ETSI TR 187 020 V1.1.1 (2011-05)

Technical Report

Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436

Reference
DTR/TISPAN-07044

Keywords
privacy, RFID, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™, **TIPHON**™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

CEN and CENELEC have based their IPR policy on that of ISO, IEC and ITU-T. Patents or pending patent applications relating to a CEN or CENELEC publication may have been declared on this basis to CEN or CENELEC. Information on these declared patents or pending patent applications is made available by CEN and CENELEC via an on-line list of declarations (ftp://ftp.cen.eu/CEN/WorkArea/IPR/Patents.pdf).

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN). The present document has been prepared under the coordination of a technical experts group composed of representatives of each of ETSI, CEN and CENELEC and represents the agreed response of the European Standards Organizations (ESOs) to Mandate M/436 on the subject of Radio Frequency Identification Devices (RFID) in relation to data protection, information security and privacy.

NOTE: This work was funded under EC/EFTA Contract reference SA/ETSI/ENTR/436/2009-02.

1 Scope

The present document provides the results of the coordinated response of the European Standards Organizations (ESOs) to Phase 1 of EC mandate M436 on the subject of Radio Frequency Identification Devices (RFID) in relation to privacy, data protection and information security.

The present document outlines a standardization roadmap for privacy and security of RFID. The development of the roadmap involved analyses of RFID from a number of perspectives:

- analysis of OECD guidelines [i.17] and relevant data protection;
- analysis of privacy and its link to behaviour;
- analysis of EU directives on data protection and privacy and their implications on RFID;
- review of the role of PETs for RFID (see clause 7); and
- analysis of security threats to RFID and their implications (see Annex C).

The resulting requirements set defines the data protection, privacy and security needs of RFID and was used as input to the standards gaps analysis and the development of requirements to PIA for RFID and RFID PEN testing frameworks. An outline of the PIA framework requirements is given in clause 9.

Overview of the standardization gaps and requirements for RFID PEN testing is given in clause 10. The standardisation gaps analysis and resulting overall RFID standardisation roadmap is given in clause 4.

The present document recommends a plan of activities for Phase 2 of EC Mandate M436 as follows:

- identifies the use of existing technical measures described by standardisation in order to promote confidence and trust (by end users organizations and the general public) in RFID technology and its applications;
- identifies where new technical measures described by standardisation are required in order to promote confidence and trust (by end users organizations and the general public) in RFID technology and its applications. These measures will be developed in the course of phase 2 of the mandate.

In addition the present document describes the results of modelling the role of RFID in privacy and personal data as defined by European Directives alongside a Threat Vulnerability and Risk Analysis (TVRA) of the use of RFID technology and its applications, including the results of a generic and an industry specific Privacy Impact Assessment (a guide to PIA is given in Annex A).

NOTE: Many of the risks identified as part of the present document are equally applicable in other tracking scenarios (e.g. CCTV, car number/licence plate recognition, face recognition, mobile phone cell tracking). Under the terms of the Mandate, the present document covers only those areas in the data acquisition part that are specific to RFID. The other tracking scenarios are included in the work of the Article 29 Data Protection Working Party.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] EC Mandate 436: "Standardisation mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies Applied to Radio Frequency Identification (RFID) and Systems".

[i.2] ISO/IEC 15961 (all parts): "Information technology - Radio frequency identification (RFID) for item management - Data protocol: application interface".

[i.3] ISO/IEC 15962: "Information technology - Radio frequency identification (RFID) for item management - Data protocol: data encoding rules and logical memory functions".

[i.4] ISO/IEC 18001: "Information technology - Radio frequency identification for item management - Application requirements profiles".

[i.5] ISO/IEC 14443 (all parts): "Identification cards - Contactless integrated circuit(s) cards - Proximity cards".

[i.6] ISO/IEC 15693: "Identification cards - Contactless integrated circuit(s) cards - Vicinity cards".

[i.7] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity imanagement and their resolution in the NGN".

[i.8] ITU-T Recommendation X.200: "Information technology - Open Systems Interconnection - Basic Reference Model: The basic model".

