PD CEN/TR 16684:2014

BSI Standards Publication

Information technology — Notification of RFID — Additional information to be provided by operators

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 16684:2014.

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

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

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

Published by BSI Standards Limited 2014

ISBN 978 0 580 84084 5
ICS 35.240.60

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

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

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16684

June 2014

ICS 35.240.60

English Version

Information technology - Notification of RFID - Additional information to be provided by operators

Technologies de l'information - Notification d'identification par radiofréquence (RFID) - Informations complémentaires à fournir par les opérateurs

Informationstechnik - Notifizierung von RFID: Zusätzliche vom Betreiber zur Verfügung zu stellende Information

This Technical Report was approved by CEN on 8 March 2014. It has been drawn up by the Technical Committee CEN/TC 225.

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

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

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

Contents

Page

Foreword

This document (CEN/TR 16684:2014) has been prepared by Technical Committee CEN/TC 225 “AIDC technologies”, the secretariat of which is held by NEN.

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

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

The other deliverables are:

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

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

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

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

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

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

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

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

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

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

0 Introduction

0.1 General

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 document will provide the additional information of the RFID application that will need to be provided to a citizen by accessing the source identified on the sign where the RFID application is operating. This information will be aligned with the details set out in the Recommendation, but some of this might not be available at the outset, a TR is the preferred form of initial delivery to establish basic requirements.

0.2 Overview

On March 15th 2007, the European Commission presented to the European Parliament a communication about the steps towards a Policy Framework for Radio Frequency Identification in Europe. Here below is an extract:

"COMMISSION RECOMMENDATION of 2009/05/12 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification {SEC (2009) 585}{SEC (2009) 586}.

Radio frequency identification (RFID) is a technology that allows automatic identification and data capture by using radio frequencies. The salient features of this technology are that they permit the attachment of a unique identifier and other information – using a microchip – to any object, animal or even a person, and to read this information through a wireless device. RFID is not just "electronic tags" or "electronic barcodes". When linked to databases and communications networks, such as the Internet, this technology provides a very powerful way of delivering new services and applications, in potentially any environment.

RFID technology is indeed seen as the gateway to a new phase of development of the Information Society, often referred to as the "internet of things" in which the internet does not only link computers and communications terminals, but potentially any of our daily surrounding objects – be they clothes, consumer goods, etc. It is this prospect that provoked the European Council of December 2006 to ask the European Commission to review the challenges of the next generation of Internet and networks at the 2008 Spring Council.

RFID is of policy concern because of its potential to become a new motor of growth and jobs, and thus a powerful contributor to the Lisbon Strategy, if the barriers to innovation can be overcome. The production price of RFID tags is now approaching a level that permits wide commercial and public sector deployment. With wider use, it becomes essential that the implementation of RFID takes place under a legal framework that affords citizens effective safeguards for fundamental values, health, data protection and privacy.

It is for these reasons that the Commission carried out a public consultation on RFID in 2006, which highlighted the expectations of the technology based on the results of early adopters but also the concerns of citizens about RFID applications that involve identification and/or tracking of persons.

Data protection, privacy and security

In the public debate on RFID, there are serious concerns that this pervasive and enabling technology might endanger privacy: RFID technology may be used to collect information that is directly or indirectly linked to an identifiable or identified person and is therefore deemed to be personal data; RFID tags may store personal data such as on passports or medical records; RFID technology could be used to track/trace people's movements or to profile people's behaviour (e.g., in public places or at the workplace). Indeed, the Commission's public consultation underlined the concern of citizens about the potential of RFID to be an intrusive technology. Adequate privacy safeguards are called for as a condition for wide public acceptance of RFID. Respondents to the online consultation expect these safeguards to emerge from privacy enhancing technologies (70%) and awareness raising (67%); specific legislation on RFID was seen as the best solution by 55%. In addition, views are evenly balanced on whether societal applications are really positive, with about 40% of responses on each side. Stakeholders have raised concerns about potential infringements of fundamental values, privacy and greater surveillance, especially in the workplace resulting in discrimination, exclusion victimisation and possible job loss.

It is clear that the application of RFID must be socially and politically acceptable, ethically admissible and legally allowable. RFID will only be able to deliver its numerous economic and societal benefits if effective guarantees are in place on data protection, privacy and the associated ethical dimensions that lie at the heart of the debate on the public acceptance of RFID.

The protection of personal data is an important principle in the EU. Article 6 of the Treaty on the European Union states that the Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms; Article 30 requires appropriate provisions on the protection of personal data for the collection, storage, processing, analysis and exchange of information in the field of police co-operation. The protection of personal data is set as one of the freedoms in Article 8 of the Charter of Fundamental Rights.

The Community legislation framework on data protection and privacy in Europe was designed to be robust in the face of innovation. The protection of personal data is covered by the general Data Protection Directive regardless of the means and procedures used for data processing. The Directive is applicable to all technologies, including RFID. It defines the principles of data protection and requires that a data controller implements these principles and ensure the security of the processing of personal data. The general Data Protection Directive is complemented by the ePrivacy Directive which applies these principles to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. Due to this limitation, many RFID applications fall only under the general Data Protection Directive and are not directly covered by the ePrivacy Directive.

Pursuant to these Directives, public authorities in Member States are charged with the monitoring whether the provisions adopted by Member States are correctly applied. They will have to ensure that the introduction of RFID applications complies with privacy and data protection legislation. It may therefore be necessary to provide detailed guidance on practical implementation of new technologies, such as RFID. For these purposes both directives foresee the drawing up of specific codes of conduct. This process implies a review of these codes at national level by the competent data protection authority, and a review at European level through the "Article 29 Working Party". "

One of the action items contained in the communication was the creation of a Stakeholders Group with the task to provide an open platform allowing a dialogue between consumers associations, market actors and National and European authorities in order to support the European Commission in its effort to promote awareness campaigns at Member state and citizen level about the opportunities and challenges of RFID. The outcome of the work performed by this Group was the publication of a PIA Framework that was endorsed by Article 29 Working Party on February 11th 2010.

In parallel, on May 12th 2009, the European Commission published a Recommendation on the implementation of Privacy and Data protection principles supported by Radio frequency Identification (RFID) . This document provides:

— guidance to Member States on the design and operation of RFID applications in a lawful, ethical and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data,

— guidance on measures to be taken for the deployment of RFID applications to ensure that national legislation implementing Directives 95/46/EC, 99/5/EC and 2002/58/EC is, where applicable, respected when such applications are deployed, and

— defines the scope of this Technical Report (see Clause 1).

The RFID Recommendation underlines the risks linked with the RFID technology and the obligations of the RFID operators to deal with the associated risks in its introduction through the bullet points (4), (5), (6), (8) and (13):

"*(4) RFID technology enables the processing of data, including personal data, over short distances without physical contact or visible interaction between the reader or writer and the tag, such that this interaction can happen without the individual concerned being aware of it.*

(5) *RFID applications hold the potential to process data relating to an identified or identifiable natural person, a natural person being identified directly or indirectly. They can process personal data stored on the tag such as a person's name, birth date or address or biometric data or data connecting a specific RFID item number to personal data stored elsewhere in the system. Furthermore, the potential exists for this technology to be used to monitor individuals through their possession of one or more items that contain an RFID item number.*

(6) Because of its potential to be both ubiquitous and practically invisible, particular attention to privacy and data protection issues is required in the deployment of RFID. Consequently, privacy and information security features should be built into RFID applications before their widespread use (principle of 'security and privacy by design').

(8) Member States and stakeholders should, especially in this initial phase of RFID implementation, make further efforts to ensure that RFID applications are monitored and the rights and freedoms of individuals are respected.

(13) RFID application operators should take all reasonable steps to ensure that data does not relate to an identified or identifiable natural person through any means likely to be used by either the RFID application operator or any other person, unless such data is processed in compliance with the applicable principles and legal rules on data protection."

It also gives clear instruction linked with Public awareness of RFID applications in paragraph 8:

"*Member States should ensure that operators take steps to inform individuals of the presence of readers on the basis of a common European sign, developed by European Standardisation Organisations, with the support of concerned stakeholders. The sign should include the identity of the operator and a point of contact for individuals to obtain the information policy for the application.*"

On December 8th 2008 the European Commission Enterprise & industry Directorate-General issued a Standardization Mandate to the European Standardization Organizations CEN/CENELEC and ETSI applied to RFID, which was divided in two phases.

— Phase 1 consisting in a gap analysis in terms of standardization started in 2009 and ended on 31st May 2011. The deliverable was the ETSI/TR 187020.

— This deliverable has been accepted by the European Commission (Directorate General Information and Society, and Directorate General Enterprises) in 2011, and Phase 2 was initiated on January 2nd 2012 with the signature of a contract with CEN Technical Committee 225 to develop a Standardization programme as set for in the ETSI/TR 187020.

1 Scope

This Technical Report is to assist operators of applications in areas where radio frequency interrogators are deployed, to identify the types of information that are called for in the recommendation.

The Technical Report provides all the current information to assist operators to develop and publish a concise accurate and easy to understand information policy for each of their applications.

The policy should at least include:

- the identity and address of the operators;
- the purpose of the application;
- 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;
- a summary of the privacy and data protection impact assessment;
- 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.

2 Terms and definitions

For the purposes of this document the terms and definitions given in CEN/TS 16685:2014 apply.

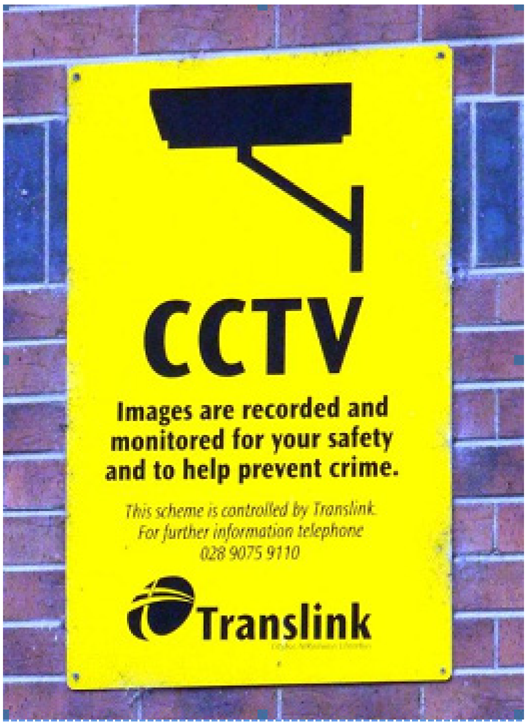
3 CCTV as an Exemplar

This Technical Report points to the practicality of using the well established, and publicly accepted, practice of signage in Europe relating to the use of CCTV cameras in both public and private (but accessible to the public) spaces to capture still and moving images for protection of public safety and private property as a model for RFID notification signage

Although not standardized, CCTV signs are already in widespread use in public places across Europe, relating to the use of cameras in both public and private (but accessible to the public) spaces to capture still and moving images for protection of public safety and private property.

Typical locations are airports, train and bus stations and retail shops. This signage displays three elements: an emblem, the purpose of the application, and an address where to get additional information. This signage appears to be acceptable to the general public and to the operators, and its full logo/text implementation also appears to satisfy the concerns of the privacy lobby.

Some examples of CCTV signage of UK/Ireland are shown below:


CCTV
Images are recorded and monitored for your safety and to help prevent crime.
This scheme is controlled by Translink.
For further information telephone
028 9075 9110
Translink

NOTE

1) CCTV logo with text reinforcement ‘CCTV’;

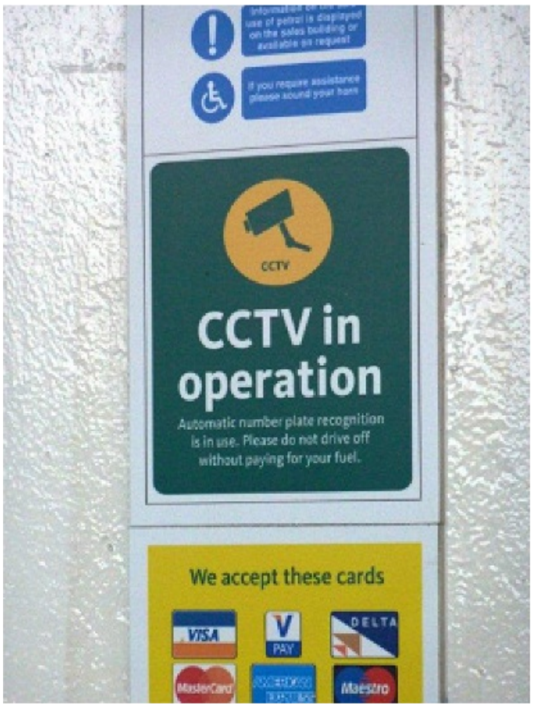
2) Statement of system intent;

3) Operator of system;

4) Contact details;

5) Operator logo separate from CCTV logo.

Figure 1 — CCTV logo, Bus Station Northern Ireland


use of petrol is displayed
on the sales building or
available on request
If you require assistance
please sound your horn
CCTV
CCTV in operation
Automatic number plate recognition is in use. Please do not drive off without paying for your fuel.
We accept these cards
VISA
V PAY
DELTA
MasterCard
Maestro

NOTE

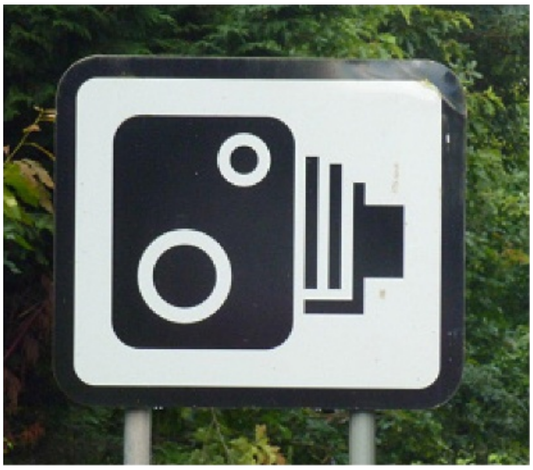
1) CCTV logo with text reinforcement ‘CCTV in operation’;

2) Statement of system intent (automatic number palate recognition) and warning;

3) Operator of system NOT indicated: where this is indicated, often it says contact station manager, reflecting that many filling stations are franchised. So signage maybe standard Texaco format, but station is run by Malthurst;

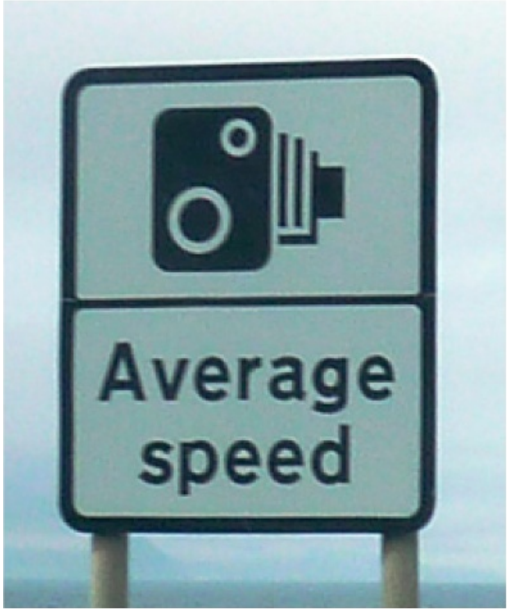
4) Signage in stack with disability assistance, handling information and credit card information.

Figure 2 — CCTV logo, Filling Station in Scotland



NOTE A commonly seen warning sign, which is on a white background, is the Speed Safety Camera sign used in the UK and Eire and some other European countries.

Figure 3 — Speed Safety Camera signs



NOTE Speed camera logo: seen in Scotland. No operator declared. 1930's design of camera.

Figure 4 — Speed Safety Camera signs

4 The RFID European Emblem

4.1 General

The concept of the easily recognizable Emblem used by the CCTC signage is applied for the selection of a RFID emblem, and it can be seen that the emblem can be highly stylised yet be instantly recognizable, especially if a text 'prompt' such as RFID is included in the emblem.

Such an emblem has already been developed and standardized as ISO/IEC 29160:2012. This standard has been published on May 30th 2012.

The ISO/IEC 29160 Standard has been adopted as a European Standard and will be published as EN 16656:2014 with specific informative content to this signage requirement within Europe. In particular it provides clarification regarding the minimum size of the emblem in relation to legibility as opposed to physical size.

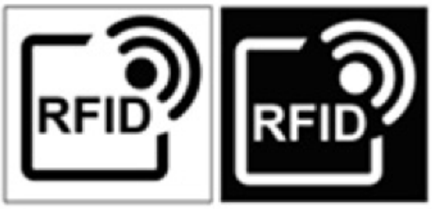


Figure 5 — RFID Emblem

It is therefore recommended that the generic version be adopted as the **Common European RFID Notification Emblem** as it combines the simple strong graphic with the reinforcing text "RFID" which will greatly assist in educating the citizen during the rollout period.

4.2 Guidelines on the use of the Common European RFID emblem

Bullet point 24 on page 4, clauses 15 and 16 of the Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification of May 12th 2009, calls for raising awareness among the public and the enterprises about the features and capabilities of RFID, and for the mitigation of the associated risks for Privacy, so that it will enhance its acceptability. The implementation of a signage policy is one of the mitigating solutions to raise awareness.

In line with the above, the European Commission’s Directorate General “Information Society and Media” has published on January 15th 2012, a document called “Guidelines on the Use of the Common European RFID Sign” prepared under the RFID in Europe project funded by the ICT Policy Support Programme (ICTPSP-CIP) and, that gives guidelines to RFID operators for the use of a common European Sign. This document has received the endorsement of Unit "ICT for Competitiveness and Industrial Innovation" of the European Commission's Directorate General "Enterprise and Industry".

Unlikely the logo´s that serve the purpose of communicating a trademark of a proprietary system or a business application, the **Common European RFID emblem** shall be utilized as a **generic emblem to indicate** the **presence of an RFID application** for the notification of citizens about the RFID technology utilization either in public areas such as shops, public transport locations or libraries or directly embedded in products. The Common European RFID emblem will also provide more visibility to the signage system which enables the citizens to access additional information about the data capture application and the operator.

4.3 Definition of the Common European RFID Notification Sign

This definition should be read in the context of the completion of a Privacy Impact Assessment (PIA) of the RFID application and conforming to EN 16571:2014.

The Common European RFID Notification Sign consists of three elements:

a) a graphic emblem derived from the generic emblem defined in EN 16656:2014;

b) a textual description of the purpose of the RFID application being notified, together with the legal name of the RFID application operator and their telephone number (normally that of the designated Data Controller;

c) a textual definition of the contact point from which further information may be obtained about the application, including *inter alia* the information policy of the operator. The contact point may be defined by any of the following methods: mail address, e-mail address, telephone number, webpage URL.

The RFID Emblem facilitates recognition of the Notification Sign and recall of previously acquired knowledge about the ‘message’ the Sign is intended to transmit. For this reason, the Emblem shall be present on all Notification signs, and shall conform to the design in Appendix NN. The emblem should normally be placed above or to the left of the other elements.

It is recognized that the signage system will be applied in a very wide range of circumstances, and with potential constraints in terms of available space, printing technique, etc. The signage system is generally non-prescriptive in relation to design, font, colour, etc., in order that the signage can be printed with minimum changes in process.

The Notification Sign shall be regarded as belonging to the general set of Trade Regulation signs such as weights and measures, CE marks etc. The sign shall therefore conform to the norms of visibility, legibility and accessibility as applied in the relevant Member States.

The Notification Sign shall not be regarded as a hazard sign, and the sign shall not utilise shapes/outlines and/or colours that might imply danger.

It is recognized that the operator, especially in the case of small enterprises, buying groups, franchises, etc may delegate the contact point task to third parties such as call centres. However, this does not reduce the legal responsibilities of the operator in terms of compliance with Data Protection and Privacy regulations.

4.4 Placement of signs

4.4.1 General

The RFID Recommendation defines two situations where signage is required.

4.4.2 Presence of Readers

Clause 8 of the Recommendation notes that *"Member States should ensure that operators take steps to inform individuals of the presence of readers on the basis of a common European sign, developed by European Standardisation Organisations, with the support of concerned stakeholders. The sign should include the identity of the operator and a point of contact for individuals to obtain the information policy for the application."*

4.4.3 Placement of signs notifying the presence of readers

4.4.3.1 General

Notification signs shall be placed at the entrance to all areas where fixed RFID readers are installed or mobile RFID readers deployed.

The sign notifies the citizen that RFID readers may be operating within the signed area.

It does not purport to define the boundaries of the area where tags might be read, nor does it indicate the likelihood of reading of any tagged item carried by the citizen.

NOTE The energy field emitted by a reader, especially the common UHF propagating type, may vary in strength and shape over time due to changes in temperature and humidity, and also due to changes in the physical background which may absorb or reflect the signal. Even with constant reader field strengths, the range at which a tag may be read may vary considerably depending on tag antenna size, orientation, the electrical characteristics of the item to which the tag is attached, and whether the tag is fully passive, battery assisted or fully active

4.4.3.2 Multiple Applications

Where the sign relates to multiple applications by a single operator, the purpose of these applications may be listed on a single sign. It is recommended that the description of the purpose is kept general to reduce the need to place new signs if the purpose is modified.

4.4.3.3 Multiple Operators

Where multiple operators implement RFID applications in the same area, e.g. public transport interchanges, shopping malls, then each operator shall provide a separate sign.

4.4.4 Presence of tags

4.4.4.1 General

Clause 9 of the RFID Recommendation notes that *"On the basis of a common European sign, developed by European Standardisation Organisations, with the support of concerned stakeholders, operators should inform individuals of the presence of tags that are placed on or embedded in products."*

NOTE The “concerned stakeholders” include Government organizations, RFID application developers, RFID technology providers, Industry Associations, Standards Bodies and other operators.

In this case, the operator is defined as the legal entity that caused the tag to be placed on, or be embedded in, the product. That entity is the only entity that can be certain that a tag has been attached to a product.

4.4.4.2 Use of Emblem on tagged items

Notification shall be performed by the application of the Common RFID Emblem to the tagged product. The size of the emblem may be determined by the operator, but shall be legible as defined by trade regulation. *The e-mark for weights and measures provides a useful comparison.*

Placement of the emblem on the tagged item is at the discretion of the operator. Placement close to the tag is encouraged, especially if the tag is embedded, to improve ease of tag reading.

The colour and intensity of ink used to print the emblem is at the discretion of the operator, always subject to legibility as determined by trade regulation.

4.4.4.3 Purpose of application declaration on tagged items

In many cases, especially for fast moving consumer goods, the tagged item may become part of several applications as it moves along the supply chain.

An operator may have limited or no knowledge of these additional applications, and therefore it is not practical to require a purpose of application on such items.

In the case of consumer durables, a tag embedded for warranty, maintenance and end-of-life disposal management may be read in the premises of the citizen by a mobile reader operated by a serviceperson. In these cases, where space permits, a sign showing the purpose of the embedded tag should be placed on the item.

For contactless cards in the financial, library and public transport sectors, the purpose of the tag should be declared to the user when the card is issued. As the card will normally only be used by the person to which it was issued, then there is limited benefit to be gained from placing a purpose of application statement on the card itself.

4.4.4.4 Contact Point

In general, tagged products in the retail, library, finance and public transport sectors already carry the legal name and contact point of the entity responsible for compliance with trade regulation.

This entity is typically also the entity that caused the product to carry a tag. Providing this is the case, then the existing contact point information may also be used for RFID information.

4.5 Who should place signage on tagged items

Where there is a need to tag a product, and the PIA mitigation process indicates that a notification sign becomes necessary, then it is recommended the following organizations take action whether they are operators or not:

- product manufacturers of retail goods which add RFID tags to their retail products; - Packaging suppliers which provide RFID tagged retail product packaging;
- logistics e.g. third-party logistics providers (3PLs) which add RFID tags to retail products or retail product packaging;
- European importers which import RFID tagged retail products, or RFID tagged retail product packaging, or apply RFID tags to retail products or their retail product packaging;
- all other organizations which add RFID tags to retail products or retail product packaging.

If a retail product has a tag attached or embedded then the common European sign should be displayed on the retail product. If the product is sold inside packaging, then this packaging shall also display the notification sign.

4.6 Size of emblem

The minimum size of the RFID emblem as defined in ISO/IEC 29160:2012, Clause 4.3 is 14 mm x 13 mm with a minimum 3 mm clear, unprinted area around the RFID Emblem. These dimensions could be difficult to incorporate into the small self-adhesive RFID labels commonly used by retailers, and ERRT have expressed concerns.

However, ISO/IEC 29160:2012 also notes in Clause 4.3 that if direct marking on small components/products, a smaller emblem may be used but in no case shall the emblem be smaller than 5 x 5 mm. When represented in a normal contrast form, it may be large enough to be easily recognizable under typical use conditions. Whilst printing on to small labels is not strictly direct marking in the technical sense, the sense of the wording is also applicable to labels where the available “real estate” on the label is constrained.

Clause 4.3 also introduces the issue of legibility. This Technical Report argues that the RFID Notification sign is part of a set of signs required in the EU for the regulation of commerce: there is an existing corpus of regulation which defines the meaning of legibility, both for normally sighted and impaired vision citizens.

This Technical Report, together with the signage TS/EN that will be developed from its conclusions, is subordinate to EC and Member State law. The Technical Report may propose a minimum of 5 x 5 mm based on technical considerations, but in real life deployment for the sign, this size may need to be increased to satisfy trade regulation.

5 Guidelines on additional information

5.1 General

The signage system described above notifies the citizen of the operation of RFID systems and provides a short summary of their purpose.

Additionally the signage system provides a pointer to where more information about the system, including its privacy and data protection aspects may be obtained.

This section provides guidelines on the additional information to be maintained by operators of RFID applications as part of their Information policy, and used to answer enquiries from citizens.

The additional information to be provided for a specific RFID application will be determined by means of the PIA process. In general it covers:

- the operator of the application;
- the purpose of the application;
- the data processed;
- a summary of the relevant Privacy Impact Assessment;
- the likely risks ;
- the mitigation techniques of such risks;
- a Privacy Information Provision Policy.

In each case it is necessary to first determine whether:

- there is only one application or more in operation in the area where RFID devices are deployed;
- there is one or more operators involved.

If there are more than one application and more than one operator in a given environment, the names and addresses of each operator, will have to be provided as well as each application.

5.2 Name of the operator of the application

5.2.1 Name

The name of the RFID operator is displayed in human readable text format using European language fonts 17. The name shall be the name of a legally recognized entity. A company identifier may supplement the RFID operator's name but cannot replace it. The company identifier shall be presented on the same row and follow the displayed name. No other information in any form should be present on the same row as the RFID application operator's name or RFID application operator's identifier. Only one RFID application operator's name and identifier are to appear on any example of the common European RFID sign. The company identifier shall appear on the same row as the RFID application operator's name (or part, if the name shall be split over two or more rows) to avoid that it be confused with the contact details.

The name of the RFID application operator and their organizational identifier shall be presented above and before the contact details.

5.2.2 Contact point

There are several possibilities to contact the operator such as:

- local telephone number (preferably toll free);
- website or direct URL;
- specific e-mail address;
- QR code readable by a mobile phone;
- postal address.

The contact point shall also give the name and position of the person in charge of the application.

5.3 Purpose of the application

The paragraph here below applies to each of the RFID application and to each of the operators involved in the RFID application. Each operator shall determine the mandatory elements as shown here below, while describing the purpose of the application. The information will answer the following questions (as a minimum):

- When the application shall be presented to the general public at any location where an RFID system, RFID devices or application are or may be operated, installed or present?
- Where the application is deployed?
- Which RFID technology is used?
- Which data is being collected?
- Why is data being collected?
- What will data be used for?

- How will the data be collected?

- How long will data be kept?

- Who will use the data? For instance, are the data going to be accessible for and used by any 3rd parties?

5.4 Data processed

As specified in the bullet point n°5 of the RFID Recommendation, RFID applications hold the potential to process data relating to an identified or identifiable natural person, a natural person being identified directly or indirectly. They can process personal data stored on the tag such as a person's name, birth date or address or biometric data or data connecting a specific RFID item number to personal data stored elsewhere in the system. Furthermore, the potential exists for this technology to be used to monitor individuals through their possession of one or more items that contain an RFID item number. The application might process data which are not considered as personal data or process specific personal data.

If the application processes personal data such as personal identity, the person is clearly identified. If the application does not process personal data but may give a link between the uniquely identified item and a person carrying the item, this person becomes identifiable. If the tagged item is monitored, then the individual carrying the tag will also be monitored.

In all cases the data processed shall be clearly indicated and accessible to an enquiry.

5.5 Summary of the privacy impact assessment

5.5.1 PIA report date

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

5.5.2 RFID application operator

There are four data elements:

- 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.

5.5.3 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) only needs to address those functions that involve the individual customer, user or citizen from a privacy data and information perspective. For example in a retail store stock receipt, stock checking, and shelf replenishment do not have to be covered. Similar processes in a library, and the use of returns sorters, do not need to be covered. However, the RFID operator may choose to elaborate such functions to illustrate the benefits of RFID;

- 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 controls and mitigations that can be exercised.

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

5.5.4 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" is completely understandable within the organization, but almost meaningless outside. A more general term like "serialised product code" is better for the summary.

5.6 Likely privacy risks

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

5.7 Measures to mitigate the risks

Two classes of controls and mitigations shall be reported:

a) List of controls applied by the RFID operator. This may include information as in the following examples:

   - The chip identifier on a library tag is not stored in the system;
   - The chip identifier on a travel card is not stored in the system;
   - The serialised product code is only used for price lookup and not associated with the customer after purchase;
   - The serialised product code is stored for a period of n months for product recall of pharmaceutical products;
   - The serialised product code for clothing is stored only for the return period, but the RFID has an implemented password to obscure reading by others;
   - Your passport uses a mechanism called mutual authentication, which means that only authorised readers can read the data from the tag;

b) List of controls that the individual should apply to the tags associated with the application as identified in customer or public information provided about the tagged item. This may include information as in the following examples:

   - Your membership card should be stored in a protective sleeve when not required for use;
   - 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;
   - 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;

- The RFID bag tag should be removed from the luggage handle on leaving the secure baggage area;
- The RFID tag on the {named class of product] can be deactivated at the special station;
- Your library membership card can only be activated with an additional PIN number, ensure that you keep this secure.

Table 1 — PIA Summary of the PIA Process

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 controls and mitigations	— List of controls applied by the RFID operator — List of controls that the individual should apply to the tags associated with the application

5.8 Privacy information policy for RFID

5.8.1 General

As good practice organizations should establish a Privacy Information Provision Policy to ensure that the privacy implications of the RFID identifiable goods being passed to consumers and the public are conveyed as necessary in a complete, reasonable and accurate manner.

An RFID Privacy Information Provision Policy should be available with the PIA summary and other RFID operator information though the access mechanism identified in 5.1.

5.8.2 Consumer and members of the public choice information – promotional material

In general terms the application operator may wish to advertise or promote the benefits of the RFID capabilities of an item and when so doing any residual risks or issues that should reasonably be conveyed to the public should be included too.

The PIA analysis and report should be the key source for making such decisions about what information is needed for consumers and the public. Some illustrations from other areas are:

- Illustration: Some products are advertised as “may contain nuts” to accommodate the nut allergy risk;
- The equivalent for RFID could be residual read and eavesdropping ranges on tagged items and a notification “remains readable over short distances” or “contains RFID” or use of the RFID symbol in promotional material;

NOTE Statements of “contactless” use implying radio may not be accurate enough as a non technicalmember of the public has no means of knowing or understanding which of several radio technologies is in use.

- Illustration: If mitigation measures need to be taken by individuals to bring risks down to acceptable levels then general statements that “mitigation may be required to maintain privacy” should be made in promotional material.

5.8.3 Consumer and members of the public choice information – sales material and pre-contract information

To enable reasonably supported choice by an individual when considering whether to purchase a good or agree to use an RFID enabled service (such as contactless payments and travel cards) then more detailed information than that provided in promotional material should be considered in the Privacy Information Provision Policy.

