

BS EN 16571:2014



BSI Standards Publication

Information technology — RFID privacy impact assessment process

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

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.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

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

© 2014 CEN All rights of exploitation in any form and by any means reserved
worldwide for CEN national Members.

Ref. No. EN 16571:2014 E

Contents

Page

Foreword.....	5
Introduction	6
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Symbols and abbreviations	11
5 Structure of this European Standard	12
6 Field of reference for this European Standard	12
6.1 'RFID' as defined by the EU RFID Recommendation	12
6.2 'RFID application' as defined by the EU RFID Recommendation	13
6.3 'RFID operator' as defined by the EU RFID Recommendation	13
6.4 Relationship between the RFID PIA and data protection and security	14
6.5 Relevant inputs for the PIA process	17
6.5.1 General.....	17
6.5.2 The privacy capability statement	17
6.5.3 The Registration Authority	17
6.5.4 RFID PIA templates	17
7 RFID operator's organizational objectives of the RFID PIA	17
7.1 Overview	17
7.2 Meeting and exceeding legal requirements	18
7.3 When to undertake the RFID PIA.....	19
7.3.1 General.....	19
7.3.2 Undertaking a PIA at the design stage before the RFID system becomes operational	19
7.3.3 Undertaking a PIA at a review and update the design-based PIA	19
7.3.4 Undertaking a PIA to contribute to the development of a template	19
7.3.5 Undertaking a PIA with an established template.....	20
7.3.6 Undertaking a PIA at the introduction of a new function within the RFID application	20
7.3.7 Undertaking a PIA based on changes in RFID technology	20
7.3.8 Undertaking a PIA when a privacy breach has been reported.....	20
8 Tools to simplify the process	21
8.1 RFID operator responsibility	21
8.2 RFID technology privacy capability tools - overview.....	21
8.3 Registration of RFID privacy capability statements by RFID product manufacturers	21
8.3.1 General.....	21
8.3.2 Obligations of the Registration Authority	21
8.3.3 Appointment.....	22
8.3.4 Resignation	22
8.3.5 Responsibilities of the RFID product manufacturers	22
8.4 RFID technology privacy capability tools - details.....	23
8.4.1 RFID integrated circuit privacy capabilities	23
8.4.2 RFID tag privacy capabilities	23
8.4.3 RFID interrogator privacy capabilities.....	23
8.4.4 The default privacy capability statement	23
8.4.5 Using CEN/TR 16672 to construct privacy capabilities for products using proprietary protocols.....	24
8.5 Templates	24
8.5.1 General.....	24

8.5.2	Developing a template	24
8.5.3	Who should prepare the templates?	25
8.5.4	The role of stakeholders in template development	25
9	RFID PIA - a process approach	26
9.1	Introduction	26
9.2	Process Steps	26
9.3	Achieving the correct level of detail	27
9.3.1	General	27
9.3.2	Level 0 – no PIA	27
9.3.3	Level 1 – small scale PIA	27
9.3.4	Level 2 – PIA focussed on the controlled domain of the application	27
9.3.5	Level 3 – Full scale (complete) PIA of the application	28
9.3.6	Reducing the effort for the SME organization	28
9.4	Process methodology	29
10	Preparing the RFID functional statement	30
11	Preparing the description of the RFID applications	31
11.1	Introduction	31
11.2	Multiple applications	31
11.3	RFID application overview	32
11.3.1	General	32
11.3.2	Determine which RFID technology is intended or being used	32
11.3.3	Determine the RFID components used in the application	33
11.3.4	RFID applications on portable devices	34
11.4	Data on the RFID tag	36
11.4.1	General	36
11.4.2	Determine what inherent identifiable features are possessed by the RFID tag	36
11.4.3	Listing the data elements encoded on the RFID tag	37
11.4.4	Determine whether encoded data can be considered identifiable	37
11.4.5	Determine whether personal data is encoded on the tag	38
11.5	Additional data on the application	38
11.6	RFID data processing	38
11.7	Internal transfer of RFID data	39
11.8	External transfer of RFID data	39
11.9	RFID application description sign off	39
12	Risk Assessment	40
12.1	Procedural requirements derived from the RFID Recommendation	40
12.1.1	Common procedure requirements for all RFID operators	40
12.1.2	Requirements for retailers that are RFID operators	41
12.1.3	Procedure requirements for manufacturers of products eventually sold to consumers	42
12.2	Asset identification and valuation	42
12.2.1	General	42
12.2.2	Identification of assets	43
12.2.3	Valuing assets	44
12.3	Threat identification and evaluation	47
12.3.1	General	47
12.3.2	Identification and classification of threats	48
12.3.3	Evaluating threats	49
12.3.4	The process for the SME organization	50
12.4	Identifying vulnerabilities and enumerating the associated risk levels	50
12.4.1	Basic procedure	50
12.4.2	Procedure to account for exposure time	51
12.5	Initial risk level	51
12.6	Countermeasures	53
12.6.1	General	53
12.6.2	Identifying countermeasures	53