[i.9] ISO/IEC 18000 (all parts): "Information technology - Radio frequency identification for item management".

[i.10] European Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.

NOTE: (Notified under document number C(2009) 3200), Official Journal L 122, 16/05/2009 P. 0047 - 0051.

[i.11] CENELEC EN 62369-1: "Evaluation of human exposure to electromagnetic fields from short range devices (SRDs) in various applications over the frequency range 0 GHz to 300 GHz - Part 1: Fields produced by devices used for electronic article surveillance, radio frequency identification and similar systems".

[i.12] Capgemini (2005): "RFID and Consumers - What European Consumers Think About Radio Frequency Identification and the Implications for Business".

[i.13] ISO/IEC 19762-1: "Information technology - Automatic identification and data capture (AIDC) techniques - Harmonized vocabulary - Part 1: General terms relating to AIDC".

[i.14] ISO/IEC 19762-3: "Information technology - Automatic identification and data capture (AIDC) techniques - Harmonized vocabulary - Part 3: Radio frequency identification (RFID)".

[i.15] ETSI TS 102 165-1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis".

[i.16] Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[i.17] Recommendation of the OECD Council in 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data (the OECD guidelines for personal data protection.

[i.18] ISO/IEC 27000 (2009): "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

[i.19] ISO/IEC 27001 (2005): "Information technology - Security techniques - Information security management systems - Requirements".

[i.20] ISO/IEC 13335: "Information technology - Security techniques - Guidelines for the management of IT security".

NOTE: ISO/IEC 13335 is a multipart publication and the reference above is used to refer to the series.

[i.21] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.22] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (R&TTE Directive).

[i.23] Article 29 Data Protection Working Party Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications.

[i.24] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.25] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.26] EUROPEAN DATA PROTECTION SUPERVISOR, Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework" COM(2007) 96, 2008/C 101/01.

[i.27] Microsoft: "The STRIDE Threat Model", 2005.

NOTE: Described in http://msdn.microsoft.com/en-us/magazine/cc163519.aspx and http://msdn.microsoft.com/en-us/library/ee823878(CS.20).aspx.

[i.28] NIST SP 800-115: "Technical Guide to Information Security Testing and Assessment", September 2008.

[i.29] ISSAF: "Information Systems Security Assessment Framework (ISSAF), draft 0.2.1B", 2006.

[i.30] ISO/IEC 29167 (all parts): "Information technology - Automatic identification and data capture techniques".

[i.31] German BSI TG 03126-1 Application area "eTicketing in public transport".

NOTE: German BSI documents are available from www.bsi.bund.de.

[i.32] ETSI TR 101 543: "Electromagnetic compatibility and Radio spectrum Matters (ERM); RFID evaluation tests undertaken in support of M/436 Phase 1".

[i.33] ISO/IEC 29160: "Information technology - Radio frequency identification for item management - RFID Emblem".

[i.34] ISO 11784: "Radio frequency identification of animals - Code structure".

[i.35] ISO 11785: "Radio frequency identification of animals - Technical concept".

[i.36] ISO 14223: "Radiofrequency identification of animals - Advanced transponders".

[i.37] ISO 9000: "Quality management systems - Fundamentals and vocabulary".

[i.38] Council Recommendation 1999/519/EC of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz).

[i.39] M/305 EN: Standardisation mandate addressed to CEN, CENELEC and ETSI in the filed of elctrotechnology, information technology and telecommunications.

[i.40] CENELEC EN 50357: "Evaluation of human exposure to electromagnetic fields from devices used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications".

[i.41] CENELEC EN 50364 (2001): "Limitation of human exposure to electromagnetic fields from devices operating in the frequency range 0 Hz to 10 GHz, used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications".

[i.42] CENELEC EN 50364 (2010): " Limitation of human exposure to electromagnetic fields from devices operating in the frequency range 0 Hz to 10 GHz, used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications".

[i.43] CENELEC EN 50499 (2008): "Procedure for the assessment of the exposure of workers to electromagnetic fields".

[i.44] Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003 on waste electrical and electronic equipment (WEEE) - Joint declaration of the European Parliament, the Council and the Commission relating to Article 9.

[i.45] ISO/IEC 24791-5: "Information technology - Radio frequency identification (RFID) for item management - Software system infrastructure - Part 5: Device interface".

[i.46] ISO/IEC 24791-3: "Information technology - Automatic Identification and Data Capture Techniques - Radio-Frequency Identification (RFID) for Item Management - System Management Protocol - Part 3: Device management".

[i.47] ISO/IEC 24791-2: "Information technology - Automatic Identification and Data Capture Techniques - Radio-Frequency Identification (RFID) for Item Management - System Management Protocol - Part 2: Data management".

[i.48] ISO/IEC 18092: "Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)".

[i.49] OSSTMM: "Open Source Security Testing Methodology Manual".

[i.50] COM(2008) 804 final; Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: "Towards an accessible information society".

[i.51] ETSI EG 202 116: "Human Factors (HF); Guidelines for ICT products and services; "Design for All".

[i.52] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.53] EPCglobal: "Low Level Reader Protocol (LLRP)", V1.1.

NOTE: Available from: http://www.gs1.org/gsmp/kc/epcglobal/llrp/llrp_1_1-standard-20101013.pdf.

[i.54] Directive 2004/40/EC of the European Pariliament and of the Council of 29 April 2004 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (18th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC).

[i.55] ISO 14000: "Enviromental Management".

[i.56] EPCglobal: "Discovery, Configuration and Initialisation (DCI) standard".

[i.57] EPCglobal: "Tag Data Standard".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 202 387 [i.24], ISO/IEC 27001 [i.19], ISO/IEC 13335-1 [i.20], ISO/IEC 19762-3 [i.14], ISO/IEC 19762-1 [i.13] and the following apply:

agency: ability and opportunity of the individual to make independent choices

air interface: conductor-free medium, usually air, between a transmitter and the receiver through which communication, e.g. data and telemetry, is achieved by means of a modulated inductive or propagated electromagnetic field

anonymity: act of ensuring that a user may use a resource or service without disclosing the user's identity

asset: anything that has value to the organization, its business operations and its continuity

authentication: ensuring that the identity of a subject or resource is the one claimed

confidentiality: ensuring that information is accessible only to those authorized to have access

data 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

NOTE 1: 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.

NOTE 2: "RFID Operator" means data controller in the context of the present document.

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

data subject: 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

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

disruptive technology: technology which has a rapid and major effect on technologies that existed before

NOTE: Examples of disruptive technologies include the Sony Walkman, the mobile phone, and the Internet.

High Frequency (HF) RFID systems: RFID systems that operate in the frequency band centred around 13,56 MHz

identifier: unique series of digits, letters and/or symbols assigned to a subscriber, user, network element, function, tag or network entity providing services/applications

identity: set of properties (including identifiers and capabilities) of an entity that distinguishes it from other entities

identity crime: generic term for identity theft, creating a false identity or committing identity fraud

identity fraud: use of an identity normally associated to another person to support unlawful activity

identity theft: acquisition of sufficient information about an identity to facilitate identity fraud

identity tree: structured group of identifiers, pseudonyms and addresses associated with a particular user's identity

impact: result of an information security incident caused by a threat and which affects assets

information security incident: event which is the result of access to either stored or transmitted data by persons or applications unauthorized to access the data

integrity: safeguarding the accuracy and completeness of information and processing methods

Low Frequency (LF) RFID systems: RFID systems that operate in the frequency band below 135 kHz

mitigation: limitation of the negative consequences of a particular event

non-repudiation: ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

personal data: any information relating to an identified or identifiable natural person

privacy: right of the individual to have his identity, agency and action protected from any unwanted scrutiny and interference

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

processing of personal data: any operation or set of operations which is performed upon personal data, whether or not by automatic means

NOTE: Examples of processing are collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

pseudonymity: act of ensuring that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use

NOTE: This is similar to the act of providing an alias and examples include the TMSI service in 2G networks and the ASSI service in TETRA.

radio interception range: range at which an attacker can gain knowledge of the content of transmission

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

risk: potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the attacked system or organization

taxonomy: practice and science of classification

threat: potential cause of an incident that may result in harm to a system or organization

threat agent: entity that can adversely act on an asset

Ultra High Frequency (UHF) RFID systems: RFID systems which operate either at 433 MHz or within the band 860 MHz to 960 MHz

NOTE 1: Devices that designed to operate at 433 MHz generally cannot operate at 860 MHz to 960 MHz and vice versa.

NOTE 2: The UHF frequency range is defined as lying from 300 MHz to 3 000 MHz with UHF RFID occupying a small subset of the range.

unlinkability: act of ensuring that a user may make multiple uses of resources or services without others being able to link these uses together

unobservability: act of ensuring that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used

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

NOTE: As defined in ISO/IEC 13335 [i.20], a vulnerability is modelled as the combination of a weakness that can be exploited by one or more threats.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Air Interface
API	Application Programming Interface
BES	Back End System
CIA	Confidentiality, Integrity and Availability
CRC	Cyclic Redundancy Check
DoS	Denial-of-Service
DPA	Data Protection Authority
DPP	Data Privacy and Protection
EAS	Electronic Article Surveillance
EMF	Electro-Magnetic Field
ESO	European Standards Organization
ICNIRP	International Commission on Non-Ionizing Radiation Protection
ICS	Implementation Conformance Statement
IEC	International Electro-technical Commission
IERC	IoT European Research Cluster
IoT	Internet of Things
ISSAF	Information Systems Security Assessment Framework
MIM	Man-In-the-MIddle
MTS	Methods for Testing and Specification
NFC	Near Field Communication
NGN	Next Generation Network
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
OID	Object IDentifier
OSI	Open Standards Interoperability
OSSTMM	Open Source Security Testing Methodology Manual
PbD	Privacy by Design
PEN	PENetration
PET	Privacy Enhancing Technology
PIA	Privacy and data protection Impact Assessment
RACI	Responsibility Assignment Matrix (RAM)

NOTE: Also known as RACI matrix.

RF	Radio Frequency
RFID	Radio Frequency Identification
RTLS	Real Time Location System
ToE	Target of Evaluation
TVRA	Threat Vulnerability and Risk Analysis

4 Summary of findings and recommendations

4.1 Overview of findings

This clause summarises the findings of the present document with respect to Radio Frequency Identification Devices (RFID) in relation to privacy, data protection and information security.

The main points raised and examined in the present document are as follows:

- the existing data protection and privacy protection legislation applies to the operation of RFID systems;

- the existing definition of personal data in legislation includes the indirect gathering of behaviour and correlation of behaviour in back end systems and at interrogators;
- attacks on privacy in large ICT systems will exist irrespective of the existence of RFID and as such addressing privacy has to be both independent of the technology and at the same time recognise the specific threats introduced by RFID technology;
- the definition of the term RFID and of RFID systems covers a wide range of technologies and capabilities and has led to confusion amongst potential users and beneficiaries of the technology;
- privacy and data protection is not just about the protection of personal data elements that are defined by law;
- data derived from observation of behaviour may imply the identity of a person;

NOTE 1: This is already considered in the definition of personal data in the data protection and privacy directive [i.54].

- RFID devices and systems containing personal data should protect that data as advised by the existing data protection and privacy directives;

NOTE 2: The opinion of the Article 29 Data Protection Working Party [i.26] is that if the tag can be associated to a person all of its data is personal data.

NOTE 3: The R&TTE directive [i.22] does not currently reference the data protection directive [i.54] and applies to the placement of articles on the market. The Data Protection Directives apply once a system commences its intended use.

- consent of data access and use without a user interface is difficult and thus privacy analysis has to be done in a way that takes these RFID specific aspects into account and thus the present document identifies a need for an RFID specific PIA process and identifies the requirements for such a process;
- the role of consent (which has to be informed, meaningful, explicit and unambiguous) in data protection is examined and the role of emblems and signs (including commercial logos) to raise awareness of the presence of RFID tags and interrogators, to enable awareness where consent is not otherwise given, is examined with the requirements to be met by such emblems and signs documented;
- the present document identifies a number of attacks that may be made against RFID systems and their components and summarises the security technologies that should be applied to minimise the risk across the system. This is done by identifying the set of security and privacy objectives to be met by the RFID system.

