BS EN 16571:2014

BSI Standards Publication

Information technology — RFID privacy impact assessment process

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 16571:2014.

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.

ISBN 978 0 580 81786 1

ICS 35.240.60

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

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

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16571

June 2014

ICS 35.240.60

English Version

Information technology - RFID privacy impact assessment process

Technologies de l'information - Processus d'évaluation d'impact sur la vie privée des applications RFID

Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID

This European Standard was approved by CEN on 14 May 2014.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

Ref. No. EN 16571:2014 E

Contents

Page

Foreword

This document (EN 16571:2014) has been prepared by Technical Committee CEN/TC 225 “AIDC technologies”, the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by December 2014, and conflicting national standards shall be withdrawn at the latest by December 2014.

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 document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

This European Standard is one of a series of related deliverables, which together comprise M/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 16656, *Information technology — Radio frequency identification for item management — RFID Emblem (*ISO/IEC 29160:2012*, modified)*;

— 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 [1)], *Information technology — RFID privacy impact assessment analysis for specific sectors*;

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

— CEN/TR 16684[2)], *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*.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: 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 the United Kingdom.

1) CEN/TR 16673 contains practical examples of PIA systems.

2) CEN/TR 16684 contains practical examples of notification signage systems.

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, and 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 programme identified in the first phase.

This European Standard is one of 11 deliverables for M/436 Phase 2. It builds on the research undertaken in the two related Technical Reports:

— CEN/TR 16673 provides an insight into how RFID privacy issues have been addressed in four sectors: libraries; retail; e-ticketing, toll roads, fee collection, events management; and banking and financial services.

— CEN/TR 16674 considers formal PIAs that are already in place, but not necessarily presented as formal national standards.

The procedures defined in this European Standard are intended to be used by individual RFID operators or entire sectors for conducting a PIA for RFID. As such, it will cite as references other deliverables included in M/436 Phase 2. A sector-based PIA can act as a template to assist in the development of a specific PIA.

1 Scope

This European Standard has been prepared as part of the EU RFID Mandate M/436. It is based on the Privacy and Data Protection Impact Assessment Framework for RFID Applications, which was developed by industry, in collaboration with the civil society, endorsed by Article 29, Data Protection Working Party, and signed by all key stakeholders, including the European Commission, in 2011.

It defines aspects of that framework as normative or informative procedures to enable a common European method for undertaking an RFID PIA.

It provides a standardized set of procedures for developing PIA templates, including tools compatible with the RFID PIA methodology.

In addition, it identifies the conditions that require an existing PIA to be revised, amended, or replaced by a new assessment process.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

3 Terms and definitions

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

3.1
competent authority
organization called for in the RFID Recommendation to receive the PIA 6 weeks before deployment of the RFID application

Note 1 to entry: The Recommendation in Point 5 (d) provides no details of the credentials of the competent authority.

3.2
controlled domain
part of an of an application that is under the direct control of the RFID operator (or data controller), including the data on the tag that is processed by the application and the RFID air interface communications

Note 1 to entry: This has close analogies with data processing under Directive 95/46/EC.

3.3
countermeasure
action, device, procedure, or technique that meets or opposes (i.e. counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause

3.4
data controller
controller
natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law

[SOURCE: Directive 95/46/EC]

3.5
Data Protection Authority
DPA
organization, or organizations, responsible for the administration of Directive 95/46/EC in a Member State

3.6
identified or identifiable person
person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

[SOURCE: Directive 95/46/EC]

3.7
individual
natural person who interacts with or is otherwise involved with one or more components of an RFID application (e.g. back-end system, communications infrastructure, RFID tag), but who does not operate an RFID application or exercise one of its functions

Note 1 to entry: In this respect, an individual is different from a user. An individual may not be directly involved with the functionality of the RFID application, but rather, for example, may merely possess an item that has an RFID tag.

3.8
information security
preservation of the confidentiality, integrity and availability of information

[SOURCE: Recommendation C(2009) 3200 final]

3.9
monitoring
activity carried out for the purpose of detecting, observing, copying or recording the location, movement, activities or state of an identified or identifiable person

[SOURCE: RFID Recommendation C(2009) 3200 final, modified — The definition itself has been adapted.]

3.10
personal behaviour information
data that identifies an individual's behaviour or behavioural characteristics

3.11
personal data
information relating to an identified or identifiable natural person ('data subject') inasmuch as 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

[SOURCE: Directive 95/46/EC, modified — The definition has been grammatically changed.]

3.12
personal identifier
data that can be used to directly or indirectly identify an individual to whom such data refers

3.13
personal privacy asset
anything that has value to the person associated with a particular RFID tag

Note 1 to entry: The loss of such an asset therefore requires protection.

3.14
privacy
right of the identified or identifiable person to have his identity and action protected from any unwanted scrutiny and interference

Note 1 to entry: Privacy reinforces the individual's right to decisional autonomy and self-determination which are fundamental rights accorded to individuals within Europe.

[SOURCE: ETSI/TR 187 020 V1.1.1 (2011-05), modified — The definition itself has been adapted.]

3.15
privacy breach
situation where personal data in an RFID application is processed in violation of one or more relevant privacy safeguarding requirements

[SOURCE: ISO/IEC 29100:2011, modified — The definition itself has been adapted.]

3.16
privacy capability statement
declaration by an RFID technology provider of RFID tags or readers of the privacy features inherent in the specified product

Note 1 to entry: Based on CEN/TR 16672, the privacy capability statement identifies in a consistent manner the extent that the features in a product support enhancements to privacy. The privacy capability statement is a more precise input to the PIA process than the generic protocol standard because it is product-specific.

3.17
privacy risk
potential that a given threat will exploit vulnerabilities of personal privacy asset and thereby cause harm to the attacked system or organization

[SOURCE: ETSI/TR 187 020 V1.1.1 (2011-05), modified — The definition itself has been adapted and the defined term was "risk" originally.]

3.18
Registration Authority
RA
organization appointed by CEN to maintain a publicly accessible register of factors associated with a standard

Note 1 to entry: For EN 16571, the RA is responsible for maintaining a register of privacy capability statements.

3.19
residual risk
risk remaining after countermeasures have been implemented to reduce the risk associated with a particular threat

[SOURCE: ETSI/TR 187 020 V1.1.1 (2011-05)]

3.20
RFID
radio frequency identification
use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to read from or write to an RFID tag

[SOURCE: RFID Recommendation C(2009) 3200 final]

3.21
RFID application
application that processes data through the use of tags and readers, and which is supported by a back-end system and a networked communication infrastructure

[SOURCE: Recommendation C(2009) 3200 final]

3.22
RFID application operator
RFID operator
natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an application, including controllers of personal data using an RFID application

[SOURCE: RFID Recommendation C(2009) 3200 final]

3.23
RFID interrogator
RFID reader
interrogator
reader
fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags

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

3.24
RFID PIA report
detailed internal report of the results of the PIA process

Note 1 to entry: Except for the reference in Recommendation, in Point 5 (d), of making the assessment available to a competent authority, the RFID PIA report is considered a confidential document.

3.25
RFID PIA summary
part of the RFID PIA process that is publicly available in the interests of transparency

3.26
RFID tag
RF tag
tag
transponder
RFID device having the ability to produce a radio signal or a RFID device which re-couples, back-scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer

[SOURCE: RFID Recommendation C(2009) 3200 final]

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

3.27
RFID threat
physical, hardware, or software mechanism with the potential to adversely impact a personal privacy asset and associated data types or a data subject through unauthorized access, destruction, disclosure, modification of data and / or denial of service

3.28
RFID vulnerability
weakness of an asset or group of assets that can be exploited by one or more threats

[SOURCE: ISO/IEC 27005:2011, modified — The definition itself has been adapted and the defined term was "information security risk" originally.]

3.29
template
input information and data intended to assist in reducing the effort required to complete a PIA, where a number of RFID applications share some common features

Note 1 to entry: The degree of detail of a template is a matter of decision for the originator of such a document. It may vary from a description of the application to a more sophisticated analysis, and can be used as a generic tool to prepare the PIA report, but is never a substitute for a PIA report, which is the responsibility of each RFID operator.

3.30
uncontrolled domain
part of an of an application that the RFID operator (or data controller) cannot control, including the capability of a third party legitimately or illicitly reading data from the RFID tag in any form factor, whether with reading devices conform to the air interface protocol or circumvent it

4 Symbols and abbreviations

For the purposes of this document, the following symbols and abbreviations apply.

— AIDC Automatic Identification and Data Capture
— AFI Application Family Identifier
— CEN European Committee for Standardization (French = Comité Européen de Normalisation)
— DSFID Data Storage Format Identifier
— EN European Standard
— EPC Electronic Product Code
— ETSI European Telecommunications Standards Institute
— GS1 Global Standards One
— HF High Frequency
— IEC International Electrotechnical Commission
— ISO International Organization for Standardization
— NFC Near Field Communication
— PIA Privacy Impact Assessment
— RF Radio Frequency
— RFID Radio Frequency Identification
— SME Small and medium-sized enterprise
— TR Technical Report
— TS Technical Specification
— UHF Ultra High Frequency

5 Structure of this European Standard

This European Standard contains the specification and description of the RFID privacy impact assessment (PIA) process. The purpose of the following clauses, and their associated annexes, is as follows:

a) Clause 6 specifies what the RFID Recommendation considers to be RFID technology (which is not necessarily aligned with the structure of various technology standard committee domains and scopes), what is an RFID application, and what is an RFID operator.

b) Clause 7 describes some of the strategic considerations that an RFID operator needs to take into account before undertaking an RFID PIA. This includes taking responsibility over and above the requirements of the Recommendation.

c) Clause 8 and its associated annexes describe some of the tools and other mechanisms that can be employed to simplify the process of undertaking the PIA. These tools have the additional advantage of providing consistency between similar PIA reports.

d) Clause 9 is the first clause associated with the actual process of undertaking an RFID Privacy Impact Assessment. This particular clause deals with determining the detail required for the RFID PIA.

e) Clause 10 provides the lowest level of deliverable from the PIA process, which is an RFID functional statement. This is the output when Clause 9 determines that a PIA is not required.

f) Clause 11 provides the necessary details to prepare the description of the RFID application(s). This description covers all aspects from the RFID tag to how the RFID data is held on the application.

g) Clause 12 provides all the details to undertake the risk assessment itself, starting with references to the Recommendation as the principle behind the procedures. The process itself comprises:

   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.

h) Clause 13 provides the details that should be included in the RFID PIA summary, which is to be made available publicly to citizens and customers.

i) Clauses 14 and 15 address the need for document revision control and for monitoring and reporting incidents that impact the RFID application.

6 Field of reference for this European Standard

6.1 'RFID' as defined by the EU RFID Recommendation

Based on the definitions of RFID, RFID tag and RFID reader cited in the Recommendation (see Clause 3), this European Standard shall apply to technologies that comply to, or operate at, the same radio frequencies as shown in Table 1.

As such it shall apply to technologies commonly known as RFID, contactless cards, near field communications (NFC), personal identification cards and contactless payment cards that use radio frequency for communication purposes.

Table 1 — RFID and related technology standards within the scope of this European Standard

Core Reference Standard [a]	Related Standards	Frequency	See Footnote
ISO/IEC 14443		13,56 MHz	[b]
ISO/IEC 15693 (all parts)	ISO/IEC 18000-3 Mode 1	13,56 MHz	
ISO/IEC 18000-2	ISO 11784 ISO 11785 ISO 14223 (all parts)	125 kHz (type A), 134,2 kHz (type B)	
ISO/IEC 18000-3 Mode 2		13,56 MHz	
ISO/IEC 18000-3 Mode 3		13,56 MHz	[c]
ISO/IEC 18000-4		2,45 GHz	
ISO/IEC 18000-61	ISO/IEC 18000-6 Type A	(860 to 960) MHz	
ISO/IEC 18000-62	ISO/IEC 18000-6 Type B	(860 to 960) MHz	
ISO/IEC 18000-63	ISO/IEC 18000-6 Type C	(860 to 960) MHz	[d]
ISO/IEC 18000-64	ISO/IEC 18000-6 Type D	(860 to 960) MHz	
ISO/IEC 18000-7		433 MHz	
ISO/IEC 18092		13,56 MHz	[e]
ISO/IEC 21481		13,56 MHz	[f]
JIS X6319–4		13,56 MHz	[g]

[a] There are different editions of some of these standards. Artefacts that comply with a particular edition have different features to artefacts that comply with another edition.

[b] ISO/IEC 14443 supports two types of communication known as type-A and type-B. Many products used in the public transport sector may use a pre-ISO/IEC 14443, Calypso rev 1 radio protocol.

[c] Also known as GS1 EPCglobal HF C1.

[d] Also known as GS1 EPCglobal UHF C1 Gen 2.

[e] Also known as NFC IP1.

[f] Also known as NFC IP2.

[g] The Japanese standard JIS X6319–4 has not been approved at the ISO level, but is sometimes referred as FeliCa.

6.2 'RFID application' as defined by the EU RFID Recommendation

The definition of RFID application cited in the Recommendation (see Clause 3) precisely determines the field of reference of RFID applications covered by this European Standard.

6.3 'RFID operator' as defined by the EU RFID Recommendation

Based on the definition of RFID operator cited in the Recommendation (see Clause 3) this European Standard shall apply to any operator that carries out a reading (decoding) process on an RFID tag. It shall also apply to any operator that carries out a writing (encoding) process on an RFID tag.

The requirement for an organization that only performs the encoding function to undertake a PIA is based on two fundamental premises:

— Generally, the European Convention on Human Rights requires an individual's privacy to be protected and this applies to personal data and the possibility of tracking someone's whereabouts and movements in the public sphere, or drawing up a pattern of someone's movements.

— Specifically, the Recommendation makes this clear, particularly in preamble paragraphs 5 and 6, and in recommendation point 5 (a) "that operators… 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 does not mean that the organization encoding the RFID tag has to have any understanding of applications that other RFID operators might employ. What it does mean is that the RFID operator that is the encoder, needs to assess the privacy risks of both the data being encoded and of any inherent chip identifier on the tag being used for tracking or building up a behavioural pattern of an individual.

6.4 Relationship between the RFID PIA and data protection and security

Figure 1 shows how the RFID PIA relates to the application and two other key functions. Although the RFID PIA process is applied independently, there are some relationships with processes to ensure system security and data protection.

There are similarities in some of the methodologies described in this European Standard with those defined in ISO/IEC 27005 for security. Furthermore, in undertaking the RFID privacy impact assessment, risks might be identified which suggest that the security aspects of the application need to be reviewed.

Data protection is covered by European national laws based on the Directive 95/46/EC. The RFID PIA only addresses data protection for the data elements held on the RFID tag or directly associated with the RFID application. This means that a combination of the external exposure of RFID tags and the data held on the application require some additional consideration with respect to data protection. These aspects will be discussed within this European Standard.

All three of these functions have a common theme: a breach in any one of them has an adverse impact on the organization's reputation. However, at the time of writing this European Standard an organization is only required to address data protection to meet legal requirements; currently privacy and security are good practices.

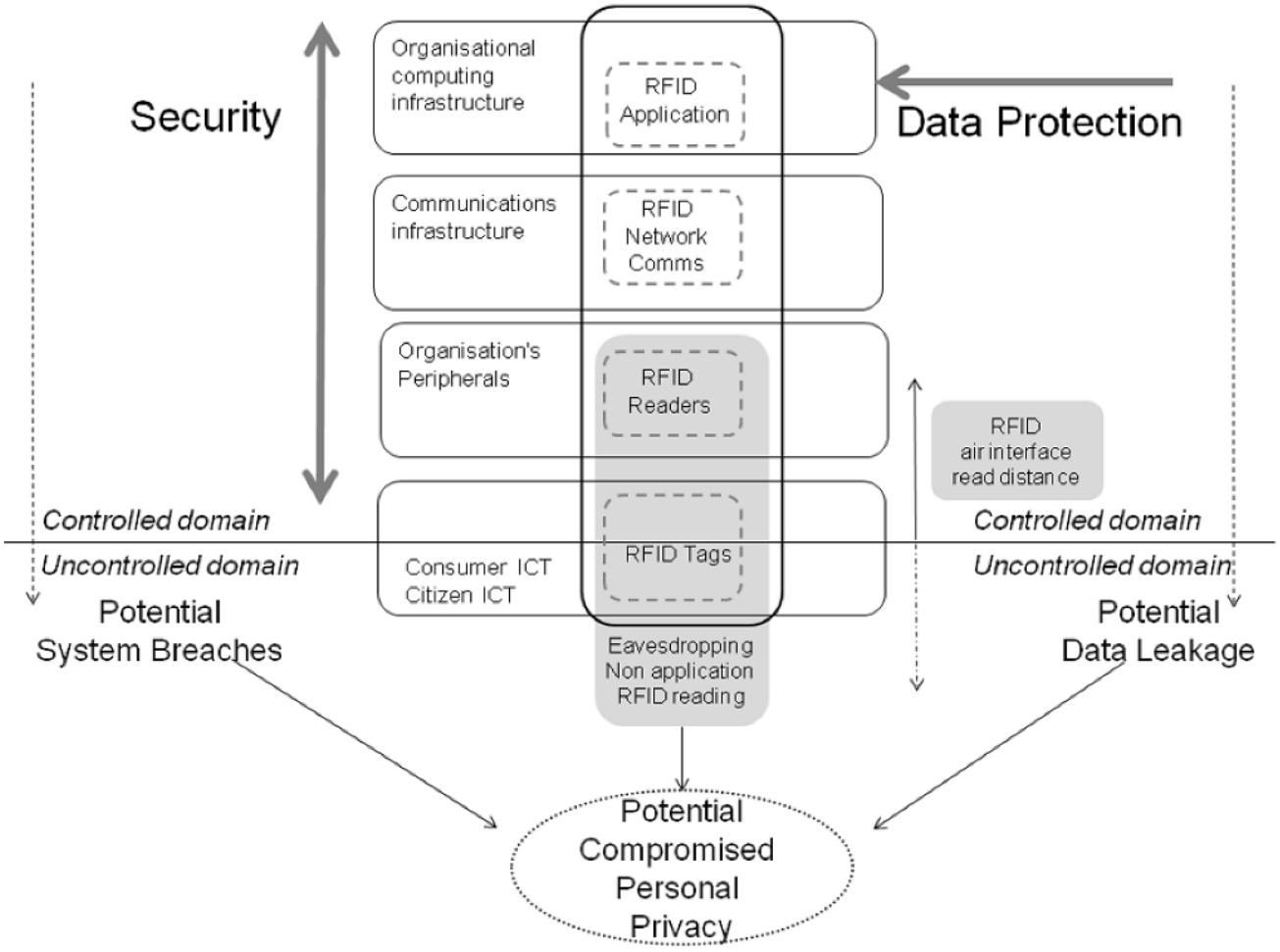

Figure 1 — Interrelation between RFID privacy, security, and data protection functions

Data protection comprises all processing of data such as collection of data, accuracy of data and use of data. Most importantly, it is addressed by legal requirement for compliance as set out in Directive 95/46/EC. CEN CWA 16113 defines a set of voluntary good practices to help businesses and data managers comply with Directive 95/46/EC. The document is targeted for use by SMEs in the European Union.

Security of data is additionally protected by the implementation of security procedures for protection computer systems, using procedures defined, e.g. in the ISO/IEC 270xx series. There is no legal requirement to implement such systems, but some breaches of computer security can be the direct cause of infringement of data protection. While privacy is the individual's right to determine the use of any information about him, from an RFID perspective this presents a challenge between data protection, data security and privacy.

It is important to understand the implications of the controlled and uncontrolled domains. Within the controlled domain, the RFID operator (or data controller) not only has full responsibility but also control of the application. When an RFID tag leaves the controlled domain, it might still be readable in one of three states:

a) It has reached the end of its functional use but can still be readable, e.g. an RFID tag on a retail product having completed a sales transaction at a retail store that has RFID data capture.

b) It is intended to be readable at some later point in time or space, e.g. a public transport card, or contactless payment card, or employee access badge.

c) Having been provided for an RFID function, but where the final point in the process has no RFID data capture, where the RFID leaves that point still readable. Examples include:

1) RFID baggage tags, where the departing airport uses RFID data capture, but the arrival airport does not.

2) Retail products that are source-encoded by a manufacturer or distributor, but which are sold via retail outlets with no RFID capabilities.

3) Library books that are source-encoded as part of a consortium of libraries, but where the specific library has no RFID capabilities.

These three states present different scenarios to the citizen or consumer, and the amount of control that s/he can exercise with the knowledge that RFID tags are being used. In the case of state (a) on-site information should notify that RFID data capture is being used. In the case of state (b) the person needs to be aware that for the RFID tag or card to be usable in future it has to remain readable, subject to any privacy capability features that might be deployed by the card issuer. For state (c), the logically expected RFID operator does not exist, and the particular operator is not considered an RFID operator by the Recommendation, but that responsibility is transferred closer to, or at the source of encoding data on the RFID tag. The Recommendation clearly defines an RFID operator (see 3) as have sole or joint responsibility for an RFID application.

The uncontrolled domain has these potential exploits:

— Security standards are designed to protect all the operator’s data processing from intrusion and loss and the ISO 270xx series is built around security in depth from the core to the periphery of systems and networks. Security beaches may lead to any of the organization’s data being available beyond their control.

— Data protection of data collected about individuals has been applied mainly within the controlled domain, with few requirements related to the protection of personal data as an RFID tag moves beyond the controlled boundary. Key data protection challenges for RFID are exploits that include, for example, collection without permission, purpose creep and uncontrolled data sharing.

— Some of the privacy exploits can occur beyond the boundary of a legitimate RFID application, which does place some responsibility on the RFID operator, specifically with respect to the human right to privacy. Privacy focusses on the individual and protection against illegal, unauthorized or unreasonable and intrusive access to their domestic personal processing and their personal data.

As soon as an RFID operator has concluded a communications transaction between the operator's interrogator and the RFID tag, the tag is deemed to enter the uncontrolled domain if it is still capable of being read by another interrogator. For RFID tags that are intended for multiple use, this is a normal procedure. For single use tags, the RFID operator might consider that the viable use has expired. However, while the tag contains data that makes the person identifiable, the person holding the tag has a reasonable expectation of his or her privacy being protected. This expectation extends to the uncontrolled domain and needs to be address by the RFID operator.

In the uncontrolled domain shown in Figure 1, there are potential compromises to privacy related to the data on the tag and its ability to provide privacy protection. This might be exacerbated by potential security breaches and potential personal data leakage from uncontrolled sharing of data, both internal to an organization with other applications or between organizations under data sharing agreements. The key issue arising with these other data loss paths for the RFID privacy impact assessment is the linkability of any lost data to the RFID tag and it’s data.

With the ongoing development and spreading of RFID technology into a wider range of use there will be a need for the RFID operator to keep under active review any current or proposed legislation changes with regard to illicit use of RFID technology by individuals.

RFID brings many benefits to an application, but the external risks beyond the bounds of an application boundary also need to be taken into account. If these external risks are not properly considered, RFID can

expose an individual to privacy threats and in consequence also expose an organization to increased security risks, data protection risks and loss of reputation with regard to the individual.

6.5 Relevant inputs for the PIA process

6.5.1 General

With a remit to consider reducing barriers to the RFID PIA production through cost and effort reduction, this European Standard describes a number of efficiency tools and processes in Clause 8.

The relationship between these measures and the core process is described in the following subclauses.

6.5.2 The privacy capability statement

RFID technology providers produce this document to record the features for protecting privacy for specific tag and reader products. It is an early input into the RFID operator's PIA process.

6.5.3 The Registration Authority

In order to reduce costs and effort for RFID technology providers and RFID application operators, the Registration Authority maintains the register of voluntarily submitted privacy capability statements to act as a common source of these statements.

The beneficial effects include one-off provision of such statements by technology providers, independently of the knowing which applications are undergoing the RFID PIA process. The RA provides application operators with an easily accessible source for the input information needed for their PIA. The RA can also provide privacy capability statements for specific tags or readers that are no longer being supplied to the market but may nonetheless be incorporated into an implementation.

6.5.4 RFID PIA templates

Where a high degree of commonality exist between RFID applications that are used by a number of RFID operators, a template may be produced by a responsible collective entity on behalf of such operators, consisting of PIA analysis and documentation that is common to that groups of operators. A preferred approach, when applicable (e.g. the same application is distributed across the Internal Market), is for the template to be a Single European-wide PIA template. Such European-wide PIA templates shall be relevant and used across the Internal Market and European countries without requiring any changes and be impacted for specific countries or national preferences.

The template is an input to the PIA process for an operator. It enables RFID operators that can use the template to require considerably less effort to complete the RFID PIA. RFID operators only have to provide information that is not included in the template plus those parts of the privacy impact assessment that are unique to their operation in order to complete their RFID PIA.

7 RFID operator's organizational objectives of the RFID PIA

7.1 Overview

This European Standard recognises that the choices of business systems and risk management procedures are organizational decisions. As such, the organization's decision-makers need to be well-informed in order to make appropriate decisions for their RFID applications.

In the clauses that address detailed technical aspects of the RFID PIA, both the RFID privacy and security aspects coincide as common objects to address risks. Therefore, while undertaking the RFID PIA RFID operators should also consider the ISO/IEC 270xx series of standards (see the Bibliography), which provide more details on generic security issues.

The organizational objectives of an RFID PIA include:

— ensuring that the RFID privacy protection of individuals is a core consideration in the initial considerations of the design of an RFID application and in all subsequent activities during the system development life cycle;

— ensuring that accountability for privacy issues is clearly incorporated into the responsibilities of respective system developers, administrators and any other participants, including those from other institutions, jurisdictions and sectors;

— providing decision-makers with the information necessary to make fully-informed policy, system design and procurement decisions of RFID systems, hardware and tags for proposed RFID applications;

— providing decision-makers with an understanding of the RFID privacy implications and risks, assess their likelihood, and identify the options available for avoiding and/or mitigating those risks, both within the specific RFID application and for a person possessing the RFID tag beyond the boundary of the application;

— providing decision-makers with information to ensure that residual privacy risks for an individual remain at an acceptable level;

— providing sufficient information to meet the requirement in the EU Recommendation to provide information and transparency on RFID use and develop and publish a concise, accurate and easy to understand information policy for each application;

— providing documentation on the business processes and flow of personal information associated with the RFID application for use and review by departmental and agency staff and to serve as the basis for consultations with clients, the privacy officers and other stakeholders, taking into account (if relevant to the organization) specific consumer interests and public interest issues.

The RFID PIA process shall establish:

— the internal context, in terms of all the planned communication between the RFID tag and the RFID application;

— the external context, in terms of the RFID tag leaving the organization's application environment and still being functional.

Finally, the PIA process should be undertaken during the design, implementation, and lifecycle of an RFID application.

7.2 Meeting and exceeding legal requirements

This European Standard has been developed as part of the ongoing activities based on the RFID Recommendation. The legal requirements for the back-end system are defined in the Data Protection Directive (95/46/EC). At the time of publication of this European Standard, there is no explicit European legislation addressing RFID privacy, but this is covered at a high level by the Human Rights legislation under the right to privacy. Given the significant investment that any organization makes in an RFID application, and the reputation risks of inherent features in the technology not being addressed, there are business advantages in undertaking the RFID Privacy Impact Assessment.

Undertaking an RFID PIA should be a major consideration for RFID operators that are national, regional or local government organizations.

7.3 When to undertake the RFID PIA

7.3.1 General

There are a number of situations when an RFID PIA shall be considered as defined in the following subclauses. If approached in the manner described in the following sub-clauses, a beneficial and cost-effective approach may be to consider the RFID PIA as:

— from the inception of the RFID application;

— linked to the lifecycle of the RFID application;

— re-visited at each new project phase, new situation, significant changes in the application and/or technology, change in use or processing of information/data; and

— a regular review with defined periods (comparable to quality audits).

7.3.2 Undertaking a PIA at the design stage before the RFID system becomes operational

The RFID Recommendation calls for the RFID PIA to be made available to the competent authority at least six weeks before the deployment of an application (Point 5d). This implies that the PIA process should begin at an earlier stage to ensure that the risks are identified and addressed before being embedded in the design of the RFID application.

If a PIA is not undertaken during the design stage then the reasons for that shall be documented and provided to the data protection authorities on request.

RFID operators that encode tags that are read by others shall provide their PIA when requested by an RFID operator utilizing the RFID tag for data capture. In many cases an RFID operator encoding tags (e.g. in a supply chain, in an airport for baggage handling, for contactless payment cards) might not know the organizations that have implemented RFID data capture. This has two practical implications:

— The PIA prepared by the organization encoding the RFID tag needs to address the presence of such tags in the uncontrolled domain.

— Some means is necessary of posting or publishing the summary PIA, which includes details of the data on the tag.

7.3.3 Undertaking a PIA at a review and update the design-based PIA

It is reasonably common for modifications to be made to a system between its original design, implementation and training of relevant staff. Such changes might have an impact on the original assessments made in the design-based RFID PIA. Therefore the RFID PIA should be reviewed internally 6 months after implementation to establish if the original risk assessments are still valid or need to be revised.

After this 6-month interval, the RFID PIA should be reviewed on a regular basis (e.g. once per year).

Additionally when the type of data being encoded on an RFID tag changes, the RFID operator requiring or controlling that encoding process shall review and update the PIA. This is particularly important where personal privacy data is being added or permanently removed from the RFID tag.

7.3.4 Undertaking a PIA to contribute to the development of a template

Given that there is already a significant number of RFID implementations in some sectors, business managers should consider carrying out an RFID PIA procedure for a fully operational RFID application. This approach might be useful for industry bodies and other groups to enable them to develop *good practice* guidelines and templates based on a number of applications. This will also align with requirement in the RFID

Recommendation for information and transparency on RFID use. Point 7d calls for “a summary of the Privacy and Data Protection Impact Assessment” to be part of a published information policy for each RFID application.

External stakeholders should be involved in the creation of a sector template as this can lead to increased trust in such a PIA. Commercially sensitive data does not have to be disclosed while societal representatives participate in the template creation.

An advantage of a template is that it ensures consistency across the sector, by providing a degree of rigour and logic within the RFID PIA methodology for the sector.

7.3.5 Undertaking a PIA with an established template

Where a template exists, it can reduce the effort of undertaking a PIA for an RFID operator and show that the organization is following, or possibly, exceeding peer group procedures.

An advantage of a template is that it identifies common features of an application, thus enabling consistency in undertaking the PIA process.

Where such a template exists, the RFID operator shall use a Single European-wide template. As such a national template should not be used, other than to provide language specific requirements.

7.3.6 Undertaking a PIA at the introduction of a new function within the RFID application

If a new function is added to the RFID application, the existing PIA should be reviewed as set out in 7.3.3.

If a PIA is not undertaken when a new function is included in the application then the reasons for that shall be documented and provided to the data protection authorities on request.

7.3.7 Undertaking a PIA based on changes in RFID technology

As privacy by design features are added in future to RFID tags and interrogators, these enhancements should be considered either continually (if possible), or at a new project phase. It is recognized that developments in the technology cannot be implemented immediately for an application and need to be considered as part of the overall organizational process.

If there are changes in the RFID technology within the RFID application then one of the following shall be done:

— the RFID PIA process shall be revised on the assessment of the RFID operator, or

— if a RFID PIA process is not undertaken, then the reasons for not doing so shall be made in the area of the PIA report identifier on the application description (see Clause 11).

EXAMPLE An example might be that the RFID operator wants to record the fact that new interrogators have been installed that can address enhanced security features on some tags. But the roll out of interrogators has not yet reached 20 % of the installed base. When a larger installed base is achieved, the PIA will be re-assessed.

7.3.8 Undertaking a PIA when a privacy breach has been reported

When a privacy breach has occurred in the RFID operator's own application, the RFID operator shall review the PIA. There are other external privacy breaches where the RFID operator should consider reviewing the PIA. These include when a breach has been identified in the same, or similar:

— business or organization sector in which the RFID operator performs a function;

— application used by the RFID operator;

— RFID products used by the RFID operator.

If a PIA is not undertaken when any external privacy breach has been identified then the reasons for that shall be documented and provided to the data protection authorities on request.

8 Tools to simplify the process

8.1 RFID operator responsibility

Although the RFID operator is responsible for undertaking the PIA and preparing the PIA report, several mechanisms can be employed to simplify the process without compromising the rigor that is required. Some of the tools are described below together with advice on how they might be developed.

8.2 RFID technology privacy capability tools - overview

One of the challenges for undertaking an RFID Privacy Impact Assessment is that of gaining a sufficient understanding of the privacy and security features supported by specific RFID products. Many products can claim to be conformant to the relevant International Standard, as defined in Table 1. Because these standards have many optional features an RFID operator, even a system integrator, might not be aware of all of the features that a particular tag or interrogator product supports.

In an RFID application a general rule of thumb for the RFID PIA process is to presume that the RFID interrogator's capability is the constraining feature of the air interface protocol. For example, if an interrogator has no means of invoking a command that utilises a particular privacy or security features in the RFID tag being processed, then those features contribute little or nothing to directly enhance the privacy and security countermeasures across the air interface. Such divergences are to be expected, given the different investment and product life cycles of RFID interrogators and tags. Whereas the RFID interrogator is generally considered a permanent part of the system infrastructure, new generation tags are highly likely to be introduced during the viable lifetime of the interrogator.

Some products might be subject to additional interoperability, conformance, and certification procedures. Such facts may be added to the privacy capability statement.

NOTE Some interrogators may have the capability of supporting firmware or software upgrades, which can be used to increase their functionality. If such features are available, then these need to be considered when undertaking the RFID PIA.

8.3 Registration of RFID privacy capability statements by RFID product manufacturers

8.3.1 General

This clause specifies the procedural requirement to maintain a publicly accessible register of RFID privacy capability statements of individual RFID products (e.g. integrated circuits, tags and interrogators), the details of which are defined in 8.4.

To facilitate public access by RFID operators and systems integrators, a Registration Authority has been established to maintain such a register. The obligations of the Registration Authority and of the responsibilities of technology vendors are defined in the following subclauses.

8.3.2 Obligations of the Registration Authority

The Registration Authority shall be responsible to CEN/TC 225. Its responsibilities shall be:

a) to develop 'pro forma' RFID privacy capability statements for products in each if the categories described in 8.4 that claim conformance to an air interface protocol not covered by this European Standard;

b) to receive and acknowledge RFID privacy capability statements from organizations providing such statements of their products placed in the public domain to assist with the execution of the RFID PIA in a consistent manner;

c) to make such RFID privacy capability statements available on a publicly accessible database within 30 days of receipt of the capability statement;

d) to notify the applicant organization that its RFID privacy capability statement has been published on the database;

e) to maintain the database with the information as set out in 8.3.5;

f) to process requests from RFID operators seeking information about a particular RFID product for which no RFID privacy capability statement is available on the database; the RA shall contact the relevant product manufacturer, providing promotional material of the benefits of being on the database and requesting information to be provided;

g) to provide CEN/TC 225 with an up-to-date list, before each Plenary meeting, of all Privacy Capability Statements that have been submitted to the RA by RFID product manufacturer;

h) to provide a public source for updated lists of privacy assets, their associated data types (see 12.2), threats (see 12.3), vulnerabilities, and countermeasures (see 12.6).

8.3.3 Appointment

A body approved by CEN BT (Technical Board) shall be appointed to act as the Registration Authority.

Information about the approved Registration Authority, contact details together with the URL for the register of the RFID privacy capability statements are provided in Annex A.

8.3.4 Resignation

If the Registration Authority finds it necessary to resign, 12 months' notice shall be given to the CEN/TC 225 Secretariat. The Secretariat of CEN/TC 225 shall initiate a search for a new Registration Authority. If a new Registration Authority cannot be found within 12 months, the CEN/TC 225 Secretariat shall assume the responsibilities of the Registration Authority on a temporary basis until a replacement is found.

The resigning Registration Authority shall provide all of the prevailing database structure and content to the CEN/TC 225 Secretariat so that it can be transferred with the minimum effect to the new Registration Authority.

8.3.5 Responsibilities of the RFID product manufacturers

Manufacturers of RFID products, as defined in 8.4, are invited to complete an RFID privacy capability statement for each of their products. Sample forms are shown in Annex B, and electronic versions are available from the Registration Authority, whose details are provided in Annex A.

NOTE The actual forms will differ in detail to the samples shown in Annex B, but will be of a similar nature.

RFID product manufacturers need to be aware that while the RFID privacy capability statements are a key component for undertaking the RFID PIA, it is the RFID operator who takes ultimate responsibility for undertaking the PIA, taking into account factors that also include how the RFID products are used.

RFID product manufacturers should consider their role in providing an RFID privacy capability statement as their contribution towards accurate and consistent RFID PIAs for RFID applications using their products. This European Standard places no legal responsibility on the RFID product manufacturer to undertake third party

testing, or even formally certify the submitted RFID privacy capability statement. It is accepted that the information is provided in good faith.

The RFID privacy capability statement shall be completed on a self-declaration basis to the best knowledge of an authorized, and technically competent, person undertaking the task.

8.4 RFID technology privacy capability tools - details

8.4.1 RFID integrated circuit privacy capabilities

The pro forma privacy capability statements for integrated circuits are defined in B.1. These comprise two parts: basic product details and a separate table for the privacy capability statement. Details associated with the tag, such as antenna size and read range capability are addressed in the tag capability statements.

Although the annex describes a generic capability statement, the Registration Authority (see 8.3.2) should prepare pro forma statements for each air interface protocol. This means that such privacy capability statements will only cover the range of potential features that are mandatory or optional for the particular air interface protocol.

8.4.2 RFID tag privacy capabilities

The tag privacy capability statements not only address the features of the tag, but make reference to the integrated circuit being used. The pro forma privacy capability statements are defined in Annex B. These comprise two parts: basic product details and a separate table for the privacy capability statement.

Although the annex describes a capability statement for a particular air interface protocol, the Registration Authority (see 8.3.2) should prepare pro forma statements for other air interface protocols. This means that such privacy capability statements will only cover the range of potential features that are mandatory or optional for the particular air interface protocol.

8.4.3 RFID interrogator privacy capabilities

The pro forma privacy capability statements are defined in B.2. These comprise two parts: basic product details and a separate table for the privacy capability statement.

Although the annex describes a generic capability statement, the Registration Authority (see 8.3.2) should prepare pro forma statements for each air interface protocol. This means that such privacy capability statements will only cover the range of potential features that are mandatory or optional for the particular air interface protocol.

8.4.4 The default privacy capability statement

In the situation where one or more of the device-based privacy capability statements is missing for a particular application, a default privacy capability statement should be used. The default privacy capability statement is based on the protocol specification using the pro forma in Annex B. This annex defines the default privacy capability for ISO/IEC 18000-63; the pro forma for other air interface protocols can differ.

The set of default privacy capability statements will be available on the register and will clearly identify only the mandatory privacy features supported by a particular standard. As this default statement cannot identify optional features of proprietary features built in by the device manufacturer, RFID operators should be encouraged to obtain more factual information from their suppliers.

8.4.5 Using CEN/TR 16672 to construct privacy capabilities for products using proprietary protocols

CEN/TR 16672 identifies the privacy capability characteristics for a known range of RFID technologies. On this basis, the features that it identifies should be used for constructing the privacy capability statements for proprietary products and air interface protocols.

The manufacturers of RFID products that are based on entirely proprietary technology are still expected to support the RFID PIA process, but the RFID privacy capability statements associated with their products are only required to be shared with customers using their products in RFID applications. Any manufacturer that incorporates a proprietary privacy feature in an RFID product and declares this in a publicly available product specification should prepare a privacy capability statement for submission to the Registration Authority.

8.5 Templates

8.5.1 General

The purpose of a template is to reduce the effort of producing a PIA report for RFID operators that share some common features in their RFID application.

The use of a template should be considered where a logical cluster of similar RFID applications implemented by organizations with a common function and / or built around a specific RFID application standard. A template is also relevant to address a logically similar function that employs RFID data capture.

Examples include, but are not limited to:

— airline baggage handling;

— conference and exhibition badges;

— contactless payment systems;

— employee access control systems;

— inventory control and stock taking;

— libraries using RFID for circulation and other control purposes;

— retail applications for a particular market sector;

— RF-based membership cards, for example for leisure centres;

— RF contactless cards in public transportation systems;

— RFID apps on mobile phones.

RFID operators should be involved in the creation of a template as this can lead to increased trust in such a PIA. Commercially sensitive data does not have to be disclosed while societal representatives participate in the template creation.

Where such a template exists, the RFID operator shall use a Single European-wide template. As such a national template should not be used, other than to provide language specific requirements.

8.5.2 Developing a template

Consideration should be given to determine whether a European-wide template is appropriate.

As a guideline, templates may be prepared in any number of formats and in different degrees of detail (as determined by the capability and experience of the body preparing the template:

— As a pro forma of a PIA report to be used by individual RFID operators having applications with common features.

— As an analysis of the privacy risks of particular data elements.

— Addressing part of the PIA process, as defined in Clauses 9 to 12, preferably progressing in the sequence of the clauses.

— Addressing one or more of the layers in the RFID system stack.

— Preparing miscellaneous tools, guidelines, or test procedures that address specific aspects of the PIA process.

8.5.3 Who should prepare the templates?

Templates may be prepared by a key membership organization, or a limited number of membership organizations, to which many of the RFID operators in the sector belong. This fact means that the different RFID operators in the sector will have some common purpose and basic rules by which they can co-operate, yet (where necessary) remain competitive. There is no requirement for such organizations, and therefore the templates they produce, to be established on a pan-European basis, although this is desirable wherever possible.

An organization representing RFID operators may develop the template, as follows:

— It can be based on an established common set of RFID implementations, which can enable the template to be developed based on contributions from experience.

— It can be prepared in parallel to the development of a common RFID application, or data content standard. This will ensure early consideration of privacy features as the standard is developed.

— Solution providers can also prepare templates.

Where solution providers have a membership organization (e.g. trade association or professional body) such an organization should take the lead in developing a template. However, because of the competitive nature in the marketing of some applications, an alternative approach is for individual companies to prepare a template for their customer base.

A solution provider, or representative organization, can develop the template:

— based on an established product or function, which can enable the template to develop based on contributions from experience;

— in parallel to the development of new product launches, this will ensure early consideration of privacy features as products are launched on the market.

8.5.4 The role of stakeholders in template development

It is good practice to involve stakeholders in privacy impact assessments. However there might be difficulties should there be direct involvement by stakeholders in an application operator's PIA process when commercially sensitive information be involved.

To address this issue stakeholders should be invited to participate in PIA template development where commercially sensitive information for an individual operator does not need to be included. Stakeholder

participation in template development can build greater trust and completeness in PIAs that make use of such templates.

It is desirable from the perspective of many stakeholders that templates are applicable as widely possible across Europe to ensure consistency of approach.

9 RFID PIA - a process approach

9.1 Introduction

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 person, or can be associated with a person.

In addition, RFID-related data is held on the application system. Generally speaking, the Data Protection Directive defined in 95/46/EC addresses this data. However, the implementation of RFID presents a more complex position where both internal and external risks need to be taken into account in a coordinated manner. For example, a vulnerability of RFID such as being able to read data from a tag might increase the threat of an attack on the application system. But if the RFID operator increases countermeasures 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.

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-effectiveness analysis of the risks and countermeasures. Without this the appropriate selection of countermeasures cannot be made. The emphasis on “methodical cost-effectiveness analysis” is intended to place the PIA in context.

EXAMPLE A medical centre that processes thousands of RFID transactions a week of pharmaceutical items is expected to undertake a more rigorous RFID PIA than a retail processing the same number of grocery transactions a week. This is because the pharmaceutical items create what Directive 95/46/EC defines as an association indirectly to a person's “physical, physiological, mental” identity.

It is important for the RFID operator to integrate the PIA process into the application development. The RFID operator should designate a person or group of persons to be responsible for undertaking the RFID PIA, and to be responsible for reviewing the PIA and the continued appropriateness of the technical and organizational measures to ensure the protection of personal data and privacy.

9.2 Process Steps

A number of process steps shall be followed when undertaking the RFID PIA. These are:

a) STEP 0: Prepare the RFID functional statement. In a number of applications, this is the only requirement and is effectively the same as having to undertake no RFID PIA.

b) STEP 1: Prepare a detailed description of the application.

c) STEP 2: Identify and assign a risk value to the privacy assets as follows:

   1) the personal privacy assets of an individual in possession of an RFID tag used by the RFID application, and also in the individual's possession beyond the bounds of the application;

   2) the organization’s assets that might be implicated with a privacy breach or loss of personal data associated with RFID data processing.

d) STEP 3: Identify and assess the threats to the privacy assets. This applies to individual assets beyond the domain on the application, i.e. ensuring the privacy protection is addressed. It also applies, and is linked to, threats to sets of personal data held by the RFID operator / data controller.

e) STEP 4: Identify the vulnerabilities associated with the threats and assets.

f) STEP 5: Carry out a risk assessment of the assets, where risk is a function of (asset, threat, vulnerability), taking account that there can be a number of risks.

g) STEP 6: Identify existing and new countermeasures that can be applied to mitigate risks.

h) STEP 7: Determine the residual risks. If assessed too high re-start from step 2.

i) STEP 8: Complete and sign-off the RFID PIA report.

j) STEP 9: Complete and endorse the RFID PIA summary report to be made available in the public domain.

Annex C shows a flowchart of the entire PIA process.

Annex D shows how different organizations can contribute to developing templates.

To compensate for every individual RFID operator having to go through the entire process, the tools defined in Clause 8 are intended to reduce the work content for the individual RFID operator when undertaking the RFID PIA. However, this does imply that templates shall be developed with significantly more rigour using more expertise and identifying more risks. This does not mean that an RFID PIA template will necessarily expose more residual risks. Instead, the fundamental purpose is to provide both RFID operators and individual citizens with greater assurance that the RFID PIA has considered a range of issues.

9.3 Achieving the correct level of detail

9.3.1 General

It is recognized that a challenge in undertaking an RFID PIA is to determine the level of detail necessary to undertake such a process. While this could be based on the scale of the RFID application, this is not an appropriate way to assess risk. Depending on the application, a micro-business could expose risks for an individual as significant as those of a major organization.

The PIA Framework suggested four levels of PIA (0 to 3) and explicitly stated “Industry may further refine these levels and how they impact the PIA process with further experience.” This European Standard does not change the number of levels, but as discussed in the sub-clauses below, does refine what each level means with reference to the process steps defined in 9.2. The personal privacy assets and data types associated with the RFID application largely determine the requirement to undertake a level 1, or 2, or 3 PIA. Assets and data types are defined in 12.2.

The following sub-clauses and the flow chart in Annex E define the process for each PIA level.

9.3.2 Level 0 – no PIA

If an RFID tag is not carried by, or is associated with, an individual then the PIA process may stop at step 0. Details of the requirements for preparing the functional statements are defined in Clause 10.

9.3.3 Level 1 – small scale PIA

Where no asset or associated data type on the RFID tag and on the application is defined in the category of personal privacy in 12.2 and the associated annex, the remaining risk analysis process is rationalized. Being able to exclude personal privacy data types (or more precisely data types coded as 'PI' and 'PB' in 12.2 and its associated annex) significantly reduces the assessment process. Nevertheless, the PIA process shall consider threats that apply to the air interface for the remaining assets and associated data types (i.e. coded as 'IT', 'RV', 'TH', and 'TL') for both the controlled and uncontrolled domains.

9.3.4 Level 2 – PIA focussed on the controlled domain of the application

This level of PIA is required when the application processes personal data, but such personal privacy data are not held on the RFID tag. The definitions of assets and data types that are in the category of personal privacy

are in 12.2. The risk assessment process for a level 2 PIA is mainly applied to the controlled part of the application, as follows:

— The PIA process is applied to personal privacy assets and their associated data types (or more precisely data types coded as 'PI' and 'PB' in 12.2 and its associated annex) only for the RFID-related data on the application and host computer. Although beyond the scope of this European Standard, there might be other data elements on the application where the data protection requirements also apply.

— The PIA process is applied to all other data types (i.e. coded as 'IT','RV', 'TH', and 'TL') at all layers of the privacy in depth model (Figure 2).

9.3.5 Level 3 – Full scale (complete) PIA of the application

This is the highest level of PIA and is required when the RFID tag holds personal privacy data types coded as 'PI' and 'PB' in 12.2 and its associated annex. The PIA process is applied to all assets associated with the RFID application. All relevant threats shall have their risks assessed at all the layers in the privacy in depth model (Figure 2).

9.3.6 Reducing the effort for the SME organization

All organizations do not have the same resources to undertake a PIA to the same level of detail. This European Standard provides a means for an SME to still undertake a rigorous PIA, but within the recognized constraints of having limited resources.

This effort reduction is because the level of expertise and specialization is less likely in the smallest of organization compared to larger organizations. The reduction in the required effort is applied to assets and their data types as defined in 12.2.3.3 and threats as defined in 12.3.4. Reducing the effort does not reduce the overall risk associated with an RFID application, irrespective of the size of the organization. The SME is only alleviated of additional processing of lower value assets and threats. A larger organization might have the resources to take a holistic view of all the assets and threats and have the resources to establish a project to invoke system changes. The SME might have fewer or no resources to do this, and be completely dependent on hardware, software and consulting advice from the market.

Recommendation 2003/361 defines categories of small and medium-sized enterprises (SME) with the official criteria as shown in Table 2. The main factors determining whether a company is an SME are:

— **number of employees,** and

— either **turnover** or **balance sheet total**.

Table 2 — Official ceiling criteria for SME categories

Company category	Employees	Turnover	Balance sheet total
Medium-sized	< 250	≤ € 50 m	≤ € 43 m
Small	< 50	≤ € 10 m	≤ € 10 m
Micro	< 10	≤ € 2 m	≤ € 2 m
NOTE 1 These ceilings apply to the figures for individual firms only. NOTE 2 These ceilings were re-affirmed in 2012; see http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/.			

For this European Standard the size of the organization in terms of employees is a relevant criterion because it reflects whether there is a dedicated job function with responsibilities for privacy. Similarly, turnover can be considered as relevant in terms of the market impact of the RFID application. The balance sheet is not relevant. By applying the official criterion for employees, the ability to undertake a PIA is taken into

consideration, but this is over-ridden if the organization has a large turnover with the implication that the RFID application has a larger market impact.

9.4 Process methodology

The process methodology is based on security risk assessment processes specified in ISO/IEC 27005, adapted for RFID privacy and is designed to assist the satisfactory implementation of RFID privacy based on a risk management approach, which considers:

— assets;

— threats;

— vulnerabilities;

— existing and new countermeasures.

The scope of the RFID privacy risk management process needs to be defined to ensure that all relevant assets are taken into account in the risk assessment. These assets comprise of two classes:

— the personal privacy assets of an individual holding an RFID tag associated with the RFID application;

— the organizational assets that might be implicated with the loss of privacy and or personal data, such assets being internal to the organization operating the RFID application.

These are discussed in more detail in 12.2.

For clarification personal privacy assets include those RFID identifiable items:

— carried by a person for personal purposes;

— held in the individual's home, or other residence;

— kept in an individual’s car;

— used for work and taken home (as part of working terms and conditions);

— that are part of a larger object or machine used by the individual for personal purposes (e.g. car wheel tags);

— any other situations when the RFID tag is carried by or can be associated with a person.

Threats have the potential to harm privacy assets whether those of the organization or the individual. Threats can be accidental or deliberate and can arise from within or from outside the organization. Threats are discussed in more detail in 12.3.

The existence of vulnerabilities does not cause harm in itself, as there needs to be a threat present to exploit it. A vulnerability that has no corresponding threat may not require the implementation of a countermeasure, but should be recognized and monitored for changes. Vulnerabilities can be related to properties of assets that can be used in a way, or for a purpose, other than that intended for the asset. Vulnerabilities are discussed in more detail in 12.4.

The RFID operator should identify existing countermeasures to avoid unnecessary work or cost, e.g. in the duplication of countermeasures. Privacy by design has been cited as a means of controlling RFID risks, but often the term is wrongly applied to a redesign of the technology itself. This European Standard is based on the fundamental premise that it also has to be applied to the technology as it exists. Within this framework an RFID operator can make choices of technology, and within the chosen technology the RFID operator can

choose equipment. Even within this choice, countermeasures can be applied in one part of the system to help reduce risks in another. Countermeasures are discussed in more detail in 12.6.

ISO/IEC 27005 defines a matrix that takes into account assets, threats and vulnerabilities. This is shown in Table 3. The European Network and Information Security Agency (ENISA) also uses this risk management methodology.

Table 3 — 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 risk assessment methodology linked to this table is as follows:

1) assign privacy asset values {0, 1, 2, 3, 4} as defined in 12.2;

2) assign threat values {low, medium, high} as defined in 12.3;

3) assign a value for degree of vulnerability {low, medium, high} as defined in 12.4 to the threat level;

4) read down the column for the threat / vulnerability to the row identifying the asset value to determine the risk value.

For each asset, the relevant threats and their corresponding vulnerabilities are considered. If there is a vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk (but care should be taken in case this situation changes). The appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the likelihood of the threat occurring and the ease of exploitation.

EXAMPLE If the asset has the value 3, the threat is “high” and the vulnerability “low”, the measure of risk is 5. Assume the same asset with a value of 3, but the threat is reduced to “medium” by some change of countermeasure and the vulnerability “low”, the measure of risk is 4.

10 Preparing the RFID functional statement

Some companies and organizations are RFID operators in the sense of the Recommendation (see 6.3) but do not have a need to be concerned about privacy in the sense of Directive 95/46/EC. Although these RFID operators use RFID technology, their tags are never directly in the possession of a person, even though the RFID tags may be close to a person, but in a narrowly defined environment or application, generally not associated with public exposure or access.

EXAMPLE 1 A dairy farmer could have all animals in the herd either with an RFID bolus in the stomach or an RFID ear tag. Although the farmer comes into daily contact with his cattle, this type of application is considered as not requiring an RFID PIA because of the closed nature of the farm. In contrast, an RFID application for identifying pets generally has a direct one-to-one relationship with a pet owner and such an application is in the public space, and this application should

be the subject of an RFID PIA. The RFID PIA for pets is an example of the potential for a template to be developed by organizations providing such solutions.

EXAMPLE 2 In manufacturing, warehousing, and distribution systems amongst many others, employees come into close contact with RFID tags on containers. If there is no linkage of the RFID data capture system to individual employees, then this class of application does not require a PIA. However, if the RFID tag is used for some means of productivity or piecework control, then the RFID PIA is required. The RFID PIA for a productivity or piecework control is an example where this might best be undertaken at the organizational level, with staff (or representative organizations) participating as stakeholders.

EXAMPLE 3 Having an RFID tag on a product on a manufacturing production line will generally mean that the specific manufacturing application does not require a PIA. However if the product subsequently enters the supply chain so that the tag could eventually be in the possession of a person (e.g. a consumer) then a PIA is required. In some cases the manufacturer will know that it is manufacturing and distributing a consumer product. In some situations the manufacturer has no detailed knowledge of all the ultimate end-point of its products and whether the retailers are or are not RFID operators as defined by the Recommendation (see 6.3). A retailer that is not an RFID operator but sells the product with an RFID tag is unable to undertake a PIA and take the necessary actions which result from it. Therefore the manufacturer is responsible for undertaking an RFID PIA. The RFID PIA for a manufactured product is an example of the potential for a template to be developed by organizations representing a particular manufacturing sector. For example, even though manufacturers may use the GS1/EPC global system for encoding their products, the selected data elements, privacy risks and countermeasures might differ for grocery products, food products that comply with religious or ethnic requirements, clothing, or pharmaceutical products.

The product manufacturer's responsibility for undertaking an RFID PIA is made clear in Point 10 of the Recommendation, which states:

> When conducting the privacy and data protection impact assessment as referred to in Points 4 and 5, the operator of an application should specifically determine whether tags placed on or embedded in products sold to consumers through retailers who are not operators of that application represent a likely threat to privacy or the protection of personal data.

All that the manufacturer can do is carry out the PIA for the data encoded on the tag taking account of the tag technology selected. There is no requirement to understand subsequent applications, just the risks of the data on the tag, and the risk of this being read in the uncontrolled domain

Where a PIA is assessed as not being required, it is advisable for any RFID operator to prepare an RFID functional statement, as set out in Annex F, which identifies basic technical features and details of the application. Such a document could be prepared as a template by an industry organization, and therefore the RFID operator would only need to carry out the minimum amount of work to indicate that the RFID application complied with the RFID functional statement.

If, at some stage in the future, the RFID application is deemed by a competent authority to require even the minimum RFID PIA process, then this functional statement provides the basis for beginning that process. Another trigger to consider the need for a PIA is if any of the conditions defined in 7.3 apply.

11 Preparing the description of the RFID applications

11.1 Introduction

This clause identifies factors that shall be taken into consideration to prepare the RFID application description defined in Annex G. If a template exists and provides the description of the application, this may be used after checking that it is appropriate for the specific application. Modifications shall be made as necessary.

11.2 Multiple applications

An RFID operator may be responsible for more than one RFID application. The following list identifies some of the criteria that may be used to identify whether multiple RFID applications are in place:

— There is a known existence of templates, which differ in functionality.

— The applications make use of different air interface protocols, as defined in Table 1. Because of the fundamental difference in the air interface protocols, separate PIA processes shall be undertaken.

— The function of the application is controlled by different ownership e.g. in financial services, contactless payment cards are owned by the issuer and used by the identified or identifiable person. A four-party model (the merchants, the financial schemes, the issuers and the acquirers) is involved in the overall processing of the financial transaction.

— The applications are for fundamentally different functions such as processing customer transactions and access control for staff.

RFID operators shall develop a separate PIA for each RFID application they operate. If they deploy several related RFID applications (potentially in the same context) they may undertake one PIA process if the boundaries and differences of the applications are explicitly described in the PIA Report. If RFID operators reuse one RFID application in the same way for multiple products, services or processes, they may create one PIA Report for all products, services or processes that are similar (e.g. a car manufacturer deploying the same anti-theft mechanisms in all cars and under the same service conditions).

11.3 RFID application overview

11.3.1 General

The application overview shall provide a comprehensive and full picture of the application, its environment and system boundaries. This shall cover all the functions to which the data is applied, because each of these functions might have associated risks. This needs to be in sufficient detail to address the points under the heading **'RFID application overview'**, as defined in Annex G for the application description. To achieve this the following sub-clauses need to be taken into consideration. All of 11.3 is intended to provide a technical background of the state-of the-art of RFID technology at the date of publication of this European Standard. This background and subsequent developments shall be taken into account in preparing the RFID application overview.

As an internal document there are more details than required for the publicly accessible RFID PIA summary (see Clause 14). While conducting the PIA process this fact needs to be borne in mind. The minimal version of the application overview shall address all the requirements of the RFID PIA summary. A more comprehensive internal version is intended to enable to RFID operator to address RFID privacy on a policy basis.

11.3.2 Determine which RFID technology is intended or being used

The RFID technology being used shall be identified based on the air interface protocol. This is necessary because the air interface protocol can be a significant factor on contributing to privacy. Table 1 identifies the core reference standards together with some related standards names and the frequency at which the protocol operates.

If the RFID operator is not aware of the specific air interface protocol, or the details are not listed in Table 1, then system providers should be contacted for these details.

Particular care needs to be taken when proprietary technology is being used in applications where the RFID tag contains personally identifiable data. The first impression might be that the system is more secure because the air interface protocol and other features are not declared. However, if it is possible to obtain conformant devices then privacy risks might exist. This point also applies to proprietary features added to a base standard.

11.3.3 Determine the RFID components used in the application

Figure 2 identifies all of the layers that need to be considered to assess the privacy risks associated with the RFID technology used in the application. It can be seen that the top four layers are directly concerned with RFID technology, whereas the bottom four layers are concerned with the host computer and application.

Figure 2 has been adapted from ISO/IEC 27005, but with a focus on RFID privacy. In this modified form it is appropriate for this European Standard, which needs to examine the privacy of individuals who interact first with the periphery of the application and also carry RFID identifiable items beyond the operational boundary of the application's RFID readers.

RFID operators shall consider RFID privacy not just from one perspective, but as a pervasive layered approach. RFID privacy shall be comprehensive across all layers. Adopting a layered approach is considered to be privacy in depth. The privacy in depth principle represents the use of multiple privacy and security techniques and countermeasures to help mitigate the risk of one component of the system being compromised or circumvented.

Figure 2 also illustrates the amount of control that an RFID operator can exercise on a layer. Generally, the RFID operator has less direct control on the upper layers and greater control on the lower layers.

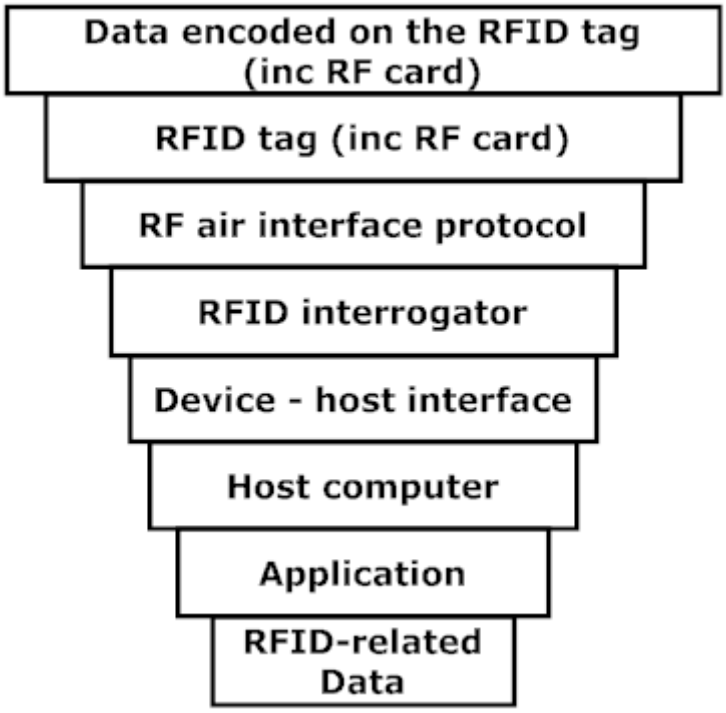

Figure 2 — RFID privacy in depth model

Each of the layers has implications that need to be considered by the RFID operator as follows:

— **Data encoded on the RFID tag**: In a closed system, the RFID operator can be in direct control of the data encoded on the RFID tag. In an open system the data elements are likely to be defined by some standard. Where this is the case this shall be stated, together with the data elements that are encoded. In many applications the RFID operator is dependent on another organization determining the data encoded on the tag (e.g. in a supply chain situation, or for contactless payment cards). In such cases the application description shall declare what encoded data is under the direct control of the RFID operator.

  An additional factor that shall be considered is that when the RFID tag leaves the application domain, the person carrying such a tag has privacy considerations that need to be taken into account.

— **The RFID tag** (the combination of the chip and antenna) is a key technology component in an RFID system. To assist RFID operators to understand the privacy capabilities of their tags, they should seek details from the register of RFID product privacy capabilities (contact details are provided in Annex A); or if the specific tagged product is not listed, then from their technology vendor. As with the data on the tag, in certain circumstances an RFID operator has no control over the specific tag products being selected by other stakeholders in the system. If the product information cannot be obtained easily, then the lowest common denominator of privacy associated with the tag needs to be used for the purpose of the RFID PIA process. This is also provided on the register.

— The **RF air interface protocol** is the technology identified in 11.3.2. The air interface protocol itself can have certain features that expose the tag to an attack such as eavesdropping or a man-in-the-middle attack. Because many air interface protocol standards define some features as optional in conformant RFID tag and readers, these need to be considered as qualifiers to the air interface protocol.

— The **RFID interrogator** is a key device to preserve the integrity of the next layers for the RFID application itself. It can be considered as the default level for privacy provisions. For example, an application might have two different types of tags compliant with the air interface protocol, one with more privacy capabilities than another. If the RFID interrogator has no commands or other features to support the higher level of privacy and security in the tag, then those features are effectively null and void.

  At the time of writing, one of the emerging challenges that face RFID operators is the increased use of RFID interrogators that do not belong to the RFID operator (e.g. smart phones and portable devices that are increasingly RFID-enabled). Such devices can increase the functionality of an RFID system, but they also can present privacy and security threats both to the RFID operator and to tags that leave the RFID operator's domain.

— The **device-to-host interface** is the communication protocol from the RFID interrogator to the host computer. If such devices are on a wired network, then radio-based risks are reduced but nonetheless suitable device authentication methods should be in place. The situation can be quite different where the RFID interrogator communicates wirelessly with the host computer. If the RFID operator owns the RFID interrogators, there are opportunities for implementing device authentication. Conversely, this means that where devices are not owned by the RFID operator, or their use is not controlled or even permitted by the RFID operator, greater care needs to be taken. Unauthorized devices can be both a risk to privacy and, probably more importantly for the RFID operator's perspective, a security risk.

— The **host computer** generally falls within the responsibility of the RFID operator's security management system.

— The **application** also falls within the scope of the RFID operator's security management procedures.

— **RFID-related data on the application**. This data generally falls under the RFID operator's responsibility for adhering to data protection regulations. However, in the case of RFID-related data, there is the potential of information held internally when combined with identifiable features on the tag when this tag outside the direct control of the RFID operator resulting in privacy risks.

11.3.4 RFID applications on portable devices

11.3.4.1 General

There are various mechanisms for adding an RFID interrogator to a portable computer or smart phone. This gives rise to a completely different form of application where data can be captured from RFID tags, processed through the application, and possibly make use of other wireless communication protocols to access services, for example from the internet. Many such applications offer the RFID operator some extremely useful functionality. However, the nature of the system architecture brings with it well-known threats to computers that are not so easily addressed as with a more fixed architecture. Consider the following examples.

EXAMPLE 1 The RFID operator of an RFID system allows staff members to use portable devices but does not necessarily have or impose total control of the applications on the device. At the time of writing this European Standard, there is an increasing trend for organizations to adopt a practice known as BYOD (Bring Your Own Device) for various business reasons. If there are no controls on the software, and even hardware that can be attached to devices, then the RFID operator needs to consider the risks involved.

EXAMPLE 2 The RFID operator allows users, or customers, to use their own devices as part of the RFID operation. In this case, not only does the main RFID operator have no means of control over what is on the individual's device, but such devices can lack security features and, worse, contain malware. Depending on the communication protocols used by the main RFID operator, privacy and security can be compromised.

EXAMPLE 3 The third scenario is where an individual is effectively an RFID operator in his or her own right, for example on a smart phone that supports NFC or another RFID air interface protocol. By installing a smart phone app that makes use of RFID technology, such an individual can operate an application that is not necessarily fully understood or sanctioned by the main RFID operator. An example might be capturing RFID data from products for price comparison purposes, which is a small technological step from existing smart phone apps that do this with bar code.

Legitimate apps that might not be authorized are one issue, but some apps can be infected by malware or, worse, be designed to compromise privacy and / or security. An issue of concern, which RFID operators need to address mainly for security purposes, is the fact that most RFID interrogators that are incorporated in portable devices can read and write data. Some protocols restrict the writing of data, but many do not.

In the RFID application overview, details shall be provided of how such devices are used and defines the ownership of the mobile devices being used.

11.3.4.2 The mobile device as a reader or as a tag emulator

As stated in 11.3.4.1, the read/write capability of mobile devices does raise the possibility of vulnerabilities being exploited in the system. Data might be changed on a tag or card without the permission of the RFID operator.

Different vulnerabilities exist where the device supports the dual function of being a reader / writer and additionally can act as a tag emulator. Such devices, operating at 13,56 MHz, exist on a large scale. Examples of relevant standards are the NFCIP-1 and NFCIP-2 protocols.

If the RFID operator of the application expects the mobile device to operate either as a reader or as a tag emulator, but the person holding the mobile device uses the other function, this could cause privacy and security issues that were not anticipated in the original design.

At the time of writing this European Standard, there is no evidence of a mobile device being used as a reader/writer, and additionally as a tag emulator for other RFID protocols. This does not mean that during the life span of this European Standard that such developments will not take place.

11.3.4.3 Mobile devices as relay devices supporting other protocols

Mobile phone devices already support communication protocols beyond those that are essential for a device to operate as a phone (e.g. voice and SMS). These additional protocols include WiFi, Bluetooth and RFID air interface protocols. This also has implications for the interpretation of Figure 2, addressing the RFID privacy in depth model. At any of the interface layers where a wireless protocol might exist, there could be more than one operating in the controlled domain, and more so in the uncontrolled domain.

The use of multiple protocols and de-coupled components is not restricted to any one RFID air interface protocol.

The fact that such relatively inexpensive devices are very rich in the support for features has already led to innovative RFID product developments, where:

a) the smart phone is used as a computer platform,

b) there is a separate front-end RFID interrogator,

c) communication between the RFID interrogator and the smart phone is via Bluetooth,

d) the Internet can be used to access additional data and services.

RFID operators are implementing such devices into systems. Examples include retailers using these de-coupled devices and the communication protocols to check on the availability of a particular size and fit of an item of clothing in a retail store, or for sales representatives to be able to use their smart phones for RFID operations in particular applications. Such innovative use of the technology increases the benefits, but there are also some associated potential risks given that in some circumstances it might be difficult to distinguish between the proper use and improper use of the technology. Therefore, there are some issues that the RFID operator and even the data protection authorities will need to take into consideration:

— de-coupled components that communicate between each other wirelessly might enable surreptitious data capture, for example, the risk of hot listing becomes significantly easier;

— access to an Internet database could be used to look up and filter data captured from RFID tags and improve the chance of identifying a target;

— it might be possible for de-coupled devices to be used for relay attacks;

— all of this could result in exploitation of threats that are considered to require specialist equipment.

11.4 Data on the RFID tag

11.4.1 General

This clause addresses the points under the heading **'Data on the RFID tag'**, as defined in Annex G for the application description. The basic purpose is to list the data elements encoded on the tag. To achieve this part of the report the following sub-clauses need to be taken into consideration.

11.4.2 Determine what inherent identifiable features are possessed by the RFID tag

Given the definition of what is referred to as personal data, RFID operators should take into consideration that many RFID tags contain a unique chip ID. This supports three functions, which can be employed separately or individually, depending on the technology to support:

— the anti-collision process (to enable the RFID reader to communicate with only one tag when many are present);

— tag traceability and, in turn, additional features such as the accurate tracking of the item to which the tag is attached;

— more sophisticated features such as encryption.

Unless this serialized chip ID can be obscured from other RFID interrogators or made more difficult to read, then the tag, when carried by a or can be associated with a person, makes that person identifiable.

Some tags (e.g. some early ISO/IEC 18000-63 products) do not have a unique chip id to support traceability, and only depend on a random code, dynamically changed for successive read/write transactions for the anti-collision purpose. Such tags do not have an inherent identifiable feature. Therefore, it is advisable to state such a fact in the application description if all or most of the RFID tags are not inherently identifiable, independently of the encoded data.

Subclause 8.4.1 describes one way to identify the capability of a particular RFID chip or integrated circuit. If the capabilities of the specific product are not easily accessible from the Registration Authority, then the RFID operator needs to obtain that level of information from the supplier of the RFID tags.

CEN/TR 16672 sets out privacy enhancing capabilities that are supported by RFID air interface protocol standards. RFID operators shall take into consideration that although the feature may be supported by an air interface protocol:

— The specific RFID tag specified for the application might not support the particular feature.

— Even if the RFID tag supports the feature, then the RFID interrogator(s) used in the application might not support the feature. This is more likely to be the case where older generation readers are used with newer generation RFID tags.

— Even if RFID tags and readers support privacy enhancing functions, the RFID operator still needs to consider the business implications of adopting such a feature.

11.4.3 Listing the data elements encoded on the RFID tag

Not all tags in a particular RFID operation will contain the same data elements. This is particularly the case where there is an application standard for RFID that defines some data elements as optional. In such a case, the RFID operator should determine the probability of different data elements being present on the RFID.

For some applications an RFID operator might have no control or no certain knowledge of the data encoded on the RFID tag. In such cases, the RFID operator shall determine whether there is a template available that can provide such information to create the list. If a template is not available in the case where the RFID operator has no knowledge or control of the data on the RFID tag, the RFID operator should report this to the RA.

The data elements shall be subdivided into three classes:

a) the data is not unique (e.g. a batch number, a date);

b) the data represents an identity as discussed in 11.4.4, which can be associated with the person carrying the RFID tag;

c) the data is personal data as defined by the Data Protection Directive 95/46/EC Article 2, and discussed further in 11.4.5.

The data classes (a) to c)) determine the level of detail required for the risk analysis, with any increased requirement from classes a) to c).

11.4.4 Determine whether encoded data can be considered identifiable

In a similar way as set out in 11.4.2, encoded data might be identifiable.

Although the conditions cited above can make the encoded data in an RFID tag identifiable, the key issues that need to be explored in the PIA process are the associated vulnerabilities and threats that can be associated with such an identifiable tag.

Some of the conditions that make the encoded data identifiable when held by a person include the following:

— Any unique identifier that is a serialized retail product code. This might also apply to a book from a particular library, an employee's ID badge for a particular business, an RFID baggage on luggage after arriving at an airport.

— Even if such data is encoded in a manner that requires rules to convert the data into a human readable format, the encoded bits on the tag can still be uniquely identifiable and readable across the air interface.

— Where only a single data element, which in itself is not unique, is encoded there is still the possibility of the data being identifiable, for example based on distribution over time and location.

— In situations where multiple data elements are encoded on an RFID tag, none of which are unique, it might still result in the combination of encoded bits being unique. For example, removing a unique traceability code but leaving a manufacturer's industry identifier, batch number and expiry date encoded in the tag for returns purposes could still render the tag as identifiable.

11.4.5 Determine whether personal data is encoded on the tag

For this clause personal data is restricted to:

— a direct reference to a person such as the person's name, electronic communication name (e.g. e-mail address, social network name);

— an identification code or number that is directly linked to the person (e.g. passport number, membership number, account number);

— encoding on the RFID tag of indirect identifiers such as “factors specific to his physical, physiological, mental, economic, cultural or social identity” as defined in Directive 95/46/EC.

NOTE This means that the indirect identifier, such as an individual's religion, is explicitly encoded on the RFID tag in plain text or by a code value.

This is aligned with the definition of 'personal data' as defined in Directive 95/46/EC, except for the fact that for data protection purposes “identifiable” can be implicit. The indirect identifiers such as “factors specific to his physical, physiological, mental, economic, cultural or social identity” are addressed in more detail as personal behavioural assets, which are discussed in 12.2.2.

This distinction whether these personal behavioural assets are explicitly encoded on the RFID tag or on the application is necessary to comply with the different levels of PIA as defined in the Framework and described in 9.3.

11.5 Additional data on the application

The basic purpose is for the RFID operator to list the data elements used in the application that are associated with the RFID tag, but not encoded on the RFID tag.

In addition to listing these data elements, the RFID operator shall qualify which of the data elements can be considered personal data as defined by the Data Protection Directive 95/46/EC (see 11.4.5). If so, then additional precautions need to be considered as defined in Clause 12, particularly with respect to data retention.

11.6 RFID data processing

The RFID operator (or data processor) shall consider all the flows of data through all the layers, as defined in Figure 2. Particular attention needs to be placed to the reading and writing of data across the two interfaces: the RFID air interface and the device interface between interrogator and application. The RFID operator has greater control over the security of the communication protocol between the interrogator and host computer, and shall document whether these messages are transferred in plain text or are encrypted for additional security.

NOTE Encrypted messages are not required for basic data capture, for example point-of-sale data capture in a retail store, but are more relevant when specific personal data is being transferred.

Communication across a wireless-based device interface should require considerably more attention. The scenarios identified in 11.3.4 should be given particular attention. Whatever the nature of the data, the RFID operator shall consider the RFID privacy implications and should consider the security implications to the system.

This European Standard does not specify any tools or even a basic description to describe the data processing. The RFID operator may choose whatever tools are considered appropriate for the application.

11.7 Internal transfer of RFID data

A clear distinction shall be made between transferring:

— data about products or other objects;

— anonymous or aggregated data associated with individuals;

— data that can be linked to a natural person.

In the first category, normal business procedures should apply and these are beyond the scope of this European Standard. The second category requires compliance with the Data Protection Directive 95/46/EC. The general principle should be to keep this data for the minimum necessary time, but the RFID operator should also restrict access to this data. Therefore, the application description, shall clearly define:

— the identified and / or identifiable personal data involved;

— the type of recipient(s) that have access to the transferred data;

— the purpose(s) for the transfer or access in general; and

— the time span of access to the data.

11.8 External transfer of RFID data

In addition to the details defined in 11.7, the RFID operator shall consider two other conditions concerned with the external transfer of data:

a) the transfer to an organization that is not part of the same legal entity as the RFID operator (i.e. what is generally called third parties, even if there are contractual relationships in place);

b) as (a) but where the data is captured or first processed in the European Union and transferred beyond the boundary of the EU.

As this European Standard is applicable in States that are not members of the European Union, RFID operators in such countries shall determine what national rules apply to the transfer of data beyond the national boundary.

11.9 RFID application description sign off

The appropriate levels of management shall sign off the completed RFID application description. Those signing off should have the necessary skills to understand the RFID application and/or have the authority to require a system change should this be necessary.

12 Risk Assessment

12.1 Procedural requirements derived from the RFID Recommendation

12.1.1 Common procedure requirements for all RFID operators

The Recommendation directly or indirectly sets out the following requirements. These are discussed here with the interpretation and procedure applied for this European Standard:

a) Recommendation 5 (a) states that an RFID operator shall "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".

   1) Explanation: All RFID operators shall evaluate the possibility of monitoring of individuals within their application via RFID tags. Although it is out of their range of influence, they should also consider possible implications of a RFID tag being used to monitor individuals beyond boundaries of their own application.

   2) Procedure: If an RFID tag that has been processed by an application is carried beyond the boundary of that application, the RFID operator shall conduct a privacy risk assessment as defined in Clause 12.

b) Recommendation 7 (c) states that an RFID operator shall identify "what data are to be processed by the application, in particular if personal data will be processed, and whether the location of tags will be monitored".

   1) Explanation: The processing of personal data is a fundamental feature of the RFID PIA in all accepted terms of the definition of personal data in Directive 95/46/EC. The challenge is in interpreting the function of monitoring the location of tags. There are many situations where the location of tags can be monitored with no impact on personal privacy (e.g. the location of an item of clothing on a display rack, the location of a book in a library). There are at least two situations where this changes: where the movement of the RFID tag (or RF card) is monitored and associated with a person, where the RFID tag is in a defined location (not necessarily static) and a transaction takes place that involves identifying the person. In such cases, the explicit consent of the individual is necessary.

   2) Procedure: The RFID operator has a basic responsibility for addressing obvious capture and processing of personal data. In addition, the RFID operator shall consider the privacy aspects of transactional data capture that places the individual at a particular location and time, and shall separately consider any form of monitoring based on the movement of a person carrying one or more RFID tags. While the RFID operator cannot be responsible for monitoring arising from other transactions beyond the boundary of the application, there is a responsibility of advising individuals of such risks and of countermeasures that can be taken.

c) Recommendation 5 (b) states that an RFID operator shall "take appropriate technical and organizational measures to ensure the protection of personal data and privacy". Recommendation 7 (e) states the RFID operator's responsibility for identifying "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".

   1) Explanation: The RFID operator is responsible for assessing all aspects of personal data and privacy within his application. He should also consider possible implications of an RFID tag being read beyond the boundary of his own application.

   2) Procedure: The RFID operator shall identify risks and countermeasures on the internal use of RFID data and related data. The RFID operator shall provide individuals with countermeasure tools or advise on external countermeasures when the RFID tag is beyond the boundary of the application.

The individual should be responsible for ensuring that such countermeasure tools and countermeasures are implemented to preserve his / her privacy.

d) Recommendation 17 states “Member States should co-operate with industry, relevant civil society stakeholders and the Commission to stimulate and support the introduction of the ‘security and privacy by design’ principle at an early stage in the development of RFID applications.”

   1) Explanation: Mention of “the ‘security and privacy by design’ principle” implies more than an expectation on RFID being enhanced, and places a real expectation on countermeasures of various types being implemented throughout the RFID system as defined in 11.3.3.

   2) Procedure: Wherever possible the various tools described in Clause 8 should be employed to achieve some consistency between similar RFID applications and stimulate the development of common and better countermeasures. These same tools might also facilitate a progressive migration to external scrutiny without the imposition of onerous procedures.

e) Recommendation 5 (a) also states “The level of detail of the assessment should be appropriate to the privacy risks possibly associated with the application.”

   1) Explanation: The level of privacy risk needs to be identified before the level of assessment can be determined.

   2) Procedure: If the nature of the data on the tag and /or and or the application is not personal data, as defined by Directive 95/46/EC then narrower scopes and lower levels of risk assessment may be applied.

12.1.2 Requirements for retailers that are RFID operators

The Recommendation directly or indirectly sets out the following requirements. These are discussed here with the interpretation and procedure applied for this European Standard:

a) Recommendation 11 states “Retailers should deactivate or remove at the point of sale tags used in their application unless consumers, after being informed of the policy referred to in point 7, give their consent to keep tags operational. Deactivation of the tags should be understood as any process that stops those interactions of a tag with its environment which do not require the active involvement of the consumer. Deactivation or removal of tags by the retailer should be done immediately and free of charge for the consumer. Consumers should be able to verify that the deactivation or removal is effective.”

NOTE Point 7 of the Recommendation is concerned with transparency. This is addressed by EN 16570 and to some extent by Clause 14 of this European Standard.

b) Recommendation 12 goes on to state “Point 11 should not apply if the privacy and data protection impact assessment concludes that tags that are used in a retail application and would remain operational after the point of sale do not represent a likely threat to privacy or the protection of personal data. Nevertheless, retailers should make available free of charge an easy means to, immediately or at a later stage, deactivate or remove these tags.”

   1) Explanation: Although the actual procedure to deactivate or remove RFID tags at the point of sale is beyond the scope of this European Standard, the decision to invoke or relax the procedure is clearly a factor in the risk assessment procedure.

   2) Procedure: The output of the risk assessment shall clearly state which option has been employed under Recommendation point 11 (generally to deactivate or remove the RFID tag) or point 12 (generally not to deactivate or remove the RFID tag, except as a consumer choice). The RFID operator shall also identify if alternative, possibly intermediate, features are employed.

c) Recommendation 13 states “Points 11 and 12 should apply only to retailers that are operators.”

1) Explanation: This means that for some types of products there will be RFID tags probably held by individuals that have not been subjected to any form of risk assessment by the retailer selling the product.

2) Procedure: There is a situation where a retailer can be both an RFID operator in some stores and not in another where RFID tagged products are sold. In this case, the RFID operator shall assess the privacy risks in each operational situation and define any countermeasures that are implemented. Where an RFID retail operator is aware that the same products are being sold through different retail outlets with no RFID application, this should be noted in the risk assessment. The RFID operator cannot be held responsible for the risks associated by other retailers.

12.1.3 Procedure requirements for manufacturers of products eventually sold to consumers

The Recommendation directly or indirectly sets out the following requirement. This is discussed here with the interpretation and procedure applied for this European Standard:

a) Recommendation 10 states “the operator of an application should specifically determine whether tags placed on or embedded in products sold to consumers through retailers who are not operators of that application represent a likely threat to privacy or the protection of personal data”.

1) Explanation: This clearly applies to manufacturers of such products.

2) Procedure: The manufacturer that attaches or embeds RFID tags on products is an RFID operator and shall undertake the RFID PIA. As Example 3 in Clause 10 clearly indicates, the level of risk assessment will depend on the nature of the product. Templates provided by organizations representing manufactures should be used not only to reduce the work undertaken by each manufacturer, but also to provide a consistent baseline risk assessment.

12.2 Asset identification and valuation

12.2.1 General

For the purposes of this European Standard, assets shall be considered if they are associated with personal identity, which make a natural person identified or identifiable including indirect factors described in the definition of personal data in Directive 95/46/EC. This means that the asset value is not associated with the item to which the tag is attached, unless that “item” is associated with a person. It also implies, particularly when considering the identifiable factors in the definition in Directive 95/46/EC, that not all items of an apparent similar nature, can be considered in the same way. One example is food products prepared to religious rites compared to food products prepared to general European requirements. Another example is a membership card that discloses the age of a juvenile.

The assets shall be considered in two spatial and technological domains:

— The controlled domain, where the RFID operator controls devices and processes and within which the individual is present. In this domain, the RFID operator's organization also needs to fulfil its obligations as a data controller.

— The uncontrolled domain, beyond the system boundary of the RFID operator, but where the individual person carrying an RFID tag that was used in the RFID operator's domain is still exposed to privacy threats. Various points in the Recommendation as discussed in 12.1 make clear that the RFID PIA shall address this domain.

In the process of identifying and determining a value of such assets, the RFID operator may also consider other organizational assets that are more traditionally associated with systems security, for example as identified in ISO/IEC 27005. Considering the two types of asset together might be sensible from an economic and procedural viewpoint, but how this is achieved is beyond the scope of this European Standard. Here, the focus is exclusively on the set of assets that make a natural person identifiable.

12.2.2 Identification of assets

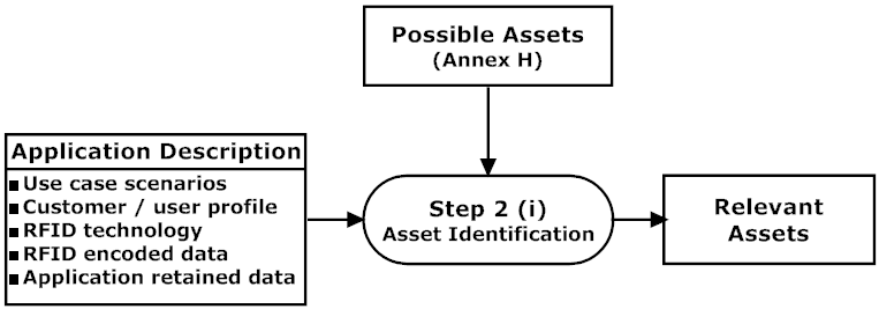

Figure 3 — Flowchart for identifying personal privacy assets

Figure 3 shows a simple flowchart that illustrates the process for identifying personal privacy assets.

The figure shows that the process, defined in this sub-clause, has the application description as a main input. A key part of the process is to consider which of the possible personal privacy assets need further consideration. The output of the process is a set of relevant personal privacy assets that require their risks to be managed.

The definition of personal privacy asset clearly requires those undertaking the RFID PIA to consider the list of possible assets from the perspective of the individual user or customer.

Two categories of assets shall be identified as appropriate for the application, based on the type or implication of the data on the RFID tag or stored on the application:

a) directly identifiable assets, where encoded data includes:

   1) an individual's name;

   2) a unique chip ID;

   3) any identifier that has a one-to-one relationship with the individual.

b) indirectly identifiable factors specific to the individual's physical, physiological, mental, economic, cultural or social identity, as included in Directive 95/46/EC for the definition of person data.

There is a relationship between a personal asset and the associated data.

EXAMPLE A membership card is considered to be a personal asset. It can contain a simple identifier linked to the person in some domain that is not necessarily obvious, or it could be an identifier on a national ID card. The membership card could encode the person's name. If instead it was a contactless payment card then account details will be encoded. The asset that needs to be considered is not the loss of the card, but the loss of the data from the card and the consequences of that loss. When data is read from an RFID tag or RF card it is not removed it is just transferred to another data repository, which might be legal or illegal. It can be seen from the example that even the same data type can provide different levels of precision in identifying a person, as can the number of data elements.

At this stage, the process is not concerned with the risks associated with that data and what might happen if such a data is exposed, nor with whether there are countermeasures in place to protect the data. The requirement is simply to identify personal privacy assets and their associated data.

Annex H identifies a set of personal privacy assets and associated data types. It is not an inclusive list, so the RFID operator shall consider assets from that list and add other relevant assets relevant to the RFID application.

Each asset will probably have more than one data type associated with it. Data types need to be identified for each of the domains described in 12.2. This is important for the PIA process because it determines the level of detail required in the subsequent analysis. All the data types associated with the application should have already been identified in the description of the application (see Clause 11). At this step in the process the RFID operator shall add the designation of data types defined in Annex H. Those data types that are designated as Personal Identifiers (PI) and Personal Behavioural Information (PB), if present on the tag or used in the application, are of critical importance to determine the level of the PIA using the following rules:

c) If any data in the category of Personal Identifiers (PI) and Personal Behavioural Information (PB) is held on the RFID tag, then a level 3 PIA shall be undertaken as defined in 9.3.5.

d) If any data in the category of Personal Identifiers (PI) and Personal Behavioural Information (PB) is not held on the RFID tag but is held on the application in association with any data captured from the RFID tag, then a level 2 PIA shall be undertaken as defined in 9.3.4.

e) If no data in the category of Personal Identifiers (PI) and Personal Behavioural Information (PB) is held on the RFID tag or on the application, then a level 1 PIA shall be undertaken as defined in 9.3.3.

An RFID operator may also include internal assets that could be directly impacted by the exposure of a risk to a personal privacy asset, for example the impact on organizational reputation or the cost of rectifying a privacy breach. A list of such assets is also included in H.2.

12.2.3 Valuing assets

12.2.3.1 General

The next step after asset identification is to assign a particular value to each asset. Figure 4 shows a simple flowchart that illustrates the process for valuing personal privacy assets.

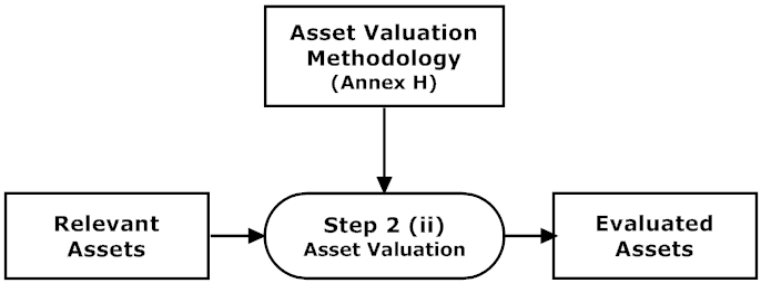

Figure 4 — Flowchart for valuing personal privacy assets

Figure 4 shows that the process, defined in this sub-clause, has the list of relevant assets as a main input. The key part of the process is that the RFID operator shall assign a value to the assets. These values are in the range 0 to 4, as defined in Table 3. The output of the process is a value to each of the personal privacy assets that require their risks to be managed. The criteria used as the basis for assigning a value to each asset should be specified in unambiguous terms. This is often one of the most difficult aspects of asset valuation since the values of some assets may have to be subjectively determined.

12.2.3.2 Valuing personal privacy assets using a data type value

It is fully acknowledged that in the initial period after the publication of this European Standard that evidence-based information will be scarce on what personal privacy assets need to be considered as relevant, and more particularly how to assess the value of these assets. To assist with this, the assets identified in Annex H have been assigned a guideline value, based on the type of data processed by the application and/or encoded on the RFID tag.

The assets are either a tagged artefact associated with a person (e.g. a contactless payment card, a smartphone) or a tagged item (e.g. a retail product, library book). These have been grouped to assist in the identification process. While it is possible to assign values to assets according to its attributes using the scale (0-4) as set out in Table 3, there is a simpler method based on using the data type(s) associated with the specific asset. These data types are those actually encoded on the tag and associated with the RFID application. It is important for the valuation process that all data types associated with the asset are assigned a value. This includes any RFID related identifier such as a chip identifier. At this stage, risks, vulnerabilities and countermeasures are ignored.

The following steps define the process that shall be used:

a) Identify all data types associated with the specific assets being valued, clearly indicating whether the data type is still encoded on the tag after leaving the RFID application and / or whether it is held on the application software.

b) Identify the guideline value assigned to each data type in Table H.3 — Data types and guideline asset value.

c) Use the highest value data type in both the controlled and uncontrolled domains for subsequent processing.

Table 4 shows a hypothetical example of undertaking this task for a membership card, containing more than the basic information.

Table 4 — Example of asset valuation

Asset Code / Description	Data Type on Application Code / Description	Value	Data Type on RFID Tag Code / Description	Value
AP17:Membership card			TH-1: Chip Id	2
	PI-2: Unique membership code	3	PI-2: Unique membership code	3
	PI-12: Photo Id reference	3	PI-12: Photo Id reference	3
	PI-13: Digital photo	4		
	TL-6: Valid dates	1	TL-6: Valid dates	1
	PI-1: Name	2		
	PI-14: Address	2		
	PI-3: Phone number	3		
	PI-4: e-mail address	3		

Based on the data type valuations in this hypothetical example, the highest value (4) on the host application is for the digital photo, but as these are all associated with an individual record, the RFID operator / data controller needs to assess the risk of losing the entire record. There are two data types with a value of (3) encoded on the RFID tag: unique membership code and photo id reference. The data capture threats and vulnerabilities within the controlled application domain will probably be better supported by countermeasures implemented by the RFID operator, than the countermeasures available in the uncontrolled domain when the RFID tag leaves the application. These considerations do not impact on the asset value, and are better addressed when considering the threats and vulnerabilities.

These valuations apply to a single instance of a personal privacy asset, for example the loss of data from a membership card, or the loss of a single record from the host application. The RFID operator then needs to consider the number of each asset that is exposed in both the controlled and uncontrolled domains (see 12.2).

This can have an impact on changing the value of the asset increasing or decreasing its value, or on the score assigned to threats and vulnerabilities.

EXAMPLE Assume that there is a means of carrying out either of the following activities:

— Details of an individual membership card can be captured in the uncontrolled domain by some illegal activity. Details of each card need to be captured individually, and the activity will probably capture a proportion of useless and unrelated data from other tags. In this case, the asset value could be based on a single instance, with the threats and vulnerabilities based on known instances.

— Details of a set of members can be captured illegally from an internal source or even accidentally lost. Besides this being a breach of data protection that is required to be reported, it can be seen that the scale of losing data can be greater in the controlled area of the application. The RFID operator needs to consider that the intended air interface communication and the device to application communication fall within the controlled area, so these need to be considered in addition to traditional data protection features. Here, it is more likely that a set of assets will be lost or illegally accessed, but that the countermeasures put in place will protect the set of records.

12.2.3.3 The process for the SME organization

In line with 9.3.6, a procedure is defined in this sub-clause to minimise the effort that an SME devotes to assessing RFID assets and data types, by reducing the number that need to be taken into account (see Table 5).

Table 5 — Guideline on the number of data types to consider

Enterprise category	Number of data types to be considered [a]
Micro	2
Small	4
Medium	6
[a] If the application has fewer data types than shown for the size of the enterprise, then all the data types shall be taken into consideration.	

In the situation where the size of organization enables fewer data types to be considered, the highest ranking data types shall be considered first. So in an organization that satisfies the small enterprise category, 4 data types are required. For illustration, applying this to the example in Table 4, this means that the highest scoring data type is the digital photo with a data type score of 4. As there are a number of data types with the value of 3, the RFID operator should first select these from the list of data types that are encoded on the RFID tag, and then continue selecting from the data types on the application.

Further procedures are discussed in 12.3.4 for the SME RFID operator to reduce the effort associated with threats.

If the RFID PIA is being undertaken to develop a template, additional consideration should be given to ensuring that all data types that are:

— encoded on the RFID tag shall be taken into consideration;

— designated as Personal Identifiers (PI) and Personal Behavioural Information (PB) shall be taken into consideration.

12.2.3.4 Valuing personal privacy assets in terms of potential business impact

In organizations where security assessments are undertaken, the RFID operator may also consider the potential business impact upon the organization that might result from possible or actual consequences of a

breach of security that result in the loss of personal privacy assets for a number of individuals. Clause H.2 identifies the class of assets that have a direct impact on the organization.

If an RFID operator decides to value assets on the basis described in this sub-clause, then the asset values shall still be in the range 0 to 4, and each of the assets identified in Table H.4 shall be evaluated. If an asset in this table is not relevant to the organization, then this shall be identified as not being applicable. The risk assessment for threats shall still be undertaken based on the procedures defined in 12.3.

The assignment of a value 0 to 4 to organizational assets in both domains (controlled and uncontrolled) is then determined using two criteria:

— the business consequences of loss or compromise of the asset, such as the potential adverse business and/or legal or regulatory consequences from the disclosure, modification, non-availability and/or destruction of information, and other personal privacy assets;

— the replacement value of the asset: the cost of recovery clean-up and replacing the information (if at all possible).

This valuation can be determined from a business impact analysis. The value, determined by the consequence for business, is usually significantly higher than the simple replacement cost, depending on the importance of the asset to the organization in meeting its business objectives. Consequences or business impact may be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or past data.

12.3 Threat identification and evaluation

12.3.1 General

For the purpose of this European Standard, RFID threats have been identified from various sources including research documents because of the absence of a common and official source of RFID threats. CEN/TR 16670 is also a source of threats.

The privacy threats related to RFID applications are associated mainly with the top five layers of Figure 2, which addresses privacy in depth. The threats that are identified are related to personal privacy, but also organizational security. This is because the inter-relationship frequently overlaps between the two types. Also, by identifying threats that some might consider as purely security threats, RFID operators are encouraged to adopt the RFID PIA as a good practice because it provides the additional benefit of protecting organizational assets. If these assets are protected, then there is the probability that the privacy of individuals is protected in the controlled domain of the RFID operator. As RFID applications expand, threats that are currently seen as applicable to the organization might be exploited by attackers in the uncontrolled domain beyond that control of the RFID operator. It is reasonable to consider that as the scale and variety of applications increases, attackers with malicious intent will continually re-assess what is effectively their *return on investment* of such activities. In this sense RFID is no different from any technology that can be exploited. By identifying a comprehensive set of threats this European Standard is intended to provide a foundation for improved risk assessment of RFID threats.

Some of the threats are completely independent of the air interface protocol, whereas others are more directly related to some air interface protocols and not others. They even pose different levels of threat, depending on the technology being used. All of these factors make it difficult for an RFID operator to fully understand the implications of RFID threats. Conversely, by not elaborating on the details and mapping these to specific technologies, this European Standard avoids being a *recipe book* for attackers.

There are also threats that are associated with the application layer but are not associated specifically with RFID. These should be addressed to preserve the privacy of individuals, but are beyond the scope of this European Standard and should be addressed within the domains of:

— security, with reference to the ISO/IEC 2700xx series of standards;

— procedures that have been established to comply with the Data Protection Directive 95/46/EC.

There are currently very few metrics for assessing the level of risk associated with RFID threats, the level of vulnerability associated with specific threats, and even a clear understanding of some of the countermeasures that can be imposed. Therefore, these aspects of this European Standard only claim to provide a foundation, which will require significantly more analysis than provided in the this European Standard.

12.3.2 Identification and classification of threats

Figure 5 shows a simple flowchart that illustrates the process for identifying threats that are relevant to a specific application.

The figure shows that the process, defined in this sub-clause, has the RFID technical specification of the RFID application as a main input. A key part of the process is that the RFID operator shall consider which of the possible threats need further consideration, taking into account the threats identified in this European Standard and from other research sources. The output of the process is a set of relevant threats that require their risks to be evaluated and managed.

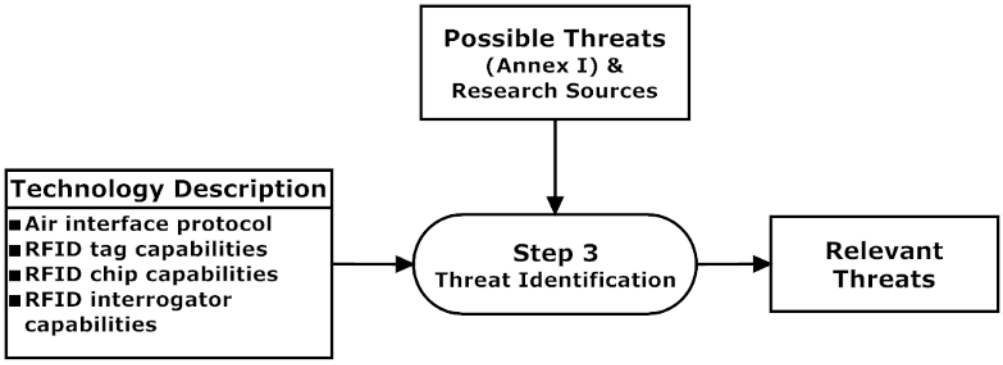

Figure 5 — Flowchart for identifying RFID threats

The RFID threats shall be classified using two vectors. The first vector is associated with defence in depth, and the threats are aligned with the layers in Figure 2 as follows:

— the data encoded on the RFID tag itself,

— the RF air interface protocol,

— the RFID interrogator,

— the device interface between the interrogator and host computer,

— the layers of the RFID system including the host computer, the application and RFID-related data.

There are some threats that cannot be applied at specific layers because the feature that the threat might attack might not be supported at the relevant layer. For example, if an air interface protocol, and /or RFID tag, and / or RFID interrogator do not support cryptography, then the associated threat is not applicable and is not included in the PIA process.

The second vector is concerned with a set of security requirements known as *confidentiality, integrity* and *availability*. In relationship to RFID privacy:

— *Confidentiality* refers to limiting information access and disclosure only to authorized users (effectively the RFID application) and preventing access by, or disclosure to, unauthorized users typically attackers. Confidentiality is of most significance to an individual's privacy where control of who has access to their data are the primary concern.

— *Integrity* refers to the trustworthiness of the information source. RFID systems can be harmed by various techniques intended to convince the RFID tag or RFID interrogator and upper layers of the system that the communications taking place are as intended in the application. 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; similarly, if electronic interference is introduced across the air interface, the presence of the tag will not be detected and therefore not be available.

The RFID threats described in Annex I are presented in a structure aligned with these two vectors.

Depending on the level of PIA, as defined in 9.3, the types of threats and the relevance of those to the layers in the privacy in depth model (Figure 2) may be reduced:

— Where a Level 1 PIA is required, only the threats at the air interface level shall be considered, and for the reduced number of assets and associated data types, i.e. excluding the data types designated 'PI' and 'PB'.

— Where a Level 2 PIA is required, the data types designated 'PI' and 'PB' are known not to be stored on the RFID tag, but are held on the application system. This means the threats that apply to these data types shall be considered only at the layers up to the air interface protocol. The threats of all other data types shall be considered at all layers in the privacy in depth model.

12.3.3 Evaluating threats

The next step after identifying the threats is that the RFID operator shall assign a particular value to each threat that is relevant to the technology used in the application. This is to achieve a score of low, medium or high threat level as defined in Table 3.

One of the challenges faced in developing this European Standard is that the actual incidence of RFID threats is either unknown, or based on academic research. When a threat is exploited in association with a particular application, RFID operators and vendors are, possibly justifiably, reluctant to publicise any facts associated with this. With respect to air interface related threats, measurements presented in CEN/TR 16670 could help in evaluating the threats.

In the absence of evidence-based metrics, this European Standard has taken into account research into the cost of being able to implement a threat using various sources for the cost factors. For example, a low cost is where a threat only requires the use of standard equipment to change encoded data or to read data from the tag. In contrast, a high cost would involve the use of specialist equipment, require specialist knowledge to operate that equipment and probably require detailed knowledge of RFID.

While this approach is simple, it does offer a robust starting point for assessing threats. Effectively:

— a threat that is identified as having low cost to invoke the threat is assessed as having a high risk level;

— a medium cost to implement the threat results in a medium risk level;

— a high implementation cost risk results in a low risk level, based on the fact that cost benefit analysis is not in favour of such a threat.

These threat levels should be considered as guidelines, and as more evidence-based information becomes available about threats, then the details provided in Annex I should be adjusted in undertaking the risk analysis.

12.3.4 The process for the SME organization

In line with 9.3.6, a procedure is defined in this sub-clause to minimise the effort that an SME devotes to assessing RFID threats by reducing the number that need to be taken into account.

As a guide, the number of RFID threats that shall be considered can be determined based on Table 6.

Table 6 — Guideline on the number of RFID threats to consider

Enterprise category		Number of threats to be considered [a]
Micro		2
Small		3
Medium		4
[a] If the application has fewer threats than shown for the size of the enterprise, then all the threats shall be taken into consideration.		

In the situation where the size of organization enables fewer threats to be considered, the highest level threats that are associated with confidentiality (code TTC) and integrity (code TTI) at the tag and tag data level shall be considered first. Then the next selection shall be in the air interface protocol layer for threats identified for confidentiality (code TCC) and integrity (code TCI). If there are still remaining threats to consider to meet the requirement set out in Table 6, then any of the other threats shall be considered.

An RFID operator is free to consider threats associated with availability (codes TTA and TCA) at these levels in the defence in depth structure as described in Figure 2. As these are slightly more associated with security, this is a matter of choice for the RFID operator. The RFID operator may extend the risk analysis to any other threat identified in Annex I.

If the RFID PIA is being undertaken to develop a template, twice as many threats as appropriate for the typical size of organization in the sector shall be taken into consideration. For example, if a trade association has member companies with between 50 and 250 employees, then the template shall consider eight threats.

12.4 Identifying vulnerabilities and enumerating the associated risk levels

12.4.1 Basic procedure

In the same way that there are few or no metrics that are evidence-based for identifying a risk level associated with a threat, equally there are none for vulnerabilities associated with that threat.

As shown in Table 3, the intention is to achieve a score of low, medium or high vulnerability risk level associated with each specific threat. In the absence of any evidence-based assessment of vulnerability, this European Standard identifies a very simple set of guidelines for assessing vulnerability risk levels, as defined in the following steps:

1) If a threat is identified in Annex I or in CEN/TR 16670 and it is feasible to apply this to the RFID technology used in the application, then its vulnerability risk level shall be 'medium' to indicate that the threat and implied vulnerabilities have been identified in research documents. This means that this is the default level of all the threats in that annex is medium, unless over-ridden by the criteria set out in the following steps.

2) If it is unlikely to implement a threat, then the vulnerability risk level shall be defined as 'low'. For example, a crypto attack cannot be implemented on an RFID tag and air interface protocol that does not support cryptographic features. If the threat is possible, then the criteria set out in the next and final step apply.

3) The vulnerability level of 'high' shall only be applied when known exploits have been identified in real applications.

These vulnerability levels should be considered as guidelines, and as more evidence-based information becomes available about threats and vulnerabilities, then the vulnerability levels (low, medium, high) should be adjusted for the particular threat.

It should be in the interest of national Data Protection Authorities to find a means of monitoring incidents where RFID privacy is actually impacted, so that the vulnerability levels can be adjusted in line with evidence.

12.4.2 Procedure to account for exposure time

When a person carries an RFID tag in the uncontrolled domain (beyond the RFID operator's control), the person's privacy is vulnerable. The basic procedure defined in 12.4.1 takes no account of the time that the RFID asset is held by the individual. Certain types of asset are likely to be held on a semi-permanent basis (e.g. contactless payment card, smart phones and membership cards) as other assets are either held for a short or transient time.

Account needs to be taken of these two different time exposures that the individual is exposed to. Although complex metrics could be applied, because the overall risk score is always in the range 0 to 8, a simple guideline is proposed.

For any asset that is held on a transient basis using the guideline of less than 50 days continual exposure, then the asset shall be considered to be held on a transient basis. Such assets are therefore considered to be less vulnerable to attack and the vulnerability level established in the three steps in 12.4.1 should be reduced by a risk of 1.

12.5 Initial risk level

The initial risk level is achieved through the following steps:

1) The RFID operator shall use the highest asset values, as defined in 12.2, taking into account the types of data encoded on the RFID tag and held on the application.

2) Each asset (e.g. a library membership card and a library book) shall have its threats assessed separately because of the possibility of different air interface protocols, tags and interrogators being used. Another important factor to be discussed in 12.6 is that different countermeasures can be applied.

3) The threats are identified against the RFID technology, using rules defined in 12.3.2. Account should be taken of the size of the organization, and therefore skill sets that might be available in addressing the number of threats. For example, an SME formally defined as small should consider at least three threats, each against the assets that are used in the application.

   To achieve this end, threats associated with the RFID tag and the data on the tag and associated with confidentiality and integrity shall be addressed first, then followed by the same confidentiality and integrity threats on the air interface protocol.

4) Each threat that is addressed has the threat level of low, medium or high. This value needs to be taken into consideration separately because the application of countermeasures might well reduce some of the higher level threats and impact on the overall risk level of the RFID application.

5) Determining the vulnerability risk level shall follow the simple rules defined in 12.4. Any of the threats that are identified in Annex I effectively have a default vulnerability level of medium. This shall be adjusted to low if the threat is unlikely to implement in the application. The risk level shall be raised to high if there is evidence of *real world* malicious implementation that is not based on pure academic research.

6) As each threat needs to be considered separately, the process repeats from step 2. The process ends when there is an initial risk value for each threat and each asset. These need to be considered separately because countermeasures have still to be considered and applied.

EXAMPLE To put these steps into context, consider an application where the asset value, determined by the data encoded on the RFID has a value of 2. At this stage, the risk level could be in the range of 2 to 6, as shown in Table 7.

Table 7 — Possible initial risks levels for asset value = 2

	Threat	Low			Medium			High		
	Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	0									
	1									
	2	2	3	4	3	4	5	4	5	6
	3									
	4									

Next the threats are identified and their risk level assessed determined by the RFID technology used. For this example assume that the highest risk level is medium. Applied to the asset value, the risk level could be in the range of 3 to 5, as shown in Table 8.

Table 8 — Possible initial risks levels for asset value = 2, threat level = medium

	Threat	Low			Medium			High		
	Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	2				3	4	5			

The final step is to consider the vulnerability level associated with the risk. For this example assume that the vulnerability risk level is high. Applied to the asset value, and the threat the initial risk level is now set at 5, as shown in Table 9.

Table 9 — Possible initial risks levels for asset value = 2, threat level = medium, vulnerability level = high

	Threat	Low			Medium			High		
	Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	2						5			

12.6 Countermeasures

12.6.1 General

The next step in the procedure is to consider the countermeasures that can be applied to reduce the risk. Countermeasures are placed at this stage in this European Standard because they include a variety of features, which range from:

— those that are embedded in the tags and devices associated with a particular air interface protocol;

— those that are available in the technology but require a conscious action by the RFID operator;

— those that are independent of the hardware and can be implemented by the RFID operator;

— those that the RFID operator can advise the individual about protecting his or her privacy.

A reason for presenting the countermeasures at this stage in the process is that it is intended to help the RFID operator undertaking the first PIA to understand how privacy risks can be reduced. In subsequent iterations of the Privacy Impact Assessment, these countermeasures will already be in place, and therefore the risk factor should have been reduced accordingly from the earlier steps in the process.

12.6.2 Identifying countermeasures

12.6.2.1 General

Figure 6 shows a simple flowchart that illustrates the process for identifying countermeasures that can be applied to the threats identified for the application.

The figure shows that the process, defined in the sub-clause, has the relevant threats that were identified as the output of 12.3. A key part of the process that the RFID operator shall consider is what countermeasures are available to address against the specific threats, with an objective of reducing the risk value. The output of the process is a set of relevant countermeasures that the RFID operator agrees shall be implemented as part of the PIA process.

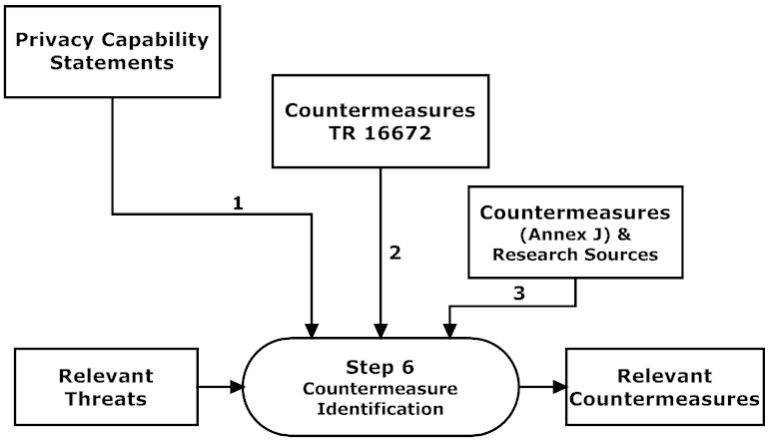

Figure 6 — Flowchart for identifying countermeasures

The countermeasures are identified in Annex J, which:

— presents a list of countermeasures and indicates whether the countermeasure is addressed in the privacy capability statements (Annex B), CEN/TR 16672 or have been identified from research materials;

— identifies a mapping of threats at the different layers in the defence in depth model (Figure 2) with appropriate countermeasures identified for many of the threats.

By considering the countermeasures in the sequence defined in the following sub-clauses, the RFID operator should be able to identify countermeasures against the specific threats that are being considered and assess whether the countermeasure is appropriate to implement in the RFID application. As some threats have a significant number of countermeasures, the RFID operator should consider the feasibility and economics of implementing the individual countermeasure and select the most appropriate countermeasures for the application.

The RFID operator should also take into account the fact that the threats themselves probably vary for different assets, and therefore the countermeasures being applied by the RFID operator might differ for different types of asset. For example, a retailer selling a variety of products might have a very low risk value assigned to the vast majority of products and a higher risk value to just a few. In this case, selectively applying countermeasures to the higher risk assets could be an appropriate course of action that is both economically viable for the RFID operator and reduces the risks to the individual.

12.6.2.2 Countermeasures from the privacy capability statements

The privacy capability statements are specific to RFID tags, integrated circuits, and interrogators, all of which need to be identified for the RFID application. Outline details of the privacy capability statements are in Annex B, and the specific product details should be available from the Registration Authority.

When considering the privacy capability statements relevant to the application, the RFID operator shall take account of the following:

— Generally speaking, the capabilities of the interrogator are the constraining features. For example, if the interrogator cannot support a particular countermeasure, then even if the RFID tag supports this feature the general assumption should be that the countermeasure cannot be used.

— Investments in RFID infrastructure, particularly interrogators, are expected to last for many years. Generally, the oldest device is probably the one that imposes more constraints than others. If the RFID operator is implementing a continual improvement programme installing new devices, then a countermeasure can be considered relevant for the PIA process if applicable to 75 % of the interrogators in the infrastructure. If this guideline is used in the assessment, then this should clearly be stated.

— In a similar way, if the RFID operator has absolute control over the purchase of RFID tags, the tags that are assessed to apply to 75 % of the application may be taken into account in the risk assessment so long as this fact is declared.

— In situations where the RFID operator has no control over the choice of RFID tags, then the tag with the lowest countermeasures should be taken into consideration, representing a worst case scenario. However, if templates are used and reliable statistics can be provided, then the privacy capability statements of more robust tags may be taken into consideration, again with a declaration of the supporting facts.

— The RFID operator also needs to be aware that even if an RFID product supports a particular countermeasure, it may need to be implemented as part of the application. A very simple example is that most RFID tags support the locking of data, which can prevent data modification but if the function is not implemented in the application, then it is effectively null and void.

12.6.2.3 Countermeasures in CEN/TR 16672

Most of the countermeasures that are on the privacy capability statement are drawn from CEN/TR 16672. This provides a description of each countermeasure and also broadly identifies whether the countermeasure is supported by a particular RFID air interface protocol standard. As such, it may be used as a default source of information if the privacy capability statement is not available for a particular product. However, care should be

taken because many of the features specified in an RFID air interface protocol standard are optional and specific products may not support the feature.

CEN/TR 16672 also lists a number of countermeasures that are not explicitly part of the hardware or air interface but which may be implemented to enhance privacy and security by the application. An obvious example is the removal of the tag, which might not be feasible in all applications. Other examples include the use of more sophisticated techniques (e.g. digital signatures), but these are generally only feasible in applications where all tags and readers are under the control of the same system.

12.6.2.4 Other countermeasures

Annex J also currently lists over 20 other countermeasures that have been identified from research.

12.6.3 Reassessing risk levels

If a countermeasure is applied to a given threat, then the guidance that is provided by this European Standard is to reduce the risk level by one unit. This cautious approach is proposed because of the uncertainty of the impact of specific countermeasures against a given threat, given the fact that for some threats a number of countermeasures are possible. They cannot all have equal weight in their success, or in their cost to the RFID application.

If the RFID operator decides to remove, destroy, or render untraceable a tag before it moves from the controlled to the uncontrolled domain, then it is logical to reassign the risk level to zero. However, there are some potential cost implementations in providing full assurance that this is the case. The RFID operator should take into consideration whether the complete elimination of being able to read the RFID tag in the uncontrolled domain can be achieved. If not, then a slightly higher residual risk should be set.

EXAMPLE If an RFID operator uses a command to render tags unreadable, unless a procedure exists to subsequently read all tags after this command has been invoked and prove that the tags are unreadable there is the possibility that some tags are still readable. Evidence exists – not specifically related to privacy - in applications such as libraries where multiple commands need to be invoked that all commands are not invoked on all tags. This is more likely where multiple tags are involved or where the items are not stationary.

For other countermeasures that are intended to make the RFID tag unreadable or extremely difficult to read in the uncontrolled domain, the risk level may be reduced by more than –1, but some residual risk should remain given the impossibility to provide complete assurance. For example, even if an RFID operator provides shielded wallets for membership cards, there is no assurance that the wallet will be used on all occasions. Although this might be made the responsibility of the individual, access to the data on the membership card might still pose a threat to the overall application.

If the risk levels against each threat for each asset are still considered high by the RFID operator, then the PIA process shall be restarted. In addition to considering enhancements to the technology, some assessment should be given to the data held on the tag.

12.7 Residual risks

After the entire process of assessing risks, including eventual iterations of the PIA process, a set of risk levels is derived for each threat for each asset. These are the residual risks for the Privacy Impact Assessment. In addition to being part of the PIA itself, they require to be reported as part of the summary PIA.

At this stage, the RFID operator has enough information to identify a longer term strategy for further reductions to the risk levels by undertaking research and system changes. These objectives should be set out in the PIA report, together with a simple plan for research and implementation of such features. This can include any aspect of the PIA process, including re-evaluating assets, encoded data types and those on the application system, migration to a more robust RFID product, a better understanding of the threats, vulnerabilities and countermeasures.

12.8 RFID PIA endorsement

The appropriate levels of management shall endorse the completed RFID PIA report. Those endorsing the PIA report and PIA summary should have the necessary skills to understand the RFID application and/or have the authority to require a system change should this be necessary.

13 Worked example of the risk assessment process

Annex K provides a worked example to assist with an understanding of the risk assessment process. This covers the process from identifying assets, considering threats, vulnerabilities and countermeasures up to the point of arriving at an application risk score. It also addresses how the effort for the SME can be reduced without compromising the risk analysis

14 The PIA summary report

14.1 PIA report date

This is the date when the PIA was undertaken or reviewed. Ideally this summary should be no older than one year.

14.2 RFID application operator

The four data elements listed on the document in Annex L are the same as for the RFID application operator on the description of the application on the PIA report (see 11.3).

14.3 RFID application overview

There are only three data elements from the same subject area as on the description of the application:

— The purpose(s) of the applications(s) shall address those functions that involve the individual customer, user or citizen from a privacy data and information perspective.

— The geographical scope should identify whether the system operates locally, nationally, or internationally. Ideally in a multi-site operation a list of sites should be available.

— The types of users/ individuals impacted by the RFID application shall clarify whether this applies to all users; e.g. it is impossible to selectively remove RFID tags from library books. If this applies selectively, e.g. to some public transport cards, then options should be defined.

NOTE This is more associated with whether an individual has a choice, rather than the countermeasures that can be exercized (see 12.6).

— If the RFID PIA risk assessment has been undertaken based on a template, this information shall be provided. The intention is to indicate that organizations have co-operated and that higher consistency between the risk assessment is possible.

14.4 Data on the RFID tag

This is the same list of data elements as defined for the description of the application, except that the data elements shall be described in plain language as they need to be understood by the lay person. For example in a retail application the term “SGTIN” (Serialized Global Trade Item Number) is completely understandable to those who know the GS1 system. However an additional explanation can be helpful, e. g. “serialized product code”.

14.5 RFID Privacy Impact Assessment score

The final PIA risk assessment score shall be provided, based on the residual risks. If more than one asset is involved in the application (e.g. an RFID enabled loyalty card or NFC app plus RFID tags on products), then each asset (artefact type) shall be scored separately.

14.6 RFID countermeasures

Two classes of countermeasures shall be reported:

a) list of countermeasures applied by the RFID operator; this may include information as in the following examples:

   1) the chip identifier on a library tag is not stored in the system;

   2) the chip identifier on a travel card is not stored in the system;

   3) the serialized product code is only used for price lookup and not associated with the customer after purchase;

   4) the serialized product code is stored for a period of a number of months appropriate for product recall of pharmaceutical products;

   5) the serialized product code for clothing is stored only for the return period, but the RFID has an implemented password to obscure reading by others;

b) list of countermeasures that the individual should apply to the tags associated with the application; this may include information as in the following examples:

   1) your membership card should be stored in a protective sleeve when not required for use;

   2) the RFID tag on the swing ticket on an item of clothing should be removed as soon as the customer decides to keep the item of clothing;

   3) the RFID sensor tag should remain on the piece of meat to monitor its temperature if kept refrigerated, and not frozen, until prepared for cooking;

   4) the RFID bag tag should be removed from the luggage handle on leaving the secure baggage area;

   5) the RFID tag on the {named class of product} can be deactivated at the special station;

   6) your library membership card can only be activated with an additional PIN number, ensure that you keep this secure.

15 Revision control

While the PIA process should ideally be under continual review, it is accepted that revisions might be periodic or ad hoc. The criteria for a review include:

— significant changes in the RFID application such as expanding on the original purpose;

— changes in the type of information process either as held on the tag or on the application;

— reports of breaches in similar RFID applications;

— the availability of a new or enhanced template;

— the availability of improved RFID technology. However, it is acknowledged that the residual value of existing investments and the migration to the new technology need to be taken into consideration;

— periodically: ideally no more than one year should elapse, the existing PIA should be re-assessed. If no material changes have occurred, then all that is required is to indicate this fact with an updated date.

One factor that has not been taken into account in these criteria is the identification of a new incident that has direct impact on the application. This is discussed in Clause 16.

16 Monitoring and incident response

The RFID operator shall be responsible for monitoring incidents that are either reported or directly associated with the RFID application, or with identical technologies that are being used in the application.

In the absence of ongoing vulnerability reports the RFID operator has the responsibility to carry out due diligence. One way that such a burden could be reduced is for the organizations responsible for developing templates to undertake the task.

Annex A
(normative)

Details of Registration Authority

Details of the Registration Authority are available from the CEN-CENELEC Management Centre (CCMC) website.

You may request information using the following link: http://www.cen.eu/helpers/Pages/contactus.aspx.

Annex B
(informative)

RFID manufacturer's product privacy capability statements

B.1 RFID integrated circuit (chip) privacy features

Table B.1 is a pro forma for the product details to be provided by the manufacturer of the integrated circuit (the chip). It is based on the ISO/IEC 18000-63 structure, and can easily be adapted for other air interface protocols. The Registration Authority (see Annex A) should provide technology specific forms, which might be available on line.

Table B.2 represents all the privacy features addressed in CEN/TR 16672 for all RFID technology at the time of publication of this European Standard. Details of each of the features are described in that Technical Report. The Registration Authority (see Annex A) should provide technology specific forms, which might be available on line. These will only list those features that are supported by the specific RFID air interface technology.

Table B.1 — Product details for the RFID integrated circuit (chip)

Manufacturer	
Product commercial reference	
Product type reference (if different from the commercial reference)	
Complies with standard (use references from CEN/TR 16672 if possible)	
Frequency range	
RFID integrated circuit supported commands (use the command codes in the air interface protocols referenced in CEN/TR 16672 if possible) (e.g. ISO/IEC 18000-63)	
Memory structure [a]	
MB00: reserved memory (size in bits)	
MB01: UII memory, excluding protocol and CRC words (size in bits)	
MB10: TID memory (size in bits)	
MB10: TID memory serialized	Yes / No
MB11: user memory (size in 16-bit words)	
[a] The table illustrates the structure for a segmented tag (e.g. ISO/IEC 18000-63). For tags with a single memory (e.g. ISO/IEC 15693 (all parts)) state size in terms of block size (bytes) and number of blocks, also indicate if separate memories support the AFI and DSFID.	

Table B.2 — Privacy capability features supported by the RFID integrated circuit (chip)

Privacy capability feature	Supported Yes / No
Password protection [a]	
Password protection with security timeout	
Password protection with cover coding [a]	
Cryptographic protection	
Symmetric-key cryptography	
Public-key cryptography	
Application of access protection features [a]	
Unique chip ID or Tag ID [b]	
Chip selection with random number	
Programmable reduced read range	
Untraceable	
Hide	
Kill	
Read (Lock) protection	
Temporary read Lock protection	
Permanent (or Perma) read Lock protection	
Write (Lock) protection	
Temporary write Lock protection	
Permanent (or Perma) write Lock protection	
Verification using a password	
Additional proprietary features supported by the integrated circuit. Please use the names of features defined in CEN/TR 16672 where possible.	

[a] In ISO/IEC 18000-3 Mode 3 and ISO/IEC 18000-6:2004/Amd:2006, the password only protects the reserved memory bank. The cover coding does not help in protecting the consumer privacy as it only applies for protecting the password.

[b] For ISO/IEC 18000-6:2004/Amd:2006, the TID may not be unique as this is not a requirement in the standard, however, most product vendors provide serialization.

Table B.3 is a pro forma for the product details to be provided by the manufacturer of the RFID tag. It is common for all tags.

Table B.4 represents the privacy features addressed in CEN/TR 16672 for all RFID technology at the time of publication of this European Standard. It is based on the ISO/IEC 18000-63 structure, and can easily be adapted for other air interface protocols. The Registration Authority (see Annex A) should provide technology specific forms, which might be available on line. These will only list those features that are relevant to the specific RFID air interface technology.

Table B.3 — Product details for the RFID tag

Manufacturer	
Product commercial reference	
Product type reference (if different from the commercial reference)	
Complies with standard (use references from TR [00225074] if possible)	
Frequency	
Battery assisted passive tag	Yes / No
Active tag	Yes / No
Batteryless passive tag	Yes / No
RFID IC (chip) manufacturer	
RFID IC (chip) manufacturer's commercial product reference	
Type of tag (dry/wet inlay, glass tag, metal mount, etc.)	
Tag size: longer X shorter dimension (mm)	

Table B.4 — Privacy capability features supported by the RFID tag

Privacy capability feature	**Details**
Maximal read range (m) under legal regulations (2W erp)	
Maximal write range (m) under legal regulations (2W erp)	
Delta RCS or load modulation index (following ISO 18046-3)	
Sensitivity degradation	
Polarization (for propagative tags)	
Destruction mechanism of the antenna using some product feature [a]	
Additional proprietary features supported by the tag	
[a] For propagative RFID systems (at frequencies above 400 MHz), the act of cutting the tag's antenna usually drastically reduces read ranges to less than a few centimetres.	

B.2 RFID interrogator privacy features

Table B.5 is a pro forma for the product details to be provided by the manufacturer of the interrogator. It is based on the ISO/IEC 18000-63 structure, and can easily be adapted for other air interface protocols. The Registration Authority (see Annex A) should provide technology specific forms, which might be available on line.

Table B.6 represents all the privacy features addressed in CEN/TR 16672 for all RFID technology at the time of publication of this European Standard. Details of each of the features are described in that Technical Report. The Registration Authority (see Annex A) should provide technology specific forms, which might be available on line. These will only list those features that are supported by the specific RFID air interface technology.

Table B.5 — Product details for the RFID interrogator

Manufacturer	
Product commercial reference	
Product type reference (if different from the commercial reference)	
Complies with standard (use references from CEN/TR 16672 if possible)	
Frequency range	
Interrogator supported commands (use the command codes in the air interface protocols referenced in CEN/TR 16672 if possible) (e.g. ISO/IEC 18000-63)	
Communication interface to the application	
Wired (define)	
USB (version)	
Wireless (define protocol)	

Table B.6 — Privacy capability features supported by the RFID interrogator

Privacy capability feature	Supported Yes / No
Password protection [a]	
Password protection with security timeout	
Password protection with cover coding [a]	
Cryptographic protection	
Symmetric-key cryptography	
Public-key cryptography	
Application of access protection features [a]	
Unique chip ID or Tag ID [b] (see NOTE 2)	
Chip selection with random number	
Reduced read range on the tag	
Untraceable	
Hide	
Kill	
Read (Lock) protection	
Temporary read Lock protection	
Permanent (or Perma) read Lock protection	
Write (Lock) protection	
Temporary write Lock protection	
Permanent (or Perma) write Lock protection	
Tag verification using a password	
Additional proprietary features supported by the interrogator. Please use the names of features defined in CEN/TR 16672 where possible.	

[a] In ISO/IEC 18000-3 Mode 3 and ISO/IEC 18000-6:2004/Am1:2006, the password only protects the reserved memory bank. The cover coding does not help in protecting the consumer privacy as it only applies for protecting the password.

[b] For ISO/IEC 18000-6:2004/Am1:2006, the TID may not be unique as this is not a requirement in the standard, however, most product vendors provide serialization.

Annex C
(informative)

RFID Privacy Impact Assessment flowchart

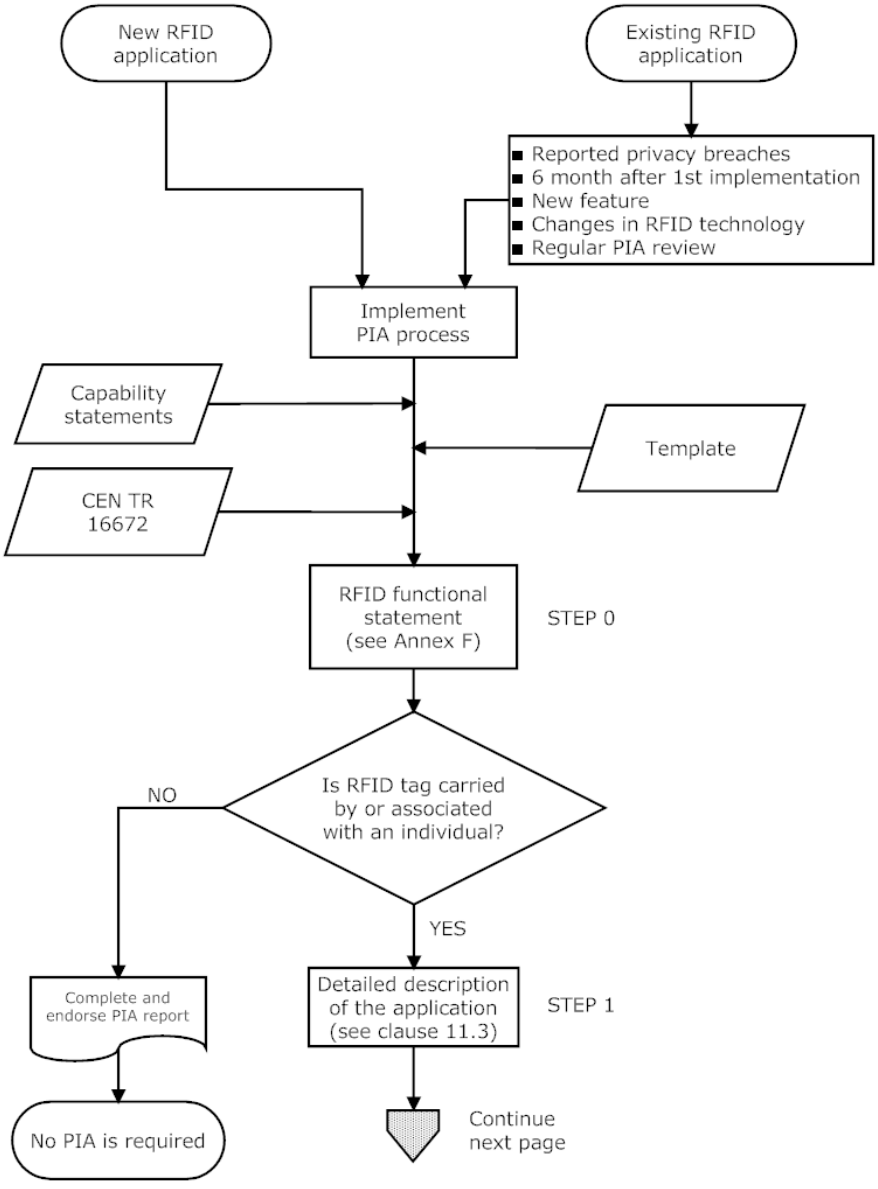

Figure C.1 *(continued)*

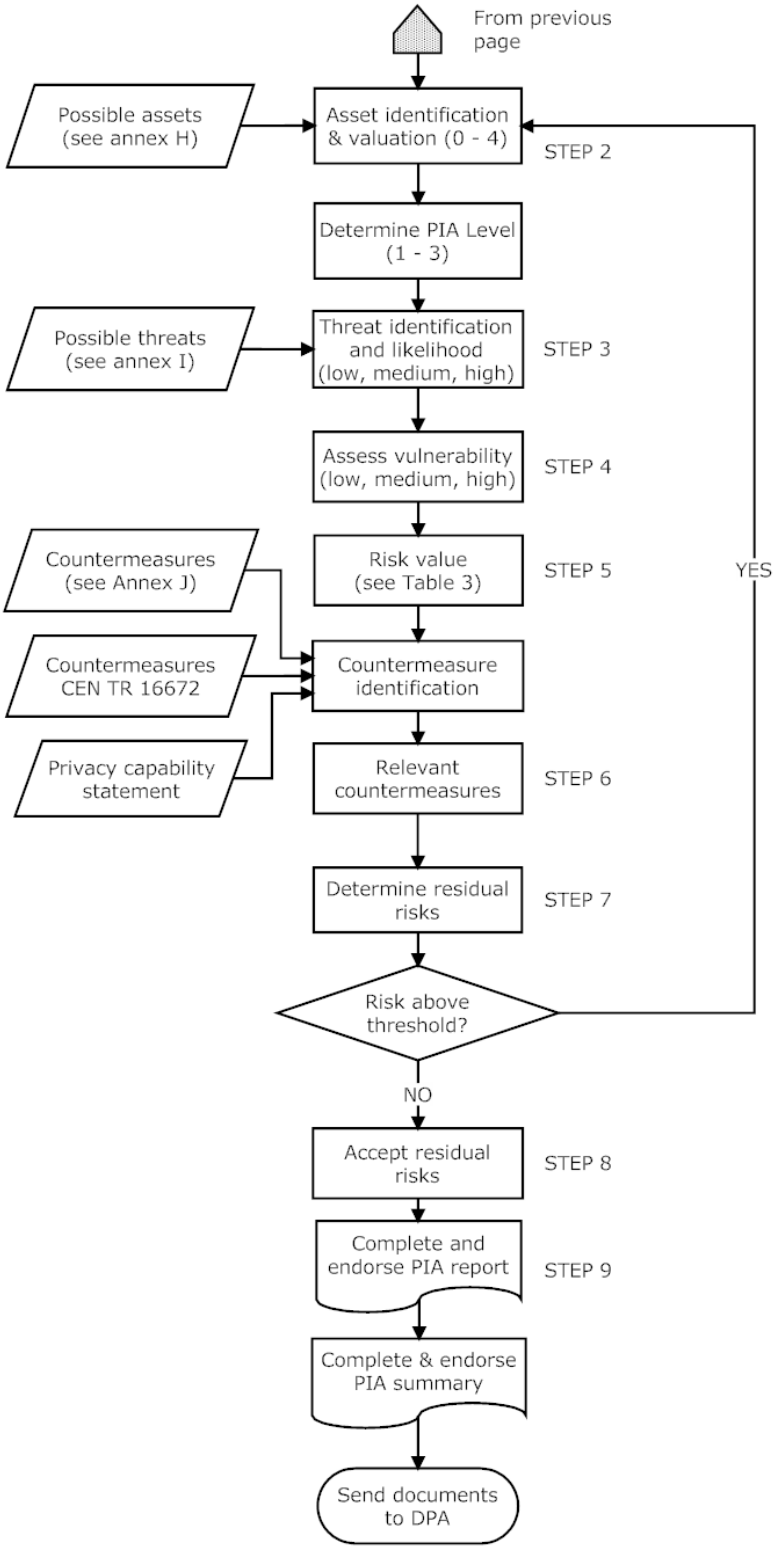

Figure C.1 *(end)*

Annex D
(informative)

Template development

Process Steps (from 9.2)	RFID operator membership organization	RFID solution provider or membership organization	Other solution provider or membership organization	User or employee stakeholder organization
0 Prepare the RFID functional statement	Yes	Possibly, if this is a common application	Possibly, if this is a common application	
1 Prepare detailed description of application	Yes	Possibly, if this is a common application	Possibly, if this is a common application	
2 Identify and assign a risk value to the privacy assets	Yes	Possibly, if this is a common application	Possibly, if this is a common application	Possibly
3 Identify and assess the threats	Possibly, but requires technical knowledge of RFID	Yes	Possibly, but requires technical knowledge of RFID	
4 Identify the vulnerabilities	Yes, because this is currently derived from the threat	Yes, because this is currently derived from the threat	Yes, because this is currently derived from the threat	Yes, because this is currently derived from the threat
5 Carry out a risk assessment of the assets, taking account that there can be a number of risks	Partly - requires knowledge of the specific implementation	Possibly - requires knowledge of the specific implementation	Partly - requires knowledge of the specific implementation	
6 Identify countermeasures	Possibly, but requires technical knowledge of RFID	Yes	Possibly, but requires technical knowledge of RFID	Possibly, but requires technical knowledge of RFID
7 Determine the residual risks	Partly, but only the RFID operator is responsible	Possibly, but only the RFID operator is responsible	Partly, but only the RFID operator is responsible	Can contribute to defining an acceptable risk level
8 Complete and sign-off the RFID PIA report	No, only the RFID operator is responsible	No, only the RFID operator is responsible	No, only the RFID operator is responsible	No, only the RFID operator is responsible
9 Complete and endorse the RFID PIA summary report	No, only the RFID operator is responsible	No, only the RFID operator is responsible	No, only the RFID operator is responsible	No, only the RFID operator is responsible

Annex E
(informative)

Flowchart to determine the RFID PIA level

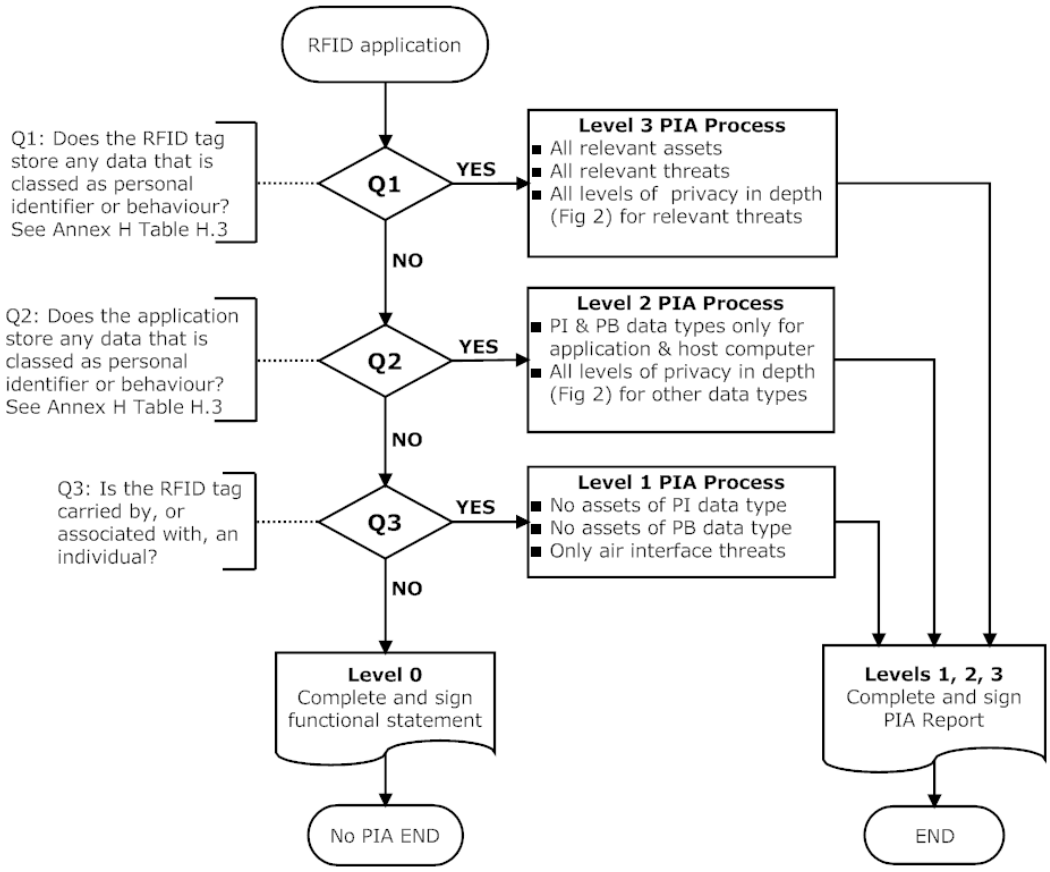

Figure E.1

Annex F
(informative)

RFID functional statement

Statement date	— Date of last change made to RFID functional statement
RFID application operator	— Legal entity name and location — Person or office responsible for RFID functional statement — Point(s) of contact and inquiry method to reach the operator — Reference to a source if the RFID functional statement is based on a template
RFID application overview	— Purpose(s) of RFID application(s), including the functions to which RFID captured data is applied that impact the individual customer, user or citizen — Geographical scope of the RFID application — Types of users/individuals impacted by the RFID application
Data on the RFID tag	— List of encoded data elements used in the application

Annex G
(normative)

RFID application description

PIA report identifier	— Date of last change made to PIA Report — Reference of PIA report, if required by a relevant authority, an internal identifier may be used
RFID application operator	— Legal entity name and location — Person or office responsible for PIA — Point(s) of contact and inquiry method to reach the operator — Reference to a source if the PIA is based on a template
RFID application overview	— RFID application name — Purpose(s) of RFID application(s), including all the functions to which RFID captured data is applied — Geographical scope of the RFID application — Types of users/individuals impacted by the RFID application — Basic use case scenarios of the RFID application — RFID application air interface protocol used — RFID devices used — Access by staff and controls — Access by customers and other users
Data on the RFID tag	— Identifiers that are part of the RFID technology — List of encoded data elements — Presence of identifiable data elements
Additional data on the application	— List of encoded data elements — Presence of identifiable data elements — Data retention of collected data and linking to other held data
RFID data processing	— Description or diagrams of data flows of internal operations involving RFID data
Internal RFID data transfer (if applicable)	— Identified and / or identifiable personal data involved — Type of data recipient(s) — Purpose(s) for transfer or access in general
External RFID data transfer (if applicable)	— Identified and / or identifiable personal data involved — Type of data recipient(s) — Purpose(s) for transfer or access in general

Annex H
(informative)

Identification and valuation of personal privacy assets

H.1 Individually held personal privacy asset

This category of assets comprises those either held by the individual or associated with an individual on a tagged item. The assets are sub-divided into generic types as shown in Table H.1 and Table H.2. The list in these tables is not exhaustive and RFID operators should consider others.

The RFID operator should use both the asset tables to identify assets relevant to the application, taking into account the minimum number of data types recommended for the size of the organization as shown in Table 5.

The associated data is encoded on the RFID tag and / or held on the application controlled by the RFID operator. The data type codes shown in the tables are listed in Table H.3. The codes used are:

— PI Personal Identifier
— PB Personal Behaviour
— TH Tag and Hardware
— RV Residual Value
— TL Time / Location
— IT Identity of Things

Table H.1 — Assets that can directly identify the individual

Code	Asset	Issuer	User
AP1	Passport	Issuing state or national authority	Citizen
AP2	National Id card	Issuing state or national authority	Citizen
AP3	Driver licence	Government	Driver
AP4	Contactless debit or credit card or 'e-wallet'	Issuing bank	Customer
AP5	Medical monitoring device - in-body sensor	Government for public health service, or provider for private health service	Patient
AP6	Medical monitoring device – implant	Government for public health service, or provider for private health service	Patient
AP7	Medical monitoring device – attached and external	Government for public health service, or provider for private health service	Patient
AP8	Medical bracelet (permanently worn)	Company	Patient
AP9	Hospital patient tag	Government for public health service, or provider for private health service	Patient
AP10	Blood donation – during donation	Blood transfusion service	Blood donor
AP11	Embedded chip – non-medical	Government, or provider company	Person implanted
AP12	NFC enabled phone	Generally telecoms provider	Phone owner / user
AP13	RFID enabled phone (not NFC)	Generally telecoms provider	Phone owner / user
AP14	Public transport card – personally registered	Issuing transport authority	Passenger
AP15	Employee access card or badge	Issuing organization or employer	Employee
AP16	Frequent traveller card	Travel organization	Card holder
AP17	Membership card	Issuing organization	Member
AP18	Loyalty card	Issuing organization or retailer	Card holder
AP19	Venue-based trackable bracelets	Issuing organization or venue organizer	Bracelet wearer (could be a child)

Table H.2 — Assets that when held can identify the individual

Code	Asset	Issuer	User
AT1	Blood donation – after donation	Blood transfusion service	Donor and recipient
AT2	Medical test / sample	Health organization (public or private)	Patient
AT3	Prescription medicines and products	Pharmaceutical manufacturer, pharmacy, doctor	Patient
AT4	Pet animal with embedded chip	Government, pet tracing agency, veterinary professional	pet owner, the pet
AT5	Airline baggage tag	Air line	Passenger
AT6	Tagged clothing of a patient or care home resident (e.g. for laundry), excluding any clothing where anonymity is intended	Laundry service / hospital / care home	Patient or resident
AT7	Tagged employee uniform (e.g. for laundry), excluding any clothing where anonymity is intended	Laundry service / employer	employee
AT8	Employee-assigned device	Employer	employee
AT9	Public transport card (not personally registered)	Card travel issuer	Card user
AT10	NFC card / token (not personally registered)	NFC card / token issuer	token holder
AT11	Retail product: food and other products compliant to religious rites	Product manufacturer / retailer	Purchaser, or family members. or friends
AT12	Retail product: Over the counter (OTC) medicines and products	Product manufacturer / retailer	Purchaser, or family members. or friends
AT13	Retail product: clothing and shoe products	Product manufacturer / retailer	Purchaser, or family members. or friends
AT14	Retail product: clothing and shoe products – age related to children	Product manufacturer / retailer	Purchaser (depending on age), or family members. or friends
AT15	Retail product: media products (books, music)	Product manufacturer / retailer	Purchaser, or family members. or friends
AT16	Retail product: “portable” consumer hardware (e. g. phones, computers, music players)	Product manufacturer / retailer	Purchaser, or family members. or friends
AT17	Retail product: “fixed” consumer hardware (e. g. desktop PC, TV, washing machine)	Product manufacturer / retailer	Purchaser, or family members. or friends
AT18	Library book – capable of linking to Data Types PB-3, PB-4, or PB-5	Library	Book borrower
AT19	Library book – other than AT18	Library	Book borrower
AT20	Vehicle immobilisers	Product manufacturer / retailer	Purchaser, or family members. or friends
AT21	Vehicle parts and spares e.g. tyres	Product manufacturer / retailer	Purchaser, or family members. or friends

Code	Asset	Issuer	User
AT22	In-vehicle tags (for tolls, car parks, access)	Service provider	Service user, family members, friends, employee depending on the type of vehicle and driver
AT23	Smart locker	Service provider	Service user
AT24	Visitor card / badge	Card badge issuer	visitor
AT25	Sports or event ticket	Ticket issuer	Purchaser, or family members. or friends

Table H.3 — Data types and guideline asset value

Code	Data Type	Value	Notes / Examples
PI-1	Name	2	
PI-2	Unique personal code	3	
PI-3	Telephone number	3	
PI-4	e-mail address	3–4	Value 4 if explicitly identifying a name; 3 if the name is anonymous
PI-5	Social media name(s)	2–3	
PI-6	Date of birth	2	
PI-7	DNA	4	
PI-8	Biometric finger ID reference	2–3	
PI-9	Digitized biometric finger	4	
PI-10	Biometric facial ID reference	2–3	
PI-11	Digitized biometric facial	3–4	
PI-12	Photo ID reference	2–3	
PI-13	Digitized photo	3–4	
PI-14	Address	2	
PI-15	Citizenship / Nationality	2–3	Possibly more sensitive if the person in not a national
PI-16	Racial origin	2–3	
PI-17	Ethnic origin	2–3	
PI-18	Blood group	2–3	
PI-19	Account details	3	
PI-20	Court offences and proceedings	3	
PB-1	Medical condition	3	
PB-2	Health status (dynamic)	3	
PB-3	Age	2–3	Particularly for juveniles. Children 3 adults 2
PB-4	Sexual orientation	3	
PB-5	Religious belief	2–3	Majority belief in the culture 2 minority belief 3
PB-6	Political affiliation / opinion	2–3	

Code	Data Type	Value	Notes / Examples
PB-7	Trade union membership	1–2	
TH-1	RFID chip ID	2	
TH-2	Mobile phone ID	2–3	Includes codes that are used for communication, device ID, or SIM card: — actual phone number — IMEI – International Mobile Equipment Identity — IMSI – International Mobile Subscriber Identity
TH-3	Media Access Control (MAC) address	2–3	Formats: MAC-48, EUI-48, EUI-64 Used for LAN network, wireless and Bluetooth communication
TH-4	IPv4 / IPv6 address	2–3	For their role as identifiers (many IP addresses are permanently rather than dynamically allocated) potentially all IPv6 addresses are static
RV-1	Residual value on a loyalty card	0–1	This can be a monetary value or the accumulated points on a loyalty card. The value is based on the average residual value.
RV-2	Residual value on a frequent traveller card	1- 4	This can be a monetary value or the accumulated points on a loyalty card. The value is based on the average residual value. As a guide the value 4 equates to a value of € 5000.
RV-3	Residual value on a travel card	1–2	This can be a monetary value as the remaining credit on a travel card. The value is based on the average residual value.
RV-4	Residual value on a financial card or payment phone	1–4	This can be a monetary value as the remaining credit value on a credit card or bank balance on a debit card. The value is based on the average residual value. As a guide the value 4 equates to a value of € 5000.
TL-1	Location	2–3	This can be an identifier of the site where data is captured from the RFID tag –more generic than travel (TL-2 to TL-5) because they can identify regular behaviour
TL-2	Travel: start location	2	
TL-3	Travel: end location	2	
TL-4	Travel route	2	
TL-5	Data and time of travel	2	
TL-6	Valid dates	1	Start and/or expiry date of a service

Code	Data Type	Value	Notes / Examples
IT-1	Unique retail product code	0–3	Value 3 relates to objects that convey beliefs and behaviours value 0 is for everyday items of no privacy concern
IT-2	Unique item code	0–3	Value 3 relates to objects that convey beliefs and behaviours value 0 is for everyday items of no privacy concern

H.2 Assets that apply to the organization

It might be difficult for an RFID operator to value all relevant individually held personal privacy assets associated with the application. It might be easier to identify the possible consequences resulting from a loss of data of the personal privacy assets. Such a loss of data could be due to one or more incidents of data being captured in the uncontrolled domain, where data could be captured illegally, or by a set of data being lost internally within the organization (which might also be deemed to be a breach of data privacy).

The consequences include impacts on the organization's confidentiality, integrity, availability, non-repudiation, accountability, authenticity, or reliability as defined in Table H.4.

Table H.4 — Organizational assets impacted by the loss of personal data

Code	Description
AO1	Infringement of laws / regulations
AO2	Breach of public order
AO3	Financial loss
AO4	Cost of implementing new controls
AO5	Loss of market value of the organization – e.g. significant reduction in share value
AO6	Loss of customer / user income
AO7	Loss of customer / user confidence
AO8	Breach of confidentiality
AO9	Loss of goodwill/negative effect on reputation
AO10	Resignation of key personnel
AO11	Disruption to business activities
AO12	Disruption of internal operation
AO13	Impairment of business performance
AO14	Exposure of customer details

Annex I
(informative)

RFID threats

I.1 Threats associated with the data encoded on the RFID tag and the RFID tag (or RF card) itself

I.1.1 General

The threats listed in Table I.1 are associated with the top two layers of the RFID privacy in depth approach (Figure 2). For reference, all the tag related threats have the code beginning TT. Specifically:

— TTC threats associated with confidentiality at these two associated layers

— TTI threats associated with integrity

— TTA threats associated with availability

The list contains all those threats that have been identified at the time of publication of this European Standard but the list should be extended as new types of threat are identified.

Table I.1 — Threats associated with RFID tags and their data

Code	Description	Threat level
TTC-1	Side channel attack	Low
TTI-1	Physical data modification	High
TTI-2	Cloning	Medium
TTI-3	Spoofing	Medium
TTI-4	Physical tag switching	High
TTI-5	RF tag switching	High
TTI-6	Tag reprogramming	Medium
TTA-1	Tag removal	High
TTA-2	Tag destruction	High
TTA-3	Disabling the tag by command abuse	Medium
TTA-4	Exhaustion of protocol resources	Low
TTA-5	De-synchronization attack	Medium

I.1.2 Side Channel Attack

In a side channel attack, the information that is usually exploited includes timing information, power consumption or even electro-magnetic fields. This type of attack requires sufficient time, specialist equipment, and deep knowledge of the internal systems on which the cryptographic and other algorithms are implemented.

I.1.3 Physical data modification

This is unauthorized changing of encoded data on the tag by deleting, modifying or adding data. It makes use of conventional air interface write commands and standard interrogators. The data might simply be corrupted because the bytes in the air interface command have no semantics, or the changes could be made based on the encoding rules for the application. An example of this second case might be changing a product code to gain some financial advantage. In terms of individual privacy, changing some personal data might restrict access to services, loss of reputation, financial loss and identity fraud.

I.1.4 Cloning

Cloning is one of the impersonation techniques that can used to duplicate data from one tag to another. Data acquired from the tag by whatever means is written to another tag. Unless the technology and application require the interrogator to authenticate the RFID tag, cloning is possible.

Cloning the unique chip ID presents a significantly bigger challenge for the attacker, but some researchers claim that this is possible.

There is also a special case of cloning that needs to be considered where the application accepts multiple AIDC technologies. Cloning data from an RFID-enabled card can be replicated in magnetic stripe.

NOTE In some payment card systems, information that might be cloned from an AIDC card could be used in payment situations known as 'cardholder not present' for purchases made on the Internet or by telephone. In this case, the clone is virtual and requires no encoding on another RFID tag.

I.1.5 Spoofing

Spoofing is effectively a variant of cloning that does not physically replicate an RFID tag. In this type of attacks an attacker impersonates a valid RFID tag to gain its privileges. This impersonation requires specialist equipment to gain full access to the same communication channels as the original tag. This includes knowledge of the protocols and secrets used in any authentication that is going to take place.

I.1.6 Physical tag switching

Tag switching is associated with transferring an RFID tag from one item to another by an attacker in the hope of gaining an advantage, e.g. to purchase a higher value item at a lower price. In the case of membership cards, this could also be to enhance privileges e.g. in a library a juvenile member of a family may use an adult's membership card to access age-restricted material. Other examples might include an underage person using a sibling's membership card to access a club. While this is mainly a security issue for the RFID operator, where cards contain personal information, the threat does impinge on both the victim's and even the attacker's privacy.

I.1.7 RF tag switching

It is also possible to switch the communication between tags by exploiting the air interface protocol. Depending on the protocol used in the RFID application, it is worth noting that switching a tag can occur during one single session. In that case, a communication is initiated with an authorized tag (during handshaking for example) then a bogus tag with different privileges is used for the rest of the communication.

I.1.8 Tag reprogramming

This type of impersonation requires the attacker to acquire new, or reusable, tags that comply with the same air interface protocol as the application being attacked and create 'quasi-compliant' encoded data. This differs from cloning, because the re-programmed tag does not have to be an exact copy, just one that passes as acceptable to the RFID interrogator and application. While many RFID applications, even basic ones, can detect such tags (e.g. because of the use of serialized product codes) there are other applications where reprogrammed tags could be a threat to an organization.

I.1.9 Tag Removal

Unless a tag is permanently affixed to an item, it can be removed. This threat is different from tag switching, because the advantage to the attacker derives from having no RFID tag on the item, which might be theft or other means to deny proper ownership.

In contrast, tag removal can be used as a countermeasure for other threats.

I.1.10 Tag destruction

An RFID tag's functionality can be destroyed or severely restricted by damaging the tag. RFID tags can also be rendered deliberately inoperable by abusing privacy enforcing devices. While this can be seen as a security threat to the RFID operator, there are also situations where it might affect the individual. For example, if a public transport tag is accidentally damaged, then the individual's rights associated with it can be lost.

In a similar manner as for tag removal, tag destruction can be used as a countermeasure to protect the privacy.

I.1.11 Disabling the tag by command abuse

A number of air interface protocols have commands that are designed to perform a particular function. Key examples are writing passwords that control particular functions, such as accessing data on the tag or invoking the kill function on some tags. If the password area of memory is in the null state, an attacker can write a password to the tag that disables its functions within the application. If a password is already encoded on the tag, then there is the likelihood that the same password is used for other items within that RFID application.

The alternative of having multiple passwords carries with it problems of password management. While these features are intended either for privacy protection or security protection, they can also be misused to render the RFID tags inoperable. Identifying the encoded password could be possible using brute-force techniques.

A similar threat applies when the application depends on particular keys, such as the AFI and DSFID. If these are changed, the tag will not be recognized by the application.

I.1.12 Exhaustion of Protocol Resources

There are a number of less typical threats that fall under this category:

— Some less common, but generally secure, protocols that either limit the number of reads or unsuccessful reads before rendering a tag inactive are subject to this threat. When this threshold is reached, the tag becomes unreadable. A special case of this is where the protocol is designed to protect a tag from a privacy attack but based on a limited number of reads using pseudonyms. Once the tag runs out of pseudonyms, the tag is no longer protected.

— Depleting the power of active and passive assisted tags can also shorten their life span, thus exhausting the protocol.

I.1.13 De-synchronization Attack

A very basic de-synchronization attack is one that interrupts the communication transactions from the application and interrogator to the RFID tag. If the attacker successfully destabilises the connection between the tag and the interrogator, the data on the tag is not updated and the tag leaves the read / write zone unaltered.

I.2 Threats associated with the air interface or the device interface communication

I.2.1 General

The threats listed in Table I.2 or the device interface are associated with either the RFID air interface or the device interface of the RFID privacy in depth approach (Figure 2). The similarities are closer where the device interface uses wireless communications. For reference, all the tag related threats have the code beginning TC. Specifically:

— TCC: threats associated with confidentiality;

— TCI: threats associated with integrity;

— TCA: threats associated with availability.

The list contains all those threats that have been identified at the time of publication of this European Standard but the list should be extended as new types of threat are identified. CEN/TR 16670 includes details of practical tests on the ability to illicitly read the data on an RFID tag.

A more complex attack is on reasonably sophisticated protocols that rely on a form of synchronization between the tag and the interrogator/server. Where an attacker prevents the synchronized update of, for example, counters, time stamps, pseudonyms or keys, then the interrogator might no longer be able to read or recognise the tag.

Table I.2 — Threats associated with the RFID air interface or the device interface

Code	Description	Threat level
TCC-1	Unauthorized Tag Reading	High
TCC-2	Tracking	Medium
TCC-3	Data linking	Medium
TCC-4	Behavioural Profiling	Medium
TCC-5	Hotlisting	Medium
TCC-6	Eavesdropping or traffic analysis	Low
TCC-7	Power analysis	Low
TCC-8	Crypto attacks	Low
TCC-9	Reverse Engineering	Low
TCI-1	Relay, or man-in-the-middle attack	Medium
TCI-2	Replay Attack	Medium
TCI-3	Message (Re)construction	Medium
TCI-4	Data Modification in the air interface transmission	Medium
TCI-5	Data Insertion in the air interface transmission	Low
TCA-1	Noise	High
TCA-2	Jamming	High
TCA-3	Malicious Blocker Tags	High
TCA-4	Effects of Radio Degradation	Medium
TCA-5	Shielding of Tags	High

I.2.2 Unauthorized Tag Reading

This is sometimes known as “skimming”. Any RFID tag that can be read by an interrogator compliant with the air interface protocol is susceptible to this threat, with the attacker using standard off-the-shelf equipment. An unauthorized read leaves no trace that the activity has taken place on the tag because the bytes (information) encoded in memory remain the same as before the attack.

NOTE Some taxonomies of RFID threats also call this eavesdropping. This European Standards distinguishes unauthorized tag reading as a threat using standard equipment compliant with the air interface protocol, whereas eavesdropping is the monitoring of the radio signals. Furthermore, unauthorized tag reading generally implies tag activation (or powering) of passive battery less tags.

I.2.3 Tracking

Tracking is a continual sequence of unauthorized tag reading and predominantly seen as a privacy threat, but it can impact security too. The threat can be deployed with mobile or fixed interrogators. The challenge for the attacker using mobile devices is the need to filter out tags that are not intended to be tracked. The problem with fixed location tracking is that effectively a spatial network of linked devices needs to be established.

Authorized tracking e.g. of employees in known zones can be beneficial as it has been for years in the mining industry.

I.2.4 Data linking

This is another privacy-related threat associated with unauthorized tag reading. This particular threat depends on capturing (and possibly interpreting) data from various tags associated with an individual or set of individuals. This data is processed in such a way that a profile of the individual(s) can be constructed from the data that is captured. Examples include travel patterns or details of purchased products.

I.2.5 Behavioural Profiling

This is a privacy threat and another variant on unauthorized tag reading. In this threat, the data collected about an individual or a set of individuals is linked to an external source such as a location or time to establish a behavioural pattern.

I.2.6 Hotlisting

Hotlisting is another threat variant of unauthorized tag reading. It can be used to relate an individual carrying an RFID tag to a specific item or location. One motive for an attacker might be to capture information that might be associated with one or few individuals and identify their presence or what they are carrying. This might then result in other forms of attack.

Another attack motive might be more of a security risk for the organization with the RFID application, because the attacker could be creating a list of items of interest.

I.2.7 Eavesdropping or traffic analysis

Eavesdropping is the act of secretively listening to wireless communications without consent using radio receiving equipment of a transmission between an RFID tag and interrogator. This type of attack can be performed in either direction: tag-to-reader and reader-to-tag. As readers transmit information at much higher power than tags, the former are susceptible to this type of attacks at much greater distances and consequently to a greater degree. Eavesdropping is used to monitor or record data across the air interface for one of these purposes:

— collecting the data from the RFID tag;

— determining traffic patterns;

— collecting raw transmissions to determine communication protocols and/or encryption.

In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.

Eavesdropping can be a first step to other threats such as more structured spoofing attacks.

I.2.8 Power analysis

Power analysis is a form of attack that retrieves information by analysing changes in the power consumption of a device. Research has shown that power emission patterns are different when there is an exchange of correct and incorrect password bits or cryptographic keys.

I.2.9 Crypto Attacks

Tags that contain sensitive information are often protected by cryptographic algorithms or even simple passwords. But these can still be exposed to an attack. In this threat, the attacker is attempting to find a security feature such as the password, cypher key, a pseudo-random number generator, hash function, etc. The purpose of the attack is to identify the particular security feature using brute force or other attack mechanisms so that the secret can be disclosed and exploited more easily for the population of the tags within

the RFID application. A brute force mechanism basically produces repeated attempts at cracking the secret code and low level schemes can be solved in a short a time using standard computers.

I.2.10 Reverse Engineering

Reverse engineering is a process of taking something apart to discover how it works. In this case, the attacker has an interest in understanding the security aspects of the air interface protocol to replicate the behaviour in a different manner than intended. Implementing this threat does not necessarily require the high level of skills implied, but the effort to reverse-engineer the tag has to bring some reasonably significant benefits to the attacker.

I.2.11 Relay, or man-in-the-middle attack

To achieve this threat, the attacker needs to place a device, or devices, logically between the legitimate tag and read convincing each end point device that the communication is as intended, when the entire communication is controlled by the attacker. The classic relay attack interposes an impostor tag T_I and an impostor reader R_I between a legitimate reader R_R and tag T_R. In this attack, T_R is made to communicate with R_I and this is linked to T_I with the false message that communicates to R_R; the reverse communication is also possible. The attack has to impersonate each end point to a sufficient level to convince the real end points. This way, the attacker interrupts the legitimate communication path and manipulates the information back and forth between the legitimate RFID devices in real time.

A wrong assumption about a relay attack is that all the devices have to be present and in view of the legitimate user. Research examples have demonstrated that this attack can be invoked at greater distances than the operational read range, because the communication link within the attack does not depend on the RFID air interface protocol of the real tag and interrogator.

I.2.12 Replay Attack

A replay attack is an impersonation that involves the re-sending of valid replies (typically from the tag) and used at a later time. The replies can be obtained through eavesdropping or other attack mechanisms. In scenarios where there is no challenge-response authentication, the attacker's message appears to be valid and is acceptable to the RFID application. This enables the attacker to pose as legitimate by replaying a valid message previously accepted by the RFID interrogator or application and gain access to some resource.

I.2.13 Message (Re)construction

Some protocols include a random session identifier (or nonce) designed to make them resistant to a replay attack. However, in some cases, this uniqueness can be eliminated by analysing several messages allowing for the (re)construction of new valid messages that can be used in impersonation attempts. This allows the attacker to perform a more sophisticated impersonation attack, where a simple replay attack is not sufficient.

An associated threat is where the legitimate nonce, which by definition should be unique and unrepeatable, is generated by a weak pseudo-random number algorithm. In this case the nonce can be re-used with a new or reconstructed message. Such attacks have also been reported as threats in communications between terminals and the application.

I.2.14 Data Modification in the air interface transmission

This particular threat is different from tag reprogramming (see I.1.7), because the data on the tag remains unchanged. The RFID air interface functions by transferring bits in commands and responses. Based on the air interface coding scheme, it is possible to replace or flip bit values in a transmission. Some bit encoding rules in air interface protocols are more susceptible to this type of attack than others.

If the attack is intended to corrupt communication, then any bit values can be changed. If the intention is to impersonate a valid message, then a far more detailed understanding of the application data is required.

I.2.15 Data Insertion in the air interface transmission

This threat is associated with inserting new data into the application by appending data bits in the communication across the air interface. This is a reasonably extreme threat, as one of the means to achieve it, called “racing”, implies. The objective is to use split second timing to hijack the communication session as part of the state changes that the reader performs in the protocol to communicate with the tag. At a critical point in the processing of the states in the protocol the false information is inserted into the process potentially from either end point.

I.2.16 Noise

As a radio system, RFID communications are susceptible to interference known as noise. Most of this is unintentional and a side effect that the technology needs to address for robustness. However, an attacker can identify a source of noise and use this to interfere with the normal of the application. The attack mechanism requires no detailed knowledge of the air interface protocol.

I.2.17 Jamming

Because the RFID air interface protocol depends on radio signals, an attacker can exploit any such signals within the range of the communication between interrogator and tag. Electro-magnetic jamming can be achieved by creating a signal in the same range as used by the reader in order to prevent tags from communicating with the reader.

I.2.18 Malicious Blocker Tags

NOTE Some references refer to this type of threat more generically as a *collision attack*, without mentioning the means of executing the attack.

One of the privacy enhancing devices that has been suggested is for individuals to make use of a so called “blocker tag”. In its privacy-enhancing mode, this appears to the interrogator as an emulation of many tags being present within the reading zone, making it difficult to read the individual's tags.

As with all such devices, an attacker can abuse the same device and make it impossible for a legitimate interrogator to read a legitimate tag and causing the interrogator to stall and achieve a type of denial of service attack.

I.2.19 Effects of Radio Degradation

No RFID frequency can maintain perfect communications in all circumstances. There are negative effects that impact on the quality of communications that include: absorption (water and conducted liquids), reflection and refraction (from metal objects and surfaces), and dielectric effects and frequency in tuning (from plastics or living tissue). Each frequency suffers of these effects in different ways. An attacker can easily use one of these effects associated with the frequency and apply it to the tag to reduce the probability of it being read.

I.2.20 Shielding of Tags

Shielding is the use of mechanical means to prevent the reading of the tag. For example, products that have the functionality of a Faraday Cage are often recommended as privacy enhancing techniques. But just as they might be used to protect an individual's privacy, an attacker may use them to effectively deny presence or availability of an RFID tag.

I.3 Threats associated with the interrogator (or reader)

I.3.1 General

The threats listed in Table I.3 are associated with the interrogator layer of the RFID privacy in depth approach (Figure 2). For reference, all the interrogator (or reader) related threats have the code beginning TR. Specifically:

— TRC: threats associated with confidentiality at these two associated layers;

— TRA: threats associated with availability.

NOTE Currently no threats associated with interrogator integrity have been identified. If so these will be coded as "TRI".

The list contains all those threats that have been identified at the time of publication of this European Standard but the list should be extended as new types of threat are identified.

Table I.3 — Threats associated with the RFID interrogator

Code	Description	Threat level
TRC-1	Side channel attack	Medium
TRA-1	Exhaustion of protocol resources	Low
TRA-2	De-synchronization attack	Low

I.3.2 Side Channel Attack

This threat is similar to that described in I.1.2, except that it is applied to the interrogator.

I.3.3 Exhaustion of Protocol Resources

This threat is similar to that described in I.1.12, except that it is applied to the interrogator.

I.3.4 De-synchronization Attack

This threat is similar to that described in I.1.13, except that it is applied to the interrogator and application server interface.

I.4 Threats associated with the host application

I.4.1 General

The threats listed in Table I.4 are associated with either the host computer, application and stored data layers of the RFID privacy in depth approach (Figure 2). For reference, all the threats related to these three layers have the code beginning TA. Specifically:

— TAC: threats associated with confidentiality;

— TAI: threats associated with integrity;

— TAA: threats associated with availability.

The list contains all those threats that have been identified at the time of publication of this European Standard but the list should be extended as new types of threat are identified.

Table I.4 — Threats associated with the host, application and stored data

Code	Description	Threat level
TAC-1	Privacy and Data Protection Violations	Medium
TAC-2	Compromising of security keys	Low
TAI-1	Buffer overflow attack	Low
TAI-2	Injecting Malicious Code	Medium
TAA-1	Partial denial of service	High
TAA-2	Complete denial of service	Low

I.4.2 Privacy and Data Protection Violations

There is an entire class of threats associated with attacking the application layer to access data. Examples include: profiling, hotlisting and data linking. Other threats can also apply. All such threats should be the subject of specific risk analysis associated with the application and all of the communications that are not directly associated with the RFID system (the top four layers in Figure 2.

The RFID operator should be aware that violations of privacy and data protection on the host application are part of the data protection legal requirements and any such features require notification to the relevant authority.

It should be recognized that a violation in this area can result in the attacker obtaining significantly more data relative to some of the one-at-a-time attacks in the air interface protocol. There is also the potential for such data acquired from the application to be used to implement more specific RFID threats.

I.4.3 Compromising of security keys

Information and material about security keys is often stored on the application on a secure server. However, if such a server can be identified, then it is a prime target for a hacker/attacker to attempt obtain relevant keys associated with the RFID system.

I.4.4 Buffer overflow attack

A buffer overflow is a problem with certain programme languages when writing data to a buffer and the content overflows the buffer's boundary. As such, this is an application layer problem, but it may be exploited by tags with sufficient memory to overload any buffer in place between the RFID interrogator and the application. From an RFID perspective, in certain circumstances the threat is slightly easier to achieve using an emulation of an RFID tag instead of a real tag. The memory capacity of many tags on the market is well within the upper bounds clearly defined by the air interface protocol specifications. If interrogators and middleware have buffers being left unbounded or have no error response for exceeding their bounds, then this attack is possible.

I.4.5 Injecting Malicious Code

Malicious code could be an injected virus, worm or other malware. The capability to achieve this through simple passive RFID tags is low, but with increased memory capacity this could become an increasing threat. In addition, unauthorized smart phones with reading capabilities increase the threat because of the significant processing power available within such devices.

I.4.6 Partial denial of service

A denial of service attack is made to disable the RFID system so that it cannot be used. Flooding and spam attacks can result in the RFID system being temporarily unavailable for normal processing. A particular problem might occur with RFID applications that do not have a procedure of only permitting trusted readers (e.g. smart phones) to interface with the application. Any other reader should be distrusted because it might generate a large amount of traffic within a short space of time.

At a more basic level any of the threats defined as impacting on availability either with the RFID tag or in the communication layer effectively achieves a partial denial of service from the RFID operator's perspective, sometimes without the operator being aware of the fact.

I.4.7 Complete denial of service

If particular programs or other computer elements in the application system are hit by a successful DoS attack (completely unrelated with any RFID communication) the entire system, including the RFID edge data capture, could be rendered inoperable.

Annex J
(informative)

Countermeasures

J.1 List of countermeasures

Table J.1 provides a list of countermeasures that have been identified for RFID technology and applications. The columns of the table provide information as follows:

a) Code – is a simple reference to the countermeasure and used in subsequent tables in this annex. There are no subdivisions in the code structure because some countermeasures may be applied to many threats.

b) Description – this is a commonly accepted description, and those listed for codes C-1 to C-27 (except C-19) are more fully described in CEN/TR 16672. Others are defines in various technical literature.

c) Applies to – refers to the four subsets of the defence in depth model, indicating that the countermeasure can positively impact on specific threats in the layers addressing:

   1) T = the tag and data on the tag;

   2) C = the RFID air interface and also the device interface;

   3) R = the RFID interrogator;

   4) A = the application layers of host computer, application, and RFID-related data.

d) Annex B – a “YES” in this column indicates that the countermeasure is included in the privacy capability statements. The RFID operator needs to bear in mind that the statements are specific to the RFID technology.

e) CEN/TR 16672 — a “YES” in this column indicates that the countermeasure is included in this TR and described in more detail. A “YES-A” indicates that the countermeasure is described in the TR, but that its implementation is not achieved directly by the RFID technology, but by some application rule.