12.6.3	Reassessing risk levels	55
12.7	Residual risks.....	55
12.8	RFID PIA endorsement.....	56
13	Worked example of the risk assessment process	56
14	The PIA summary report	56
14.1	PIA report date	56
14.2	RFID application operator	56
14.3	RFID application overview	56
14.4	Data on the RFID tag	56
14.5	RFID Privacy Impact Assessment score	57
14.6	RFID countermeasures	57
15	Revision control.....	57
16	Monitoring and incident response	58
Annex A	(normative) Details of Registration Authority.....	59
Annex B	(informative) RFID manufacturer's product privacy capability statements	60
B.1	RFID integrated circuit (chip) privacy features.....	60
B.2	RFID interrogator privacy features	62
Annex C	(informative) RFID Privacy Impact Assessment flowchart.....	65
Annex D	(informative) Template development	67
Annex E	(informative) Flowchart to determine the RFID PIA level.....	68
Annex F	(informative) RFID functional statement.....	69
Annex G	(normative) RFID application description	70
Annex H	(informative) Identification and valuation of personal privacy assets	71
H.1	Individually held personal privacy asset.....	71
H.2	Assets that apply to the organization.....	76
Annex I	(informative) RFID threats	77
I.1	Threats associated with the data encoded on the RFID tag and the RFID tag (or RF card) itself.....	77
I.2	Threats associated with the air interface or the device interface communication	80
I.3	Threats associated with the interrogator (or reader)	85
I.4	Threats associated with the host application.....	85
Annex J	(informative) Countermeasures	88
J.1	List of countermeasures	88
J.2	Threat and countermeasure mappings	90
Annex K	(informative) PIA risk assessment example.....	94
K.1	Introduction	94
K.2	Ranking the assets	94
K.3	Considering threats at the tag layer and air interface layer	95
K.4	Considering threats at the interrogator layer	96
K.5	Considering threats at the device interface layer	97
K.6	Considering threats at the application layer.....	97
K.7	Considering vulnerabilities.....	98
K.8	Risk scores after considering all the threats and vulnerabilities	98
K.9	Applying countermeasures	99
K.10	Overall risk	99
Annex L	(informative) RFID Privacy Impact Assessment summary	101
Bibliography		102

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, 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.

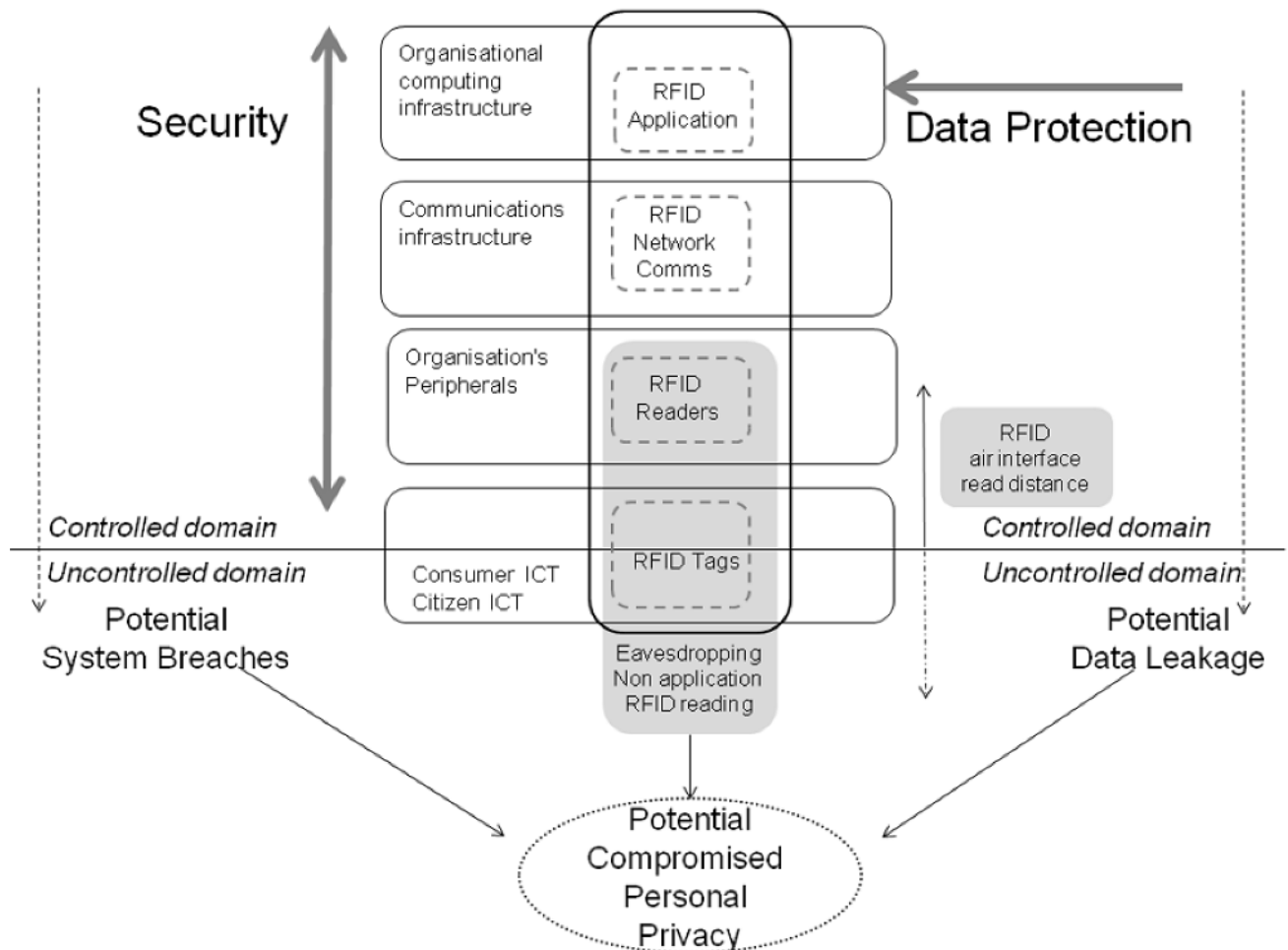


Figure 1 — Interrelation between RFID privacy, security, and data protection functions

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:

- 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.
- 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.
- 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 of 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: