused on the RFID applications and as a result makes use of much established Data Protection privacy analysis.

For example

— Of 9 privacy targets in Annex II, 8 targets are Data Protection application only requirements while 1 target relates to the peripheral technology design;

— Of the 15 privacy risks in Annex III, 14 of the privacy risks relate to the Data Protection and only to the application, while 1 privacy risk relates to the peripheral technology design.

9.3.3.2 Privacy beyond the application perimeter

When the use of tags outside the operational perimeter of an RFID application is addressed within the 2011 RFID PIA Framework, it is through discussion within Step 2 of the Framework. There it has established that there are criteria for removal of tags when a risk outside the operational domain of the application "… is likely and actually materialises into an *undismissable* risk …".

It should be noted that while the need for tag removal is addressed in the 2011 Framework, those risks that may be less than this undismissable level of privacy risk are not discussed, though residual risks are mentioned.

In contrast, the Recommendation Paragraph 5a states:

> … operators, notwithstanding their other obligations pursuant to Directive 95/46/EC: conduct an assessment of the implications of the application implementation for the protection of personal data and privacy, including whether the application could be used to monitor an individual. The level of detail of the assessment should be appropriate to the privacy risks possibly associated with the application.

This implies that all risks need to be considered, but that the detail of the assessment process should be commensurate with the application. A serious point that needs to be considered is that tag removal is not a relevant consideration where the RFID tag or card has to be used repeatedly.

To summarise: The EC PIA framework is based on the risk management approach defined in ISO/IEC 27005. This approach requires covering all use cases and business processes – also those that are not executed in the operators premises.

9.3.3.3 SME issues arising from the 2011 RFID PIA Framework

As RFID use grows, the number of occasions will increase when small companies receive RFID identifiable items via their supply chains when the SMEs themselves have no RFID application or readers.

Examining this scenario with the 2011 RFID PIA Framework :-

The PIA level qualification questions that would be very likely to be used by inventory and distribution application operators who supply such businesses are Q1 and Q2b as follows :

— Q1: Does the application process personal data or will the application link RFID data to personal data ? The most likely answer would be NO leading to

— Q2b: Is it likely that the RFID items that you process are carried by an individual? The use of English in this question creates focus on the application operation and not on potential use beyond the application. This is may well to lead to application operators for supply chain applications answering NO i.e. level 0 no PIA required.

In the context of the application operator the items are not carried by individuals but on pallets or they are held in storage areas. This leads to the real possibility that tagged items could be supplied to small retailers who are not application operators themselves, and as a result these businesses could act as a path to the public for tagged items for which no PIA has been undertaken. The situation is further complicated by global supply where the originating producer who tags the item may be outside the EU.

9.3.3.4 Processes associated with Privacy Impact Assessment processes

The 2011 RFID PIA Framework includes within section 1.2 internal procedures such as organizational responsibilities, design review and sign off, stakeholder consultation and a number of factors for PIA administration.

9.3.3.5 Focus on Mandate M436 Phase 2 PIA process

Mandate M436 Phase 2 places more focus on a comprehensive procedure, as stated in the requirements for EN 16571: AIDC technologies – Information, privacy, and data protection aspects of RFID – RFID privacy impact assessment (PIA) process:

> The aim is for this EN to be cited as the definitive procedure for conducting a PIA with the RFID and related technologies defined within its scope.

The EN should cover all aspects of an RFID system including data encoded on the RFID tag or card, wherever it might be readable, both in an application that is subject to a PIA and data capture risks beyond such a boundary at the periphery of the application.

The process should include assessment of risks due to the use of RFID technology at the periphery where that RFID design has significant implications for the application risks. For example loss or leaking of central data records that include, or link to, RFID data.

The PT-C scope for the final European Standard (EN) has common elements with the 2011 framework specifically where the 2011 Framework outlines risk assessment analysis and methodologies keeping in mind that the PT-C scope is focused on the entire scope of RFID technology rather than just the application.

9.3.3.6 Conclusions

a) The EN for RFID peripheral privacy impact assessment needs to clarify or provide different and improved approaches to that of the 2011 Framework decision tree qualifying questions for PIA levels. Initial review of application implementation" as first step of the PIA-flow is required.

b) The EN will need to address standardized threats and vulnerabilities analysis for the air interface radio technology. Threats, vulnerabilities, etc. have to be seen in the specific context of an implementation.

c) Application data protection threats and vulnerabilities are out of scope unless the design of the periphery has a direct influence on the impact of these.

d) The EN will need to include tag and reader threats and vulnerability analysis that has not been addressed by the 2011 RFID PIA Framework

e) The EN will need to include networks threats and vulnerability analysis that has not been addressed by the 2011 RFID PIA Framework

f) The EN will need to address the 'outside the operational perimeter' aspects more fully than the 2011 RFID PIA Framework.

g) It should be noted that threats, vulnerabilities, etc. for all relevant components have to be identified in the specific context of an implementation based on the individual processes, uses cases and data flows

10 The reasoning for addressing the privacy assessment at the periphery for RFID

10.1 The role played by RFID in the lives of individuals

10.1.1 The nature of RFID possession by individuals

RFID has been used or proposed for a very wide range of applications that require private individuals to carry or possess items that are RFID identifiable and where the RFID technology carries a wide range of data for processing by the relevant applications.

The nature of personal possession of RFID has been categorised into the following types:

— possession by an individual on a day to day basis as they go about their daily lives. Examples being e-tickets, contactless credit cards, clothing, car wheels, drivers' licences and so on;

— temporary possession for hours, or a few days at most, for items such as groceries and consumables;

— long term possession of a non portable nature, for example household appliances.

10.1.2 The degree of exposure to RFID risks

When an item with an RFID tag possessed by an individual interacts with readers for an application then data protection based privacy assessment applies. For the rest of the time the item is away from the read range of the defined application's readers and the tag is in an uncontrolled enviroment where any type of reader and tag interactions are possible and threats to privacy need to be assessed.

An example of a highly used RFID technology item is a contactless payment card which can be expected to be used many times a day with each reader interaction taking only seconds. A guidline for the total application usage time for such high usage applications has been taken as approximately 5 min total application use time per day. It is during this 5 minute period that Data Protection applies in practice while for the rest of the time the human right to privacy applies.

The risk exposure guidelines are:

— Data Protection risk exposure time 1 % (i.e. 5 min use a day out of 24 h) where controlled application – reader – tag interaction occurs.

— Non Data Protection risk exposure time 99 % where uncontrolled reader interactions can occur.

Conclusions:

— The RFID PIA process should be capable of dealing with items that are regularly carried, those that are only temporarily possessed and those that remain in significant privacy locations like the home for sustained periods of time but are not carried by individuals.

— The RFID PIA process should ensure that the stand alone privacy protection provided by tags is evaluated for the 99 % exposure time domain whwere the tags are away from application operator readers.

10.2 Where RFID technology is the determining factor for privacy assessment

10.2.1 The Privacy assessment technology layers

10.2.1.1 Technology layers

When an application is interacting with a tag then data flows in both directions through many layers of technology. The ISO/IEC 27000 series of standards and guidleines on security in depth help to indentify the following layers from the periphery inwards:

— Tag and tag data

— Air interface protocol

— Reader

— Device interface protocol

— Network

— Middleware

— Application software and application data

— Central system security – of processing and data storage

10.2.1.2 Tag data

With the great majority of risk exposure time being that when the tag is stand alone away from application readers it is worth considering tag data separately within the technology layers.

The data held on tags can be minimal as with most retail products where only an identification number is used and all the other application data is held centrally. On the other hand other RFID use such as travel cards may hold considerably more data and use much more capable tag designs.

The following is information that may, for example, be held on a London Transport Oyster travel card. This information was obtained by a UK Freedom of Information request in 2008 and published on the Internet via http://www.whatdotheyknow.com/request/data_stored_on_oyster_cards.

Oyster card tag data:

Generic Card Data:

— Identification number of the card,

— Pay As You Go (PAYG) Balance,

— Passenger type,

— type of discount,

— Photocard identification number if applicable,

— Staff identification number if applicable,

— the deposit value,

— Registration flag.

— PAYG top up Data: Date, Time, Location, and value added.

— Ticket Data: Type of ticket, start and expiry date, and time restriction if applicable.

— Transaction Data: Date, Time, Station number or bus route, and fare charged.

The data set is not complete as the information providers observed that “TfL is not obliged to supply some of the information you have requested, as it is subject to the following statutory exemption to the right of access to information”

10.2.2 The role of RFID technology in privacy assessment

The effects of RFID on privacy are as follows :

Tag – the tag’s design and the data held on it are highly significant

Air interface – this is wireless and varies in robustness between different protocols, but all are vulnerable to ad hoce reading using commercially available readers, and more sophisticated eavesdropping devices as addressed in CEN Technical Report: RFID threat and vulnerability analysis

Reader – the reader infrastructure and it’s lifetime before being changed is key to determining what tag protection can be implemented.

Device interface – defines the means that the application and reader communicate. Few protocols are standardised, so the obscurity of a vendor-specific can be considered contributing to security, but as this has to be declare in product specs, the weakness exists. As more handheld readers are introduced (including smartphones) then the wireless nature of the device interface will open new risks.

Network – if direct dedicated links are not used to connect readers back to the core application software then the accessibility of the network plays a key role in securing RFID data transfer.

Middleware – defines all the software, and sometimes hardware, layers between the RFID reader and application and covers both the instructions to the readers and the processing and interpretation of data from the tag and reader. A key function includes filtering (selecting relevant tag data) but this need not be as crude as reading all the data and /or all the tags and discarding those not relevant, it can also be implemented by selective reading and discarding transmitted data at the air interface level. This does stop unnecessary capture of data. Another function is to interpret the bytes encoded on the tag into a format that is meaningful to the application, and conversly to encode them in a known and memory efficient manner. Unless the encoding is subject to dynamic encryption, then the raw bytes have a one-to-one relationship with their interpretation and – depending on the data – will remain identifiable whatever the middleware does to achieve encoding. Where details of the encoding rules and other middleware features are in the public domain – vital for open systems – then the rules are also available to anyone. Even when rules are not known, encoding rules can be "cracked" as with any coding scheme.

Application software and data – this is a key area where non senitive data from a tag could be associated with other more sensitive application data to create linkability of tags to individuals.

Central System security – of processing and data storage. This plays a key role in securing the application data and that is significant to RFID privacy if the RFID data itself is personal data or if the application creates linkages that in turn create personal data.

10.3 Privacy assets

Contrary to privacy threat analysis that the roughly answers the question in what way damage can be expected, asset identification answers the question what material or immaterial subject can be damaged. Both

approaches are necessary for the selection of countermeasures. An asset indicates the things that are really of precious and prime value to a private person.

ISO/IEC 27005 makes good use of asset valuation to assist with the assessment process for an organization's data security. However that is not the same as an individual's privacy and so the questions above have been addressed :

What is to be assessed ?

The individual's privacy when the RFID technology is involved

What is to be protected ?

ISO/IEC 27005 provides a number of features that add procedures, metrics and more precision to security risk assessment. Adapting ISO/IEC 27005 to RFID privacy would offer two advantages:

— It provides a defined and tested methodology as the platform on which to build an RFID PIA process.

— It enables RFID operators and data controllers, particularly in larger organizations, who are already implementing ISO/IEC 27005 for security purposes to gain a 2transfer effect" to address RFID privacy.

RFID technology is attached to or embedded in items possessed by individuals. These are the physical assest associated with an RFID privacy impact assessment, but they are not the source themsleves of the privacy concerns or intrusion. The source of concern is the revealing of personal data from an RFID application in the 1 % exposure domain and revealing of personal data from a tag in the 99 % exposure domain.

Conclusion:

— The tag data and the degree to which appropriate protection is available are very significant to RFID privacy impact assessment.

11 The case for a cost-effective PIA process

11.1 Templates

Organizations want to keep the costs of PIAs down. Consumers want PIA standards to have a high take up which won't happen if the process and methodologies are costly. The PIA framework already identifies the potential benefit of having a sector-based or application-based template structure to contribute to this process. There are additional dimensions that need to be considered for such templates:

— They should not be too broad in scope, for example it would be wrong to assume that all retail applications could be addressed by a single template, but common features such as the use of GS1 EPCglobal systems can make a significant contribution.