The list of countermeasures may be extended as others are identified.

Table J.1 — List of countermeasures

Code	Countermeasure Description	Applies to:				Annex B	CEN/TR 16672
C-1	Password protection	T	C			YES	YES
C-2	Password protection with security timeout	T	C			YES	YES
C-3	Password protection with cover coding	T	C			YES	YES
C-4	Cryptographic protection	T	C			YES	YES
C-5	Symmetric-key cryptography	T	C			YES	YES
C-6	Public-key cryptography	T	C			YES	YES
C-7	Application of access protection features	T	C			YES	YES
C-8	Chip selection with random number	T	C			YES	YES
C-9	Programmable reduced read range		C			YES	YES
C-10	Untraceable	T	C			YES	YES
C-11	Hide	T	C			YES	YES
C-12	Kill		C			YES	YES
C-13	Read (Lock) protection		C			YES	YES
C-14	Temporary read Lock protection		C			YES	YES
C-15	Permanent (or Perma) read Lock protection		C			YES	YES
C-16	Write (Lock) protection	T				YES	YES
C-17	Temporary write Lock protection	T				YES	YES
C-18	Permanent (or Perma) write Lock protection	T				YES	YES
C-19	Verification using a password	T	C			YES	YES
C-20	Destruction mechanism of the antenna using some product feature		C			YES	
C-21	Destroy tag		C				YES - A
C-22	Remove tag		C				YES - A
C-23	Data protection using the unique chip id	T					YES - A
C-24	Write protection using the unique chip id	T					YES - A
C-25	Write protection using a digital signature in user memory	T					YES - A
C-26	Verification using the unique chip id	T					YES - A
C-27	Verification using the unique chip id and a digital signature	T					YES - A
C-28	Tamper resistant tags	T					
C-29	Limiting electromagnetic emissions	T		R			
C-30	Physical un-clonable function (PUF)	T	C				
C-31	Secure key management		C				
C-32	Limiting the number of unsuccessful reads		C				
C-33	Storing two editions of keys	T					
C-34	Storing two editions of pseudonym values	T					

Code	Countermeasure Description	Applies to:				Annex B	CEN/TR 16672
C-35	Physically shield the tag		C				
C-36	Use of blocker tag		C				
C-37	Optical tamper sensor		C				
C-38	Chip coating		C				
C-39	Distance bounding protocol		C				
C-40	Measuring signal strength and triangulation		C				
C-41	Key updating schemes		C		A		
C-42	Timestamps		C				
C-43	Challenge-response protocols with nonces[a]		C				
C-44	Restricting access to stored personal data				A		
C-45	Firewalls				A		
C-46	Intrusion detection				A		
C-47	Tamper alarm on sensor tag	T					
C-48	Data checking at interrogator or device interface, especially to an application standard				A		
C-49	Rolling codes	T	C	R			

[a] A nonce is an arbitrary number used only once in a cryptographic communication. It is often a random or pseudo-random number, the latter being less robust.

J.2 Threat and countermeasure mappings

To enable the countermeasures to be applied, they need to be considered in association with the threats. Table J.2 to Table J.5 identify the mapping between threats and countermeasures at the different layers of the defence in depth model.

Table J.2 — Threats and countermeasures associated with RFID tags and their data

Threat Code	Threat Name	Countermeasure Code
TTC-1	Side channel attack	C-28, C-29
TTI-1	Physical data modification	C-1, C-2, C-3, C-4, C-5, C-6, C-7, C-8, C-16, C-17, C-18, C-19, C-23, C-24, C-25, C-26, C-27, C-28
TTI-2	Cloning	C-4, C-5, C-6, C-7, C-8, C-10, C-11, C-28, C-30
TTI-3	Spoofing	C-4, C-5, C-6, C-7, C-8, C-10, C-11, C-28, C-30
TTI-4	Physical tag switching	C-28
TTI-5	RF tag switching	
TTI-6	Tag reprogramming	C-1, C-2, C-3, C-4, C-5, C-6, C-7, C-8, C-10, C-11, C-16, C-17, C-18, C-19, C-23, C-24, C-25, C-26, C-27, C-30
TTA-1	Tag removal	C-28, C-47
TTA-2	Tag destruction	C-28
TTA-3	Disabling the tag by command abuse	C-1, C-2, C-3, C-4, C-5, C-6, C-7, C-8, C-10, C-11, C-16, C-17, C-18, C-19, C-24, C-25, C-33, C-34
TTA-4	Exhaustion of protocol resources	
TTA-5	De-synchronization attack	

Table J.3 — Threats and countermeasures associated with the air interface

Threat Code	Threat Name	Countermeasure Code
TCC-1	Unauthorized Tag Reading	C-1, C-2, C-3, C-4, C-5, C-6, C-7, C-10, C-11, C-12, C-13, C-14, C-15, C-19, C-30, C-35
TCC-2	Tracking	Not possible to counter if the tag has a permanently encoded chip id used for anti-collision or another chip id that is not read protected. Otherwise: C-1, C-2, C-3, C-4, C-5, C-6, C-7, C-8, C-9, C-10, C-11,C-12, C-19, C-20, C-21, C-22, C-35, C-36
TCC-3	Data linking	Not possible to counter if the tag has a permanently encoded chip id used for anti-collision or another chip id that is not read protected. Otherwise: C-1, C-2, C-3, C-4, C-5, C-6, C-7, C-8, C-9, C-10, C-11,C-12, C-19, C-20, C-21, C-22, C-35, C-36
TCC-4	Behavioural Profiling	Not possible to counter if the tag has a permanently encoded chip id used for anti-collision or another chip id that is not read protected. Otherwise: C-1, C-2, C-3, C-4, C-5, C-6, C-7, C-8, C-9, C-10, C-11,C-12, C-19, C-20, C-21, C-22, C-35, C-36
TCC-5	Hotlisting	Not possible to counter if the tag has a permanently encoded chip id used for anti-collision or another chip id that is not read protected. Otherwise: C-1, C-2, C-3, C-4, C-5, C-6, C-7, C-8, C-9, C-10, C-11,C-12, C-19, C-20, C-21, C-22, C-35, C-36
TCC-6	Eavesdropping or traffic analysis	C-4, C-5, C-6, C-31
TCC-7	Power analysis	
TCC-8	Crypto attacks	C-4, C-5, C-6, C-31
TCC-9	Reverse Engineering	C-37, C-38
TCI-1	Relay, or man-in-the-middle attack	C-4, C-5, C-6, C-7, C-31, C-32, C-35, C-39, C-40
TCI-2	Replay Attack	C-41, C-42, C-43, C-49
TCI-3	Message (Re)construction	C-43
TCI-4	Data Modification in the air interface transmission	C-43
TCI-5	Data Insertion in the air interface transmission	C-43
TCA-1	Noise	This is an open problem
TCA-2	Jamming	This is an open problem
TCA-3	Malicious Blocker Tags	Detectable, but no countermeasure making this is an open problem
TCA-4	Effects of Radio Degradation	
TCA-5	Shielding of Tags	This is an open problem

Table J.4 — Threats and countermeasures associated with the RFID interrogator

Threat Code	Threat Name	Countermeasure Code
TRC-1	Side channel attack	C-29
TRA-1	Exhaustion of protocol resources	
TRA-2	De-synchronization attack	

Table J.5 — Threats and countermeasures associated with the host, application and stored data

Threat Code	Name	Countermeasure Code
TAC-1	Privacy and Data Protection Violations	C-44, C-45, C-46
TAC-2	Compromising of security keys	C-41, C-45
TAI-1	Buffer overflow attack	
TAI-2	Injecting Malicious Code	C-45, C-48
TAA-1	Partial denial of service	C-45, C-46
TAA-2	Complete denial of service	C-45, C-46

Annex K
(informative)

PIA risk assessment example

K.1 Introduction

This example is based on the membership card example in Table 4. The worked example will progress from asset identification to addressing countermeasures. It will also cover the reduction of effort that may be applied by SME organizations. The reader should understand that as this is an example of a membership card that contains personal identifiers that requires a Level 3 PIA (the highest level).

Some assumptions need to be made about the technology being used, including details that might not be known to the RFID operator. These are:

— The tag being used is ISO/IEC 18000-3 M1 (also known as ISO/IEC 15963). Although this might not offer the highest level of security, the RFID operator purchased the system based on price and service.

— There are no proprietary features on the tag being used.

— As the size of organization (in terms of personnel) increases, so too should the ability to address more complexity. In this case the organization has some form of membership. It is most likely that the larger organization will have more members.

As this is a Level 3 PIA, the following clauses take the PIA process through the layers necessary when considering privacy assessment and protection in depth.

K.2 Ranking the assets

To assist with the process, the data types have simply been ranked from high to low, as shown in Table K.1.

Table K.1 — Asset valuation, ranked by asset value

Asset Code / Description	Data Type on Application Code / Description	Value	Data Type on RFID Tag Code / Description	Value
AP17:Membership card	PI-13: Digital photo	4		
	PI-2: Unique membership code	3	PI-2: Unique membership code	3
	PI-12: Photo Id reference	3	PI-12: Photo Id reference	3
	PI-4: e-mail address	3		
	PI-3: Phone number	3		
	PI-1: Name	2		
	PI-14: Address	2		
			TH-1: Chip Id	2
	TL-6: Valid dates	1	TL-6: Valid dates	1

As this requires a Level 3 PIA, all the data types need to be considered, subject to any concessions for an SME organization, which still need to carry out the risk assessment from the highest scoring data types.

Depending on the circumstances any SME may choose to consider more of the assets, bearing in mind that some threats to the tag data and to the air interface protocol might be the same irrespective of the data. As an example, if unauthorized tag reading is a threat then it applies to all four of the data types in Table K.1. The only difference is that the other data types, having a lower asset value will result in an overall lower risk for these data types. Similar logic applies to the data held on the application. If data is lost or accessed by a hacker, any of the data could be at risk.

These are the considerations for the SME operator:

— The micro business is required to consider at least two data types. *PI-13: Digital photo* has a value of 4 and needs to be considered. There are six data types with a value of 3. The micro business could next select the data type that is present on both tag and application as this is in all the privacy in depth layers. The second data type is *PI-2: Unique membership code* on the RFID tag.

— The small business needs to consider four data types. It could add *PI-12: Photo Id reference* as encoded on the tag, and *PI-4: e-mail address* for data on the application.

— The medium-sized business needs to consider six data types. It adds *PI-2: Unique membership code* and *PI-12: Photo Id reference*.

K.3 Considering threats at the tag layer and air interface layer

The data encoded on the RFID tag and the air interface need to be considered. The threats at these two layers need to be considered together as defined in 12.3.4, taking those with the highest threat at the tag level first, then those classed as high for the air interface before moving to the medium and low threats. This means that the following threats, associated with integrity and confidentiality, need to be considered, ranked in order of high to low:

— High TTI-1 Physical data modification;
— High TTI-4 Physical tag switching;
— High TTI-5 RF tag switching;
— High TCC-1 Unauthorized Tag Reading;
— Medium TTI-2 Cloning;
— Medium TTI-3 Spoofing;
— Medium TTI-6 Tag reprogramming;
— Medium TCC-2 Tracking;
— Medium TCC-3 Data linking;
— Medium TCC-4 Behavioural Profiling;
— Medium TCC-5 Hotlisting;
— Medium TCI-1 Relay, or man-in-the-middle attack;
— Medium TCI-2 Replay Attack;
— Medium TCI-3 Message (Re)construction;
— Medium TCI-4 Data Modification in the air interface transmission;
— Low TTC-1 Side channel attack;
— Low TCC-6 Eavesdropping or traffic analysis;
— Low TCC-7 Power analysis;
— Low TCC-8 Crypto attacks;

— Low TCC-9 Reverse Engineering;

— Low TCI-5 Data Insertion in the air interface transmission.

NOTE 1 The threat *TCC-8 Crypto attacks* is not applicable because cryptographic protection is not supported by the air interface protocol being used in this example. This would be made clear in the privacy capability statements and is also stated in CEN/TR 16672. As such it not a viable threat, nor is the use of cryptographic protection a viable countermeasure.

These are the considerations for the SME as defined in 12.3.4:

— The micro business is required to consider the two highest threats. Of the three at the tag level, based on the descriptions, *TTI-1 Physical data modification* and *TTI-4 Physical tag switching* are the more likely threats to consider.

— The small business needs to consider the three highest threats. So *TTI-5 RF tag switching* should be added.

— The medium-sized business needs to consider the four highest threats. It needs to add the high level threat for the air interface: *TCC-1 Unauthorized Tag Reading*. Smartphones that support the NFCIP-2 protocol are able to read and write to the tag used in this example. Therefore this is a reasonable choice of threat to assess.

NOTE 2 Although the threats are nominally being considered against just those data types determined by the size on business, any threat on data on the tag, or on the air interface applies to any data on the tag, unless there are explicit technology-based countermeasures that enable selective application. The reduction in effort for the SME does not trivialise the PIA or make it superficial. Because the highest value data types and threats are considered, the resultant initial risk score for the application will be the same irrespective of the size of organization.

The organizations that are larger than the SME, by considering more data types and threats, will be better placed to consider privacy in depth from a policy perspective and might be better able to re-design the system. Furthermore the larger organization is likely to impact on more individuals in terms of customers, users, citizens, employees depending on the nature of the RFID application. Such issues, as the numbers of people affected, are an important consideration for the impact on the reputation of the organization. Evidence from the level of fines for breaches of data protection are a reasonable indication of the seriousness of such impacts applicable to an RFID privacy breach.

There are 21 threats listed here, and their value (high. medium, low) is based on a simple cost of implementation at the time of writing this European Standard. Technology evolves, and some of the medium or low level threats could become much more possible to exploit. The following points should be considered:

— If a medium or low level threat becomes possible because of a change in technology, then its use could be scaled up.

— Some applications with higher assets values (determined by their data type values) use the same RFID technology as a more common larger scale application. In the example in this annex, the membership card is based on a popular high frequency air interface protocol. Tags and readers are readily available, so that anyone with malicious intent could carry out tests to assess how to exploit a threat.

This means that in some applications, it could be relevant to carry out the risk assessment on a medium or low ranked threat as a precautionary measure.

K.4 Considering threats at the interrogator layer

Currently there are only three threats identified at this layer

— Medium TRC-1 Side channel attack;

— Low TRA-1 Exhaustion of protocol resources;

— Low TRA-2 De-synchronization attack.

These are likely to need to be considered only by organizations that are larger than the SME, unless there is a specific need to do so. The following are examples where assessing the risk at this layer might be important irrespective of size of organization:

— For an access control system, where staff or members are able to use their own smartphones as card emulators, but where the RFID operator has no control of the type of device or apps that are installed on the device.

— Where the RFID operator provides a smartphone 'app' to enable a customer or member to perform a function *in situ*, but might not be aware of other conflicting apps.

— Where the RFID operator is aware that portable devices are readily available to read and write data to tags, and even though not app has been authorized by the RFID operator, that there is potential for such apps to compromise the privacy of individuals.

K.5 Considering threats at the device interface layer

Threats at this layer should be of concern if the communication at this layer is wireless, and more so if the interrogator devices are smartphones or other mobile devices that are not owned or under the complete control of the RFID operator.

The threats are the same communication threats defined for the RFID air interface, but with the key exception that the protocol is likely to be based on a different technology. In principle, they include the following:

— High TCC-1 Unauthorized Tag Reading;

— Medium TCC-2 Tracking;

— Medium TCC-3 Data linking;

— Medium TCC-4 Behavioural Profiling;

— Medium TCC-5 Hotlisting;

— Medium TCI-1 Relay, or man-in-the-middle attack;

— Medium TCI-2 Replay Attack;

— Medium TCI-3 Message (Re)construction;

— Medium TCI-4 Data Modification in the air interface transmission;

— Low TCC-6 Eavesdropping or traffic analysis;

— Low TCC-7 Power analysis;

— Low TCC-8 Crypto attacks;

— Low TCC-9 Reverse Engineering;

— Low TCI-5 Data Insertion in the air interface transmission.

However, in reality some will differ in their relative importance compared to the same threat applied to an RFID air interface protocol.

K.6 Considering threats at the application layer

The two threats associated with confidentiality are:

— Medium TAC-1 Privacy and Data Protection Violations;

— Low TAC-2 Compromising of security keys.

At this layer, these are the threats more likely to impact on the individual holding an RFID tag or contactless card. As *TAC-1 Privacy and Data Protection Violations* is considered a medium threat and *TAC-2 Compromising of security keys* is a low threat, the PIA process even for any SME primarily involves these threats.

The four threats associated with integrity and availability are:

— Medium TAI-2 Injecting Malicious Code;

— Low TAI-1 Buffer overflow attack;

— High TAA-1 Partial denial of service;

— Low TAA-2 Complete denial of service.

While they have an impact on the individual holding an RFID tag or contactless card for privacy, if any of these threats is invoked the RFID operator is probably at greater risk in terms of system security.

K.7 Considering vulnerabilities

At the date of publication of this European Standard, there is no evidence that any of the threats have been implemented. Therefore, the likelihood is defined as medium or even low, where the threat is considered improbable.

This means that the combination of threats and vulnerabilities is as defined in Table K.2.

Table K.2 — Impact of threats and vulnerabilities on asset values

Threat Level	Vulnerability Level	Impact on Asset Value
High	Medium	+3
High	Low	+2
Medium	Medium	+2
Medium	Low	+1
Low	Medium	+1
Low	Low	+0

K.8 Risk scores after considering all the threats and vulnerabilities

For simplicity in this example it is possible for illustration to take the values from Table K.2 and apply them to the highest scoring threat to determine an overall risk score. In a real PIA process some of the threats might not apply to the particular air interface protocol, the tag or the interrogator (based on details from the privacy capability statements). However, Table K.3 takes the highest value for all the discussions in the previous clauses and applies them to the six data types that the largest SME would need to consider. Micro and small businesses would still result in the same application risk. Larger enterprises would have an extended list of data types enabling greater subsequent analysis of the RFID system.

Table K.3 — Impact of threats and vulnerabilities on the risks of specific data types

Data Type	Asset Value Col 1	Tag Layer Risk Col 2	RFID Air Interface Risk Col 3	Interrogator Risk Col 4	Device Interface Risk Col 5	Application Layer Risk Col 6	Overall Risk Col 1 + highest value in Cols 2–6
PI-13: Digital photo	4	N/A	N/A	N/A	N/A	+2	6
PI-2: Membership code	3	+3	+3	+2	+3	N/A	6
PI-12: Photo Id reference	3	+3	+3	+2	+3	N/A	6
PI-4: e-mail address	3	N/A	N/A	N/A	N/A	+2	5
PI-2: Membership code	3	N/A	N/A	N/A	N/A	+2	5
PI-12: Photo Id reference	3	N/A	N/A	N/A	N/A	+2	5

The table shows quite clearly the difference between the data held on the application and that on the RFID tag and exposed to the air interface protocol.

The RFID operator also needs to consider the time exposures that the individual is exposed to. If less than 50 days continuous exposure then the vulnerability may be reduced by 1 for the two data types encoded on the tag. This will depend on the type of membership organization.

K.9 Applying countermeasures

The application being considered in this annex is for a membership card, with personally identifiable information encoded on the tag. As such it is likely to result in a high initial risk.

In addition to possibly being able to reduce the vulnerability because the membership card is not permanently carried, the RFID operator should consider some of the counter measures. The nature of the specific RFID air interface protocol being used (ISO/IEC 18000-3 M1 with no proprietary features), there are few technology countermeasures that can be applied. However countermeasure *C-35 Physically shield the tag* results in at least a risk reduction of 1 level or possibly more depending on how the system is designed.

At the application layer, the following countermeasures can be applied:

— C-44 Restricting access to stored personal data;

— C-45 Firewalls;

— C-46 Intrusion detection.

These can reduce the risk level by at least 1.

K.10 Overall risk

Assume that the membership card is not permanently carried as discussed in K.8, thus adjusting the risk level by –1 to 5 for the RFID layers.

Next assume that the RFID operator provides members with a means to apply the countermeasure *C-35 Physically shield the tag* as discussed in K.9. This could be a shielded card case, thus adjusting the risk level by another –1 to 4 for the RFID layers.

The highest risk levels are now associated with the application layer, and this is an area where all operators, irrespective of size, should consider the data protection issues and countermeasures.

Annex L
(informative)

RFID Privacy Impact Assessment summary

PIA report date	— Date of last change made to PIA Report
RFID application operator	— Legal entity name and location — Person or office responsible for PIA timeliness — Point(s) of contact and inquiry method to reach the operator — Reference to a source if the PIA is based on a template
RFID application overview	— Purpose(s) of RFID application(s), including the functions to which RFID captured data is applied that impact the individual customer, user or citizen — Geographical scope of the RFID application — Types of users/individuals impacted by the RFID application
Data on the RFID tag	— List of encoded data elements
RFID Privacy Impact Assessment score	— In the range of 0 to 8, where 0 is no risk
RFID countermeasures	— List of countermeasures applied by the RFID operator — List of countermeasures that the individual should apply to the tags associated with the application

Bibliography

[1] CEN/TR 16673, *Information technology — RFID privacy impact assessment analysis for specific sectors*

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

[3] CEN CWA 16113, *Personal Data Protection Good Practices*; Available at: ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA16113.pdf

[4] ISO 11784, *Radio frequency identification of animals — Code structure*

[5] ISO 11785, *Radio frequency identification of animals — Technical concept*

[6] ISO 14223 (all parts), *Radiofrequency identification of animals — Advanced transponders*

[7] ISO 18046-3, *Information technology — Radio frequency identification device performance test methods — Part 3: Test methods for tag performance*

[8] ISO/IEC 14443, *Identification cards — Contactless integrated circuit cards — Proximity cards*

[9] ISO/IEC 15693 (all parts), *Identification cards — Contactless integrated circuit cards — Vicinity cards*

[10] ISO/IEC 18000-2, *Information technology — Radio frequency identification for item management — Part 2: Parameters for air interface communications below 135 kHz*

[11] ISO/IEC 18000-3, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

[12] ISO/IEC 18000-4, *Information technology — Radio frequency identification for item management — Part 4: Parameters for air interface communications at 2,45 GHz*

[13] ISO/IEC 18000-6:2004 [3] , *Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz*

[14] ISO/IEC 18000-7, *Information technology — Radio frequency identification for item management — Part 7: Parameters for active air interface communications at 433 MHz*

[15] ISO/IEC 18000-61, *Information technology — Radio frequency identification for item management — Part 61: Parameters for air interface communications at 860 MHz to 960 MHz Type A*

[16] ISO/IEC 18000-62, *Information technology — Radio frequency identification for item management — Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B*

[17] ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

[18] ISO/IEC 18000-64, *Information technology — Radio frequency identification for item management — Part 64: Parameters for air interface communications at 860 MHz to 960 MHz Type D*

3) ISO/IEC 18000-6:2004 is impacted by the stand-alone amendment ISO/IEC 18000-6:2004/Amd 1:2006.

[19] ISO/IEC 18092, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)*

[20] ISO/IEC 21481, *Information technology — Telecommunications and information exchange between systems — Near Field Communication Interface and Protocol -2 (NFCIP-2)*

[21] ISO/IEC 270xx (all parts), *Information technology — Security techniques*

[22] ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

[23] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

[24] ETSI/TR 187 020 V1.1.1 (2011-05), *Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436*

[25] JIS X6319–4, *Specification of implementation for integrated circuit(s) cards — Part 4: High speed proximity cards*

[26] Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification *(notified under document number C(*2009) *3200)* (2009/387/EC)[4)]

[27] MIROWSKI L., HARTNETT J., WILLIAMS R. (2009). An RFID Attacker Behavior Taxonomy, *Pervasive Computing*, October – December 2009, pp 79 - 84

[28] MITROKOTSA A., BEYE M., PERIS-LOPEZ P. (2010). Classification of RFID Threats based on Security Principles. Security Lab, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology (TU Delft). Accessed 9 August 2012: http://www.academia.edu/2197073/Classification_of_RFID_Threats_based_on_Security_Principles

[29] XIAO Q., GIBBONS T., LEBRUN H. (2008). RFID Technology, Security Vulnerabilities, and Countermeasures, *Supply Chain, The Way to Flat Organisation*, pp 357 – 382, In Tech, ISBN 978-953-7619-35-0, Vienna, Austria

[30] 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

4) Official Journal of the European Union, 16.5.2009 L122/47 to L122/51.

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.™