Areas to be explicitly considered should include :

- notification of any data use where opt out consent is not available;

- whether any privacy options affect charges for example if an opt out means that data sharing is not consented to, with perhaps the consequence that income for the organization is not then available and consequentially charges on opt out are higher.

The Privacy Impact Assessment may identify other factors relevant to informed choice for inclusion in the Privacy Information Provision Policy.

5.8.4 Consumer and members of the public choice information – means of conveying the information

The Privacy Information Provision Policy should consider the most appropriate and effective means of conveying information to consumers and the public before individuals choose to purchase goods or use services. A range of communication methods are available including:

- brochures;

- product information;

- organizational web sites;

- social networking services and Twitter;

- employees of the organization;

- videos and pictures.

The Privacy Information Provision Policy should ensure that information is easily available and not ‘hidden away’ in small print or buried in a lot of technical detail.

5.8.5 Consumer and members of the public privacy information accessibility

- The Privacy Information Provision Policy should ensure that the language used for conveying privacy information is stated clearly and understandable without specialist knowledge – for example technical or legal.

- The Privacy Information Provision Policy should ensure that the variations in information sensing capabilities of the population are taken into account.

Examples being use of appropriate text size, audio commentary on videos and braille. In exceptional circumstances possibly also factors such as audio indications for reader locations if those with poor sight need to know where readers are located.

5.8.6 Privacy related contractual and privacy policy information

Companies are developing good practice for the provision of information to consumers and the public on privacy matters. Annex A lists the contents of what is publicly available via the web from Facebook for their contract terms and conditions and their privacy policy.

The list of matters to be considered by most RFID application operators is likely to be considerably less than Facebook needs. Given that the standards being developed by CEN could apply until 2019 then some degree of looking ahead is appropriate where the technology and its applications can be expected to see considerable innovation with RFID use expanded greatly. Annex A is an informative annex that looks at Facebook for a view on the range of privacy contractual and policy matters that may come about for RFID applications in the future.

The Privacy Information Provision Policy should consider easy public access to relevant privacy contract terms and conditions and the contents of the organization’s privacy policy.

A minimum set of information provision considered by an RFID Privacy Information Provision Policy should be for contractual terms and conditions and an organization’s privacy policy:

- statement of rights and responsibilities;
- privacy and privacy protection;
- sharing your content and information;
- registration and account security;
- protecting other people's rights;
- mobile and other devices;
- payments;
- special provisions applicable to other application developers and other operators of applications;
- special provisions applicable to advertisers;
- termination;
- disputes.

NOTE Application developers and other application operators have been included as RFID spreads from closed application environments to, for example, mobile phones making use of RFID identifiable items.

5.8.7 Consumer and members of the public post sale user privacy information

Depending on the RFID application, the specific tags used for the application and any mitigation measures that require user action the PIPP should consider at least the following privacy information provision to individuals.

- Privacy options – where there are privacy options, then their descriptions with the privacy implications of those options.

- User operating instructions that impact privacy both to maintain privacy or where miss-operation would reduce privacy.

- Staff information, training and instructions necessary to maintain individuals' privacy.

- Supplementary information on significant residual risks if more detail is required than in the statement made statement in 5.6.

- Information provision to assist consumers in taking mitigation action if consumer purchased mitigation equipment should be proposed. The PIPP should consider information about where to obtain suitable quality equipment and likely costs.

- The Provision Information Provision Policy should consider what information provision should be made to consumers and members of the public if there is a loss or leak of data that would allow others to identify or target individuals through the possession of RFID identifiable items provided by the application operator.

- End of use by an individual: what privacy protecting instructions should be provided for waste disposal or recycling or secondary goods markets like car boot sales and eBay.

5.8.8 Consumer and members of the public information – means of conveying the post sale user privacy information

The Privacy Information Provision Policy should consider the most appropriate and effective means of conveying information to consumers and the public before individuals choose to purchase goods or use services. A range of communication methods are available including:

- user documentation;

- publicity and news channels;

- sales outlets;

- organizational web sites;

- social networking services;

- employees of the organization.

5.9 Consumer and public information – non application operator RFID privacy information

The Commission Recommendation dated 12 May 2009 in its recommendation 10 (page 8) identifies the role of retailers and others who may act as a route to consumers and the public for RFID identifiable items when they, as providers have no RFID capability themselves.

The RFID Privacy Impact Assessment EN process clarifies this and includes those who write data to a tag and others as application operators. The Privacy Information Provision Policy good practice identified in this section would apply to such operators who could reasonably expect the items being tagged to end up in the possession of consumers or members of the public. In these circumstances supporting information should be made available to the end providers of the goods sufficient for them to, in turn, provide reasonable information to consumers enabling informed choice.

The goods concerned should already have an RFID symbol on them. The minimum set of information that the application operator should consider in their Privacy Information Provision Policy for provision to no application operators is all the information within 5.1 to 5.9 that is from basic signage information in 5.1 through promotional material to post sale user operational and goods disposal information.

Annex A
(informative)

RFID applications in retail

Several examples of applications in the retail sector are presented below. Some operators may have more than one of these applications deployed at the same location.

Purpose 1	**Staff Administration**
Purpose Description	Appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to the staff of the data controller.
Data subjects are	Staff including volunteers, agents, temporary and casual workers Customers and clients Suppliers Members or supporters
Data classes are	Personal Details Family, Lifestyle and Social Circumstances Education and Training Details Employment Details Financial Details Racial or Ethnic Origin Religious or Other Beliefs Of A Similar Nature Trade Union Membership Physical or Mental Health or Condition Offences (Including Alleged Offences) Criminal Proceedings, Outcomes And Sentences.

Purpose 2	**Advertising, Marketing & Public Relations**
Purpose Description	Advertising or marketing the business of the data controller, activity, goods or services and promoting public relations in connection with that business or activity, or those goods or services.
Data subjects are	Staff including volunteers, agents, temporary and casual workers Customers and clients Suppliers Members or supporters
Data classes are	Personal Details Family, Lifestyle and Social Circumstances Education and Training Details Employment Details Financial Details Goods or Services Provided

Purpose 3	**Accounts & Records**
Purpose Description	Keeping accounts related to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity
Data subjects are	Staff including volunteers, agents, temporary and casual workers Customers and clients Suppliers Complainants, correspondents and enquirers
Data classes are	Personal Details Family, Lifestyle and Social Circumstances Education and Training Details Employment Details Financial Details Goods or Services Provided Racial or Ethnic Origin Trade Union Membership Physical or Mental Health or Condition Offences (Including Alleged Offences) Criminal Proceedings, Outcomes And Sentences.

Purpose 4	**Trading / Sharing in Personal Information**
Purpose Description	The sale, hire or exchange of personal information.
Data subjects are	Staff including volunteers, agents, temporary and casual workers Customers and clients Suppliers Complainants, correspondents and enquirers
Data classes are	Personal Details Family, Lifestyle and Social Circumstances Education and Training Details Employment Details Financial Details Goods or Services Provided

Purpose 5	**Crime Prevention and Prosecution of Offenders**
Purpose Description	Crime prevention and detection and the apprehension and prosecution of offenders.
Data subjects are	Staff including volunteers, agents, temporary and casual workers Customers and clients Suppliers Complainants, correspondents and enquirers
Data classes are	Personal Details Family, Lifestyle and Social Circumstances

Purpose 6	**Fundraising**
Purpose Description	Fundraising in support of the objectives of the data controller
Data subjects are	Staff including volunteers, agents, temporary and casual workers Customers and clients Suppliers Members or supporters
Data classes are	Personal Details Family, Lifestyle and Social Circumstances

Purpose 7	**Health Administration and Services**
Purpose Description	The provision and administration of patient care
Data subjects are	Members of the public, Customers and clients Suppliers
Data classes are	Dietary, other special health requirements prescription, Personal Details Family, Lifestyle and Social Circumstances Goods or Services Provided Racial or Ethnic Origin Physical or Mental Health or Condition

Purpose 8	**Property Management**
Purpose Description	The management and administration of land, property and residential property and the estate management of other organizations.
Data subjects are	Staff including volunteers, agents, temporary and casual workers Customers and clients Suppliers Complainants, correspondents and enquirers, Advisers, consultants and other professional experts
Data classes are	Personal Details Employment Details Financial Details Goods or Services Provided

Purpose 9	**Research**
Purpose Description	Research in any field, including market, health, lifestyle, scientific or technical research.
Data subjects are	Staff including volunteers, agents, temporary and casual workers Customers and clients Suppliers Relatives, guardians and associates of the data subject Advisers, consultants and other professional experts, Students and pupils
Data classes are	Personal Details Family, Lifestyle and Social Circumstances Employment Details Financial Details Goods or Services Provided Physical or Mental Health or Condition

Annex B
(informative)

RFID applications in library

Purpose 1	***Will be concluded after receiving information from national bodies***
Purpose Description	***Will be concluded after receiving information from national bodies***
Data subjects are	***Will be concluded after receiving information from national bodies***
Data classes are	***Will be concluded after receiving information from national bodies***

Most libraries implement RFID applications for the control of the circulation of borrowed items, i.e. checking out and checking in of returned books. However there are more RFID applications to be considered:

— Membership cards: These are absolutely essential for the loans and returns transactions. If they are based on bar code or magnetic stripe, then they are out of scope of M436 Phase 2. If they are based on the same RFID technology as is use for the loan items, then they are in scope, but the privacy implications are significantly different. If they are based on different RF technology (for example smart card using a different air interface protocol), then they are still within the scope of the application.

— Contactless smart cards. Most libraries charge fees for certain services and fines for a late return. Payment can be made in many ways, but some payments are made using the new contactless smart cards.

There are also some new developments in the air. Most public libraries are owned by local city or other government authorities. Cities are involved with collecting all sorts of money for all sorts of reasons: rents, local taxes, parking fines, and so on. The self-checkout kiosks in libraries are already fairly sophisticated devices, given that they can read bar code, read and write RFID tags (even support different protocols), take money and issue receipts and so forth. So the next great thing is to turn the self-check terminals into supporting multiple functions for the local government authorities. If the terminal can be used to pay for parking fines, that is a different and new application and in addition, if either a local authority ID card and/or a contactless payment card is used, it then comes within the scope of the Recommendation, bringing PIA obligations and signage policy.

There are also other RFID applications falling in scope of the Recommendation such as:

— Self check out using a Mobile phone with NFC technology

— Browsing information through Smart phones

— Smart shelves

— Library staff with RF ID badges

Annex C
(informative)

RFID applications in transportation

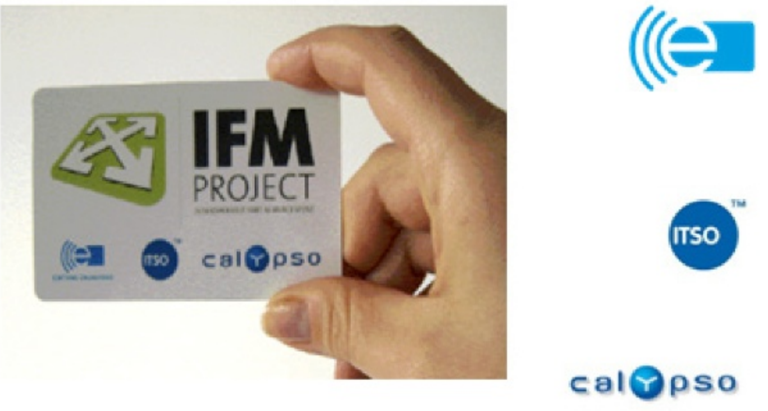
The main application of RFID technology in public transport with high level of user interaction is eTicketing, which started to take-off in late 90´s of the last century. The eTicketing utilizes different types of media such as the PICC (Proximity integrated circuit card) or NFC (Near field communication) enabled devices to store the ticket/contract and to establish communication with the PCD (proximity coupling device) or simply the reader, used for loading or validation of the contract between the user and the transport service operator or to provide access to the public transport services.

Purpose 1	**E-ticketing**
Purpose Description	The purpose of RFID use in e-Ticketing is to issue and control validity of different types of tickets/contracts (single, return, zonal, origin-destination, multi-journey, group or season ticket) or to enable direct payments for the provided tickets using a contactless chip card or NFC chip.
Data subjects are	Users of the public transport – i.e. the passengers.
Data classes are	Various eTicketing applications implemented throughout Europe may use following data related to the users: Personal facts related to Payment transactions: Age (or date of birth), First name & surname, Gender; Personal facts related to Transport transactions: Validations (in and/or out), date, place.

Purpose 2	**Public transport network optimization**
Purpose Description	Additional, but very important business related purpose of RFID based eTicketing for the transport service operators is the optimization of the public transport network through monitoring of capacity utilization or travel pattern analysis. The possibility of network optimization depends on the processes related use of eTicketing in the network.
Data subjects are	Users of the public transport – i.e. the passengers.
Data classes are	The data used for the purpose of public transport network optimization are available through the use of RFID based eTicketing in following modes: Be-in/Be-out, Check-in/Check-out, Walk-in/Walk-out. For the purpose of public transport network optimization, the personal data (if any) stored on the chip of the contactless chip cards or an NFC enabled devices are not relevant.

Utilization of logos in the public transport sector

Trading partners in the public transport sector can use different logos on the cards used for eTicketing to identify the card issuer, transportation system in which the card is valid or a logo indicating the interoperability of the transport application. There are no predefined rules for the placement of any of the mentioned types of logos on the card. Examples of the proprietary logos placed on different public transport eTicketing cards are provided as following:

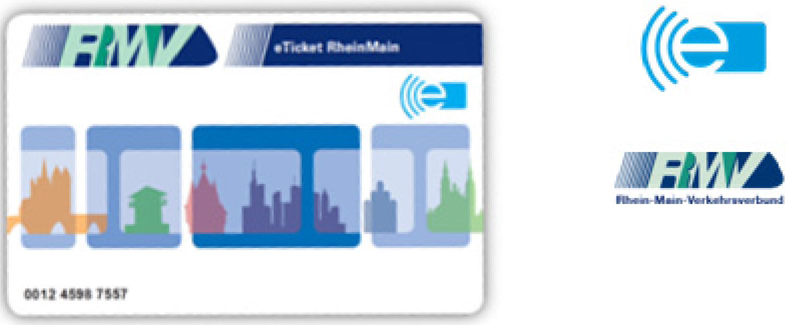


(((eTicket Deutschland logo indicating the interoperability of the transport application at public transport service providers utilizing the VDV Kernapplikation

ITSO logo indicating the interoperability of the smart card through compliance with the ITSO Specification in UK

CALYPSO logo indicating the interoperability of the smart card through compliance with the CALYPSO specification

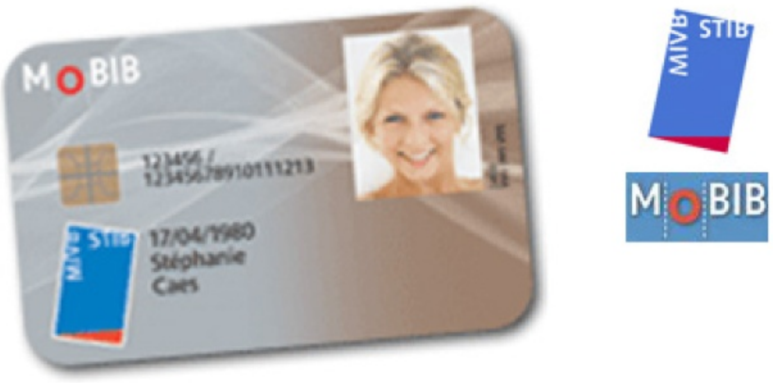
Figure C.1 — Card IFM Project



(((eTicket Deutschland logo indicating the interoperability of the transport application at public transport service providers utilizing the VDV Kernapplikation

Logo of Rhein-Main-Verkehrsverbund indicating the issuer of the card

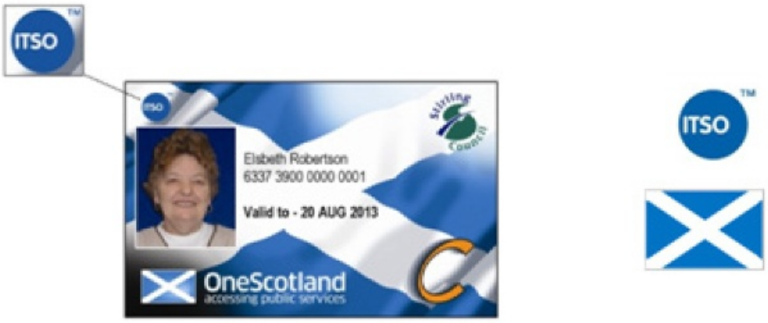
Figure C.2 — Card RMV



Logo of STIB - Société des Transports Intercommunaux de Bruxelles indicating the issuer of the card

Logo of a single transport pass in Brussels used to accommodate transport contracts

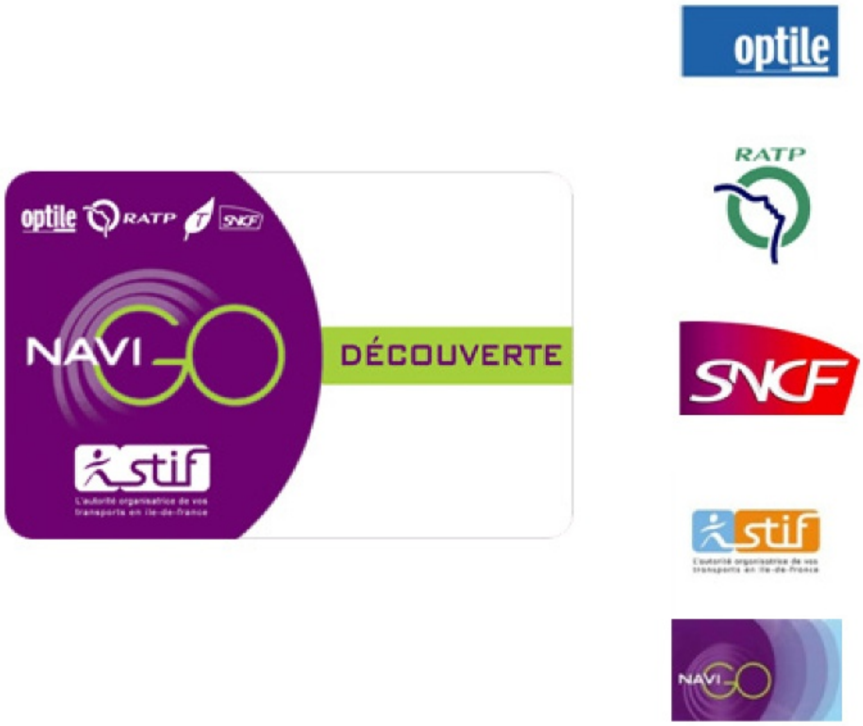
Figure C.3 — Card MOBIB



ITSO logo indicating the interoperability of the smart card through compliance with the ITSO Specification in UK

Logo of the card issuer – The Scottish Government

Figure C.4 — Card OneScotland



Logo of the Professional Transport Organization of Île-de-France (Paris and suburbs)

Logo of the Autonomous Operator of Parisian Transports

Logo of the French national railway corporation

Logo of the French public transport authority

Logo of the card scheme – Navigo

Figure C.5 — Card NaviGO

IFM project

Public transport sector in Europe has successfully demonstrated the possibilities of RFID eTicketing utilization for facilitation of public transport accessibility in the Interoperable fare management project. The IFM project is aiming to provide architecture of an ecosystem utilizing a shared contactless media (such as PICC) for interoperable eTicketing throughout Europe. In 2010, three European eTicketing associations demonstrated the use of a single PICC in three different ticketing systems.

Figure C.6 — Card IFM Project

[SOURCE: http://www.ifm-project.eu/]

In the deliverable D2.1 of the IFM Project a survey has been conducted which provides more insight into the business requirements of the public transport industry regarding the use of personal data for RFID eTicketing.

According to the survey, the objective for gathering customer personal data is to better answer the customer demands, to improve services and to improve direct marketing. A rather complete scope of personal data (first name and last name, postal address, email, telephone, gender, age, other social data) is requested when the ticket is purchased, validated, for inspection purpose and fraud control.

Personal data stored on the card, if any, are usually first name, last name, age, gender. Information is deposited on the card to fit various applications.

As transaction data are shared and exchanged, all kinds of system configuration are being used such as: central processing, distributed processing, provided to a third party.

When anonymization is done, hash code is usually changed once a month.

To fight technological fraud, control is concentrated on SAM and the central system and relies on cryptography. Hotlists are used to limit payment incidents.

Requested time for transaction data archiving is 2 years.

An IFM entity cannot disclose customer related information to third parties without specific authorization from the customer. There is an option consisting of setting up a trusted third party which can gather and keep customer's personal data at other IFM entity disposal, provided they have the right to do so. Instead of multiplying and duplicating personal data files (each for one application) as it is frequently the case, the effort should be put on defining specific roles for personal data handling stages from production to exploitation phases with specific responsibilities being attributed to defined IFM entities such as a personal data manager to be added to the overall IFM architecture.

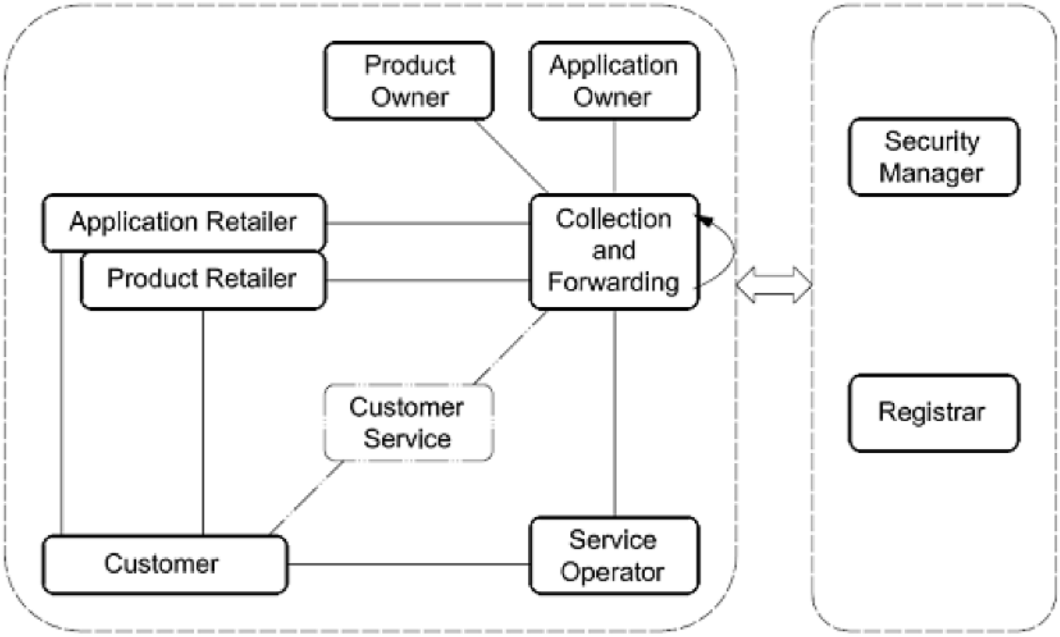


Figure C.7 — ISO 24014:— IFM operational and management entities

Annex D
(informative)

RFID applications in banking

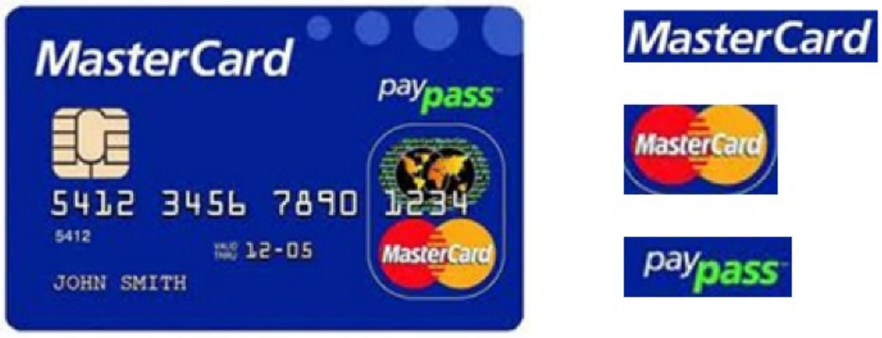
In the banking sector the RFID technology is utilized by the payment card industry to foster the business requirement of the merchants for faster low-value transactions (up to 20 EUR). Payment transaction authentication mechanisms such as entering a PIN or providing a signature are time consuming both for the cardholder and the merchant. In addition, the aim of the merchants to speed up the checkout and eliminate cash handling is coherent with the expansion strategy of the world largest payment scheme owners in the area of low value payments. The consumer (cardholder) at the POS is required to place the card in the proximity of a PCD (proximity coupling device), which is activated by the merchant in order to enable the contactless payment. If the single transaction limit exceeds 20 EUR or if a cumulative transaction limit is reached, the use of the contact EMV chip for cardholder authentication is required automatically by the PCD.

Purpose 1	**Low value transaction**
Purpose Description	The purpose of RFID use in banking/payment card industry is to provide a fast and reliable payment instrument for low value transactions.
Data subjects are	Cardholders (consumers using contactless payment cards)
Data classes are	Personal facts related to cardholders (Gender, Name); PAN (Primary account number); Expiration date; Personal facts related to Payment transactions:Transaction history

Utilization of logos in the banking sector

It is not common to have different logos on a Banking and credit card or tags as those devices are made for only one purpose and are not supposed to be used for multi-applications. This is mainly to ensure the high security of the card and its transactions. Those devices are mainly equipped with the logo of the issuer and associated partner if any. The logo of the banking company or credit card institute indicates the interoperability to a terminal of a trading partner. All major credit card companies such as VISA, MasterCard and American Express have created their own logo related to RFID to indicate the presence of RFID in their devices. There are no defined rules on providing directly further information to the consumers on the devices.

Following some examples:

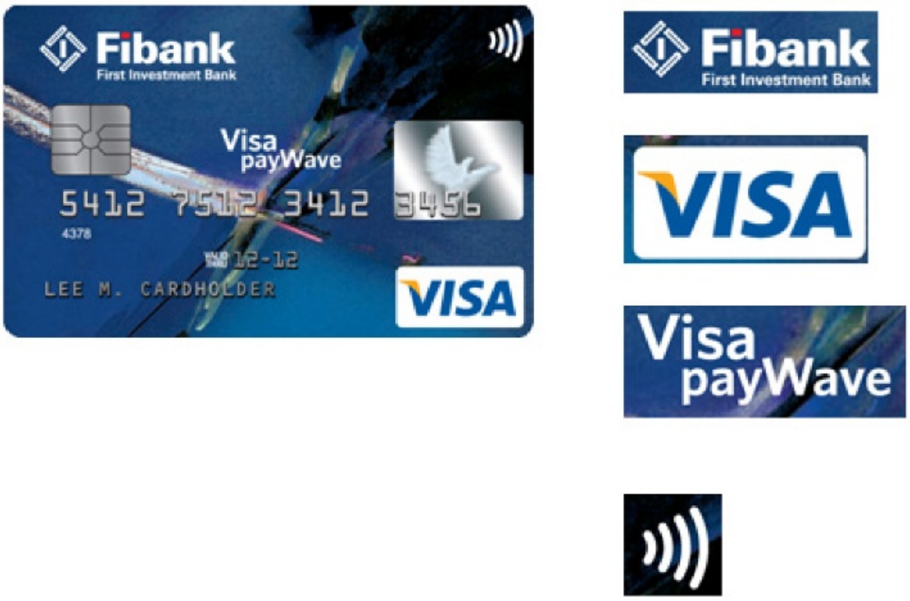


Indicates that this is a MasterCard

Logo of Mastercard

Logo to indicate interoperability to MasterCard related RFID terminals

Figure D.1 — MasterCard paypass



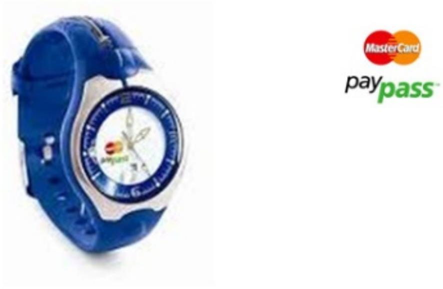
Indicates the issuer of the card

Logo of VISA

Logo indicates interoperability to VISA related RFID terminals

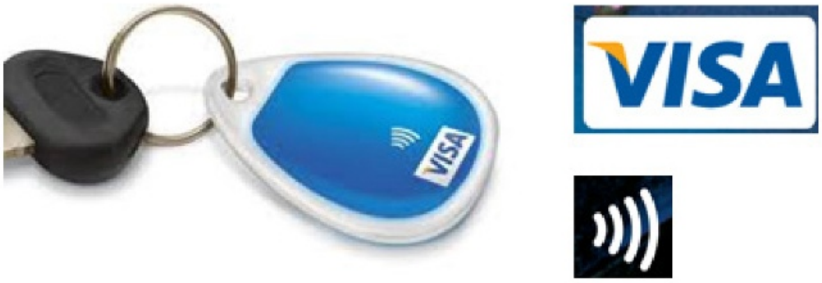
Logo to indicate that RFID technology is available in the card

Figure D.2 — Visa payWave



Logo to indicate interoperability to MasterCard related RFID terminals

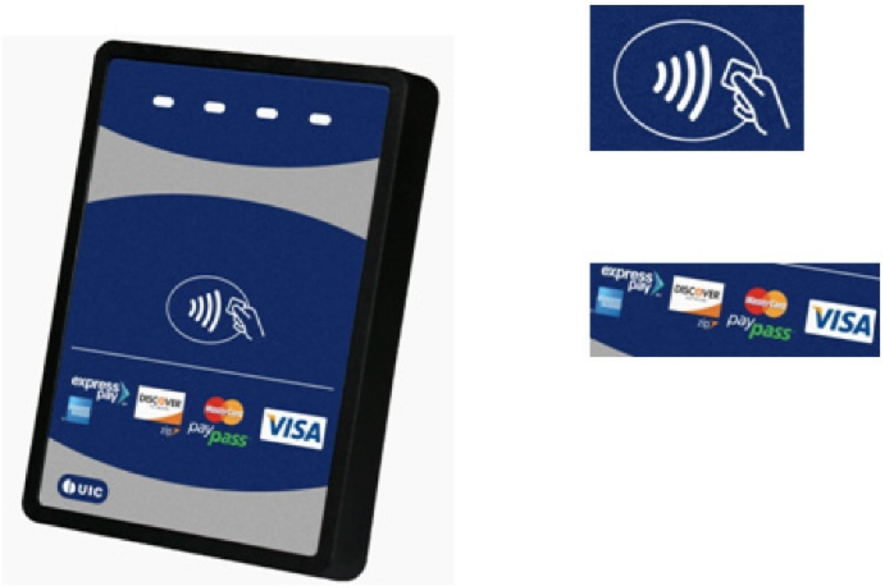
Figure D.3 — MasterCard paypass Watch



Logo of VISA

Logo to indicate that RFID technology is available in the card

Figure D.4 — Visa Key Chain



Logo for indicating an RFID interface

Logos to indicate the interoperability

Figure D.5 — Contactless Terminal

Bibliography

[1] COMMISSION RECOMMENDATION of 2009/05/12 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification {SEC (2009) 585}{SEC (2009) 586}., available at: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

[2] Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee, and the Committee of the Regions. Radio Frequency Identification (RFID) in Europe: steps towards a policy framework. {SEC (2007) 312}, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0096en01.pdf

[3] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37. Amended by Directive 2009/136/EC, available at: http://www.rfidineurope.eu/sites/default/files/RACE_deliverable_D5.1.3.1-2.pdf

[4] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[5] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[6] ETSI/TR 187 020, *Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436 available at:* http://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf

[7] Mandate 436, available at: http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/m436EN2.pdf

[8] The Article 29 Working Party has adopted a "Working paper 105 on data protection issues related to the RFID technology, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

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.

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

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

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 Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™