— Application-specific templates need to be considered based on functionality that might apply across many sectors. Two obvious examples are contactless payment cards and employee ID badges for access control. In the former example there are already established organizations like EMVco, whereas in the second case solutions are often vendor-specific.

— The nature of what constitutes a template should not be prescriptive; it could be as simple a a generic application description, with added analysis of the privacy asset implications of data elements used in a sector, to a complete set of tools to enable the PIA to be undertaken by each individual RFID operator.

— If individual RFID operators are to benefit by the cost reduction of the process, then the sector or application based tools should contribute more resources to the process than that of an individual organization. In other words, the sum of the effort should exceed the efforts required by an individual

organization. This can be achieved, and still be cost effect for all that benefit from the template, by for example undertaking a deeper risk assessment.

— Users will benefit from a more in-depth sector or application level of risk assessment, but will have the additional benefit of consistency in the PIAs undertaken in the sector or for the application.

— It also needs to be recognised that the skills required to understand the privacy implications of RFID are often not well understood. At one level there are citizens that consider that the technology is like GPS and the tag can be read from space and not from a reader that is reasonably close to a person. At the other extreme is the focus on the functional and operational aspects of the technology paying little regard to the privacy implications. While the development of a template might result in increased knowledge, we address other tools below.

— The existence of a PIA template enables it to be reviewed and revised based on new knowledge about the risks of the technology in a particular application or sector.

— The mechanism and organizational structure to develop a template also opens up greater opportunities for user stakeholders to be involved by consultation or participation, probably more so than when an individual RFID operator is completely responsible for undertaking the PIA.

11.2 Understanding the technology

It is probably true that until work on the recommendation began, privacy was the purview of a few that sometimes exaggerated the issues, or of technology experts focused on incorporating security features for some high value applications. The Recommendation brought with it a need to understand the technology. However, this and other Technical Reports that are being delivered as part of M436 show, the knowledge is not widespread. The issue is not about security nor only about the data protection issues within an RFID application.

The challenge therefore is whether any rigorous process can be developed that de-mystifies the technology and brings a consistent approach to privacy features. The work by Project Team B developing CEN/TR 16672 *Information technology - Privacy capability features of current RFID technologies* provides such a platform. Although it addresses all the main air interface protocols, there are so many optional features in the standards that it is necessary to consider individual products. We consider that the TR provides the basis for what could be called ***privacy capability statements*** to be made by manufacturers of RFID chips, tags, and readers. This only needs to be done once and becomes relevant to all RFID applications that make use of the particular product. Again this is a cost-effective way for the RFID vendor community to contribute to a cost-effective Pia process and to provide consistency to the process. Participation by vendors should provide a factual base on which to build trust in the technology and increase the use of RFID – itself an acknowledged benefit in the Recommendation.

The issue then arises on how such privacy capability statements are made available. Our proposal is that a Registration Authority (RA) is established by CEN with the responsibility of collecting and publicly publishing the statements. The RA should also be responsible for reporting to the appropriate standards committee of manufacturers that are not contributing to the process.

The publication of privacy capability statements is seen as a key tool to enable RFID operators and those preparing templates to have the facts readily available whether a particular product offers a countermeasure to a particular RFID threat.

11.3 Monitoring RFID threats and vulnerabilities

Our research has identified a significant number of potential threats and vulnerabilities that can be applied to the risk analysis methodology adapted from ISO/IEC 27005 and shown in Table 1. Many have been identified from literature and considered relevant. Only time will establish whether Threat A is more prevalent than Threat B, which will be expressed in terms of vulnerabilities. As such a threat is not applicable (because of the technology) is possible (based on research papers), ar at worst has been exploited based on evidence.

Such evidence will evolve over time and a missing piece of the jigsaw is a method to monitor what will happen in future with an expanding and evolving RFID application base. With IT systems there are established alert systems, such as US-CERT bulletins[8)] that provide updates of vulnerabilities and the patches to fix them. As with the embryonic CERT-EU[9)] the focus is largely on cyber-security. However there have been some instances, particularly associated with smart cards, where US-CERT has identified and published details of vulnerabilities.

The scale of the US-CERT operation, combined with the fact that software patches are easier to develop and implement than changing the design of an RFID chip, suggests that at best this is an outline model and not a structure to emulate for RFID privacy. A different model might be using the various DPAs in Europe that when a privacy issue associated with RFID is reported that it shared, or notified to the RA that is proposed for managing and publishing the privacy capability statements (see 10.2). This would also have the advantage of closing the loop by:

— continual improvement of specific products,

— identifying issues that could be relevant to similar products,

— enabling specific research to be undertaken to better quantify the risks.

This would be far more methodical and engineering based than the proposed solution for one smart card vulnerability on the US-CERT site, which simply stated "Replace the smart card".

11.4 Assisting the SME PIA process

The obvious way to help an SME RFID operator is by a relevant body developing an appropriate template. However this might not be practicable for many reasons: the RFID operator might not be a member of an organization representing similar operations, or such a membership body might not have the competence and skill to undertake the development of a PIA. It is also important to recognise that many European system integrators offering RFID solutions themselves fall within the SME category. While they should have more knowledge about RFID, they will lack the expertise about the application other than the basic operational requirements to develop and RFID solution based on operational requirements and not on privacy requirements.

Recognizing that an SME RFID operator that is aware of, and willing to undertake, the RFID privacy impact assessment some means of simplification is required. The assets in an RFID risk assessment are relatively few and easy to identify. What is more relevant are the number of potential threats and vulnerabilities and therefore the effort to analyse these in relation to an application. A simple solution is to reduce the number threats to consider. A more sophisticated approach should be possible by considering threats in a given sequence. The area of highest risk to personal privacy is the fact that data on the tag can be read without the knowledge of the individual, thus the tag data and the air interface. There is also a well-known security benchmark for evaluating IT system security with three goals known as *confidentiality, integrity* and *availability*. In relationship to RFID privacy:

— *Confidentiality* refers to limiting information access and disclosure only to authorised users, effectively the RFID application.

— *Integrity* refers to the trustworthiness of the information source. For example, if data has been maliciously modified, then the integrity of the communication is impaired.

— *Availability* refers simply to the availability of the information resource. In RFID terms, if a tag is physically removed then it is no longer available.

8) http://www.us-cert.gov/cas/bulletins/

9) http://cert.europa.eu/cert/plainedition/en/cert_about.html

For privacy, confidentiality and then integrity are more important. Therefore if an SME is to be able to reduce its workload, it needs to focus on the threats that impact confidentiality and integrity of the data on the tag and the air interface. This can make even a limited scale PIA very useful. If the threats can be classified in this meaningful way, it then enables an SME to focus on the more critical issues.

12 Conclusions

a) The RFID operator is responsible for undertaking the PIA and preparing the PIA report. The purpose of the RFID Privacy Impact Assessment is to determine how open to attack an individual's privacy is from the exploitation of aspects of the RFID technology when the RFID tag is carried by a or can be associated with a person. In addition, RFID-related data held on the application system has to be taken into consideration in a PIA. The implementation of RFID presents a more complex position where both internal and external risks need to be taken into account in a co-ordinated manner. If the RFID operator increases controls on the internal threats, then the malicious 'benefit' of the RFID vulnerability can be reduced. As such, this extends beyond what has traditionally been accepted as pure data protection issues.

b) The RFID PIA process requires an understanding of the system, the RFID privacy threats to the system and to individuals being identifiable through being in possession of an RFID tag. The process also calls for a methodical cost-benefit analysis of the risks and countermeasures. Without this the appropriate selection of controls and countermeasures cannot be made. The emphasis on "methodical cost-benefit analysis" should be intended to place the PIA in context. The level of determining the detail required for the PIA is crucial.

c) The risk assessment process should comprise:

    1) Identifying and assigning the values to assets associated with an individual's privacy.

    2) Identifying threats to the RFID system and providing a means of assessing the threat level.

    3) Identifying vulnerabilities and enumerating the associated risk levels.

    4) Arriving at an initial risk level, without considering any countermeasures.

    5) Considering the countermeasures that can be used to reduce the threat level, which results in the residual risks associated with each asset in the RFID application.

d) The recommendations of NIST (see 3.6) can be used mutatis mutandis for the RFID applications.

e) Key attributes for the EN on the PIA for RFID to consider incorporating are tag - reader privacy analysis (due to the non-application operator privacy threats), creating an application operator process that embraces all the necessary analysis needed for a good quality RFID application PIA while not precluding or even encouraging the use of reusable RFID PIA analysis from others that, if made use of, would need less effort from the application operator to produce their own PIA.

f) The RFID PIA needs document revision control and for monitoring and reporting incidents that impact the RFID application.

Bibliography

[1] The bibliography refers to sources used for research purposes

[2] ABIE H., BORKING J. Risk Analysis Methods and Practices, Privacy Risk Analysis Methodology, DART/05/2012, Oslo 2012

[3] Alhadeff J., Van Alsenoy B.,TAS3: Requirements: Privacy, governance and contractual options, v.2.0, Leuven,2009

[4] Australian Government Information Management Office (AGIMO)

[5] http://www.agimo.gov.au/infrastructure/authentication/agaf/impguidegovt/volume3/part5/appendix_a_-_sample_privacy_law_compliance_checklist

[6] Butin, D. M.Chicote, D. Le Métayer, Accountability by Design for Privacy, EU Prescient project, 2012

[7] CAVOUKIAN A. *Getting to the Truth about Privacy & Security*. Toronto, 2002

[8] 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, Official Journal L 281, 23/11/1995

[9] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive). Official Journal L 201, 31/07/2002 ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [of March 31, 2010] July 2010

[10] ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [of March 31, 2010] July 2010

[11] European Commission Communication COM(2007) 96 'RFID in Europe: steps towards a policy framework

[12] European Commission Recommendation C (2009) 3200 on the implementation of privacy and data protection principles in Applications supported by Radio Frequency Identification

[13] FLOERKEMEIER C. et al. "Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols," Institute for Pervasive Computing, Switzerland, 2004. Online: http://www.vs.inf.ethz.ch/res/papers/floerkem2004-rfidprivacy.pdf

[14] Karygiannis T. & L. Owens, NIST Special Publication (SP) 800-48, Wireless Network Security, 802.11, Bluetooth, and Handheld Devices., NIST SP 800-48

[15] KLITOU D. Privacy Invading Technologies: towards a common legal framework for safeguarding privacy, liberty and security in the 21st century, Dissertation, Leiden 2012.

[16] OFFICE OF THE PRIVACY COMMISSIONER (NEW ZEALAND). Privacy Impact Assessment Handbook: http://www.privacy.org.nz/library/privacy-impact- assessment-handbook.

[17] For a collection of online resources from around the world, collated by the New Zealand Privacy Commissioner's Office, see: Office of the Privacy Commissioner 2006

[18] http://www.foi.gov.uk/sharing/toolkit/pia_online_res.pdf.

[19] OFFICE OF THE VICTORIAN PRIVACY COMMISSIONER. Privacy Impact Assessments – a guide: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf

[20] PRIVACY COMMISSIONER OF CANADA. Audit report On The Protection Of Personal Information In Wireless Environments, Ottawa 2010

[21] Privacy Office of the Department of Homeland Security has released official guidance for use in drafting PIAs:

[22] www.dhs.gov/xinfoshare/publications/editorial_0511.shtm.

[23] RADACK S., ed. *Security For Wireless Networks And Devices*. National Institute of Standards and Technology Washington, 2003

[24] SPIEKERMANN S. User Control in Ubiquitous Computing: Design Alternatives and User Acceptance, Aachen, 2008

[25] Treasury Board of Canada Secretariat has produced a useful PIA e- learning tool:

[26] http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp.

[27] VAN BLARKOM G.W., BORKING J.J., OLK J.G.E. *Handbook of Privacy and Privacy Enhancing Technologies, the case of intelligent software agents*. The Hague, 2003

[28] www.cbpweb.nl/downloads_technologie/pisa_handboek.pdf

[29] WESTIN A.F. *Privacy and Freedom*. New York, 1967

[30] WP 29, Opinion 9/2011 on “The Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications”.

[31] WRIGHT D., DE HERT P. *Privacy Impact Assessment*. Dordrecht, Heidelberg, London, New York, 2012

This page deliberately left blank

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.™