4.2 Clarification of definition of RFID

The misuse of the term RFID to cover a wide range of very different technologies has been a significant contributor to the consumer concerns reviewed in the present document.

For the purposes of the present document, Radio Frequency Identification (RFID) is considered as a technology that allows objects to be "tagged" with an identifier that can be read remotely using either inductive electromagnetism or emitted radio waves. Due to the very broad range of applications, the distances at which tags may be interrogated will vary considerably according to the operational requirements. For passive systems distances may vary from a few centimetres up to 10 metres. The data content of the tag may either be fixed at manufacture or programmed subsequently by the operator. In addition the term RFID is also applied to tags with embedded microprocessors which are distinct from those with memory only and serve a different form of application.

Often an RFID system will comprise many tags and a relatively small number of interrogators (a ratio of many thousands to one may be considered typical in retail and logistics tracking applications).

NOTE 1: Frequently public perception and marketing announcements include Real Time Location Systems (RTLS), such as beacons, as an RFID technology. The scope of RFID considered in the present document does not consider RTLS and RFID as equivalent.

NOTE 2: RFID tags are categorised as transponders and on occasion the term transponder is used to describe an RFID tag.

NOTE 3: It is the tag that is read and not the object to which it is attached. Thus an object with an inappropriate or incorrectly encoded tag attached will be recognised by the system according to the tag and not by any other information.

4.3 Summary of standardisation gaps

A summary of the required standards to be developed to address the findings of the study is given below in a number of categories along with a plan for their implementation.

4.3.1 General principles

The approach to standardisation to increase consumer confidence implies a number of key points to be addressed by the ESOs. These are summarised below and specific areas where standardisation is required are outlined in subsequent clauses.

- Classification by privacy and security capability of the application (used in PIA).
- Classification by privacy and security capability of the air interface technology (to be used in PIA).
- Classification of the data protection technologies (to be used in PIA).

4.3.2 Standards to provide greater consumer awareness

The rationale for this work is described in clause 11 and Annex E and also justified in the consideration of a Consent framework under analysis of privacy and data protection in clauses 7 and 8.

The lead body for the development of standards in this area will be CEN TC225 with the close involvement of user groups represented by ANEC and by each of ETSI TC HF and ETSI USER groups. The specific standards to be developed will be the following:

- EN for common European Emblem;
- EN to specify customer and consumer information provision associated with RFID applications; and,
- EN to specify the supplementary information to be displayed in areas where RFID interrogators are deployed (Common European RFID Sign).

The Common European RFID Sign will be designed to comply with the guidelines for data protection to identify the data controller and purpose of the data that is gathered in addition to the data identified as requirements in Annex E. In addition the Common European RFID Sign will be designed to comply with the guidelines for accessibility defined by the "Design for All" initiative from the EU initiative "Towards an accessible information society" [i.50] and EG 202 116 [i.51].

4.3.3 Standards in the privacy domain (excluding PIA)

Much is made in documentation of adoption of privacy by design but there is no standard method or guidance for achieving privacy by design. The items in this area are intended to plug this gap.

- EN to specify the method of "Privacy by Design".
- EN defining a checklist for application of "Privacy by Design" method.

NOTE 1: Privacy by design is a paradigm that is not restricted to RFID and thus the standardisation effort in this area should not be considered only for RFID but rather the requirements of RFID should be considered in the standardisation.

- Tag privacy performance capability catalogue.
- Interrogator privacy performance capability catalogue.

- RFID Air Interface (radio protocol) privacy performance capability catalogue.

NOTE 2: A catalogue is a summary of the capabilities of devices. The set of capabilities and the metrics for their measurement to be provided has to be specified elsewhere as a pre-requisite of the definition of the catalogues.

NOTE 3: For all the above a checklist of capability against PETs is required.

NOTE 4: In many cases the above may not require new work but instead a catalogue of the existing capabilities to allow classification as described in clause 4.3.1.

The intent of the capability catalogues is to provide authoritative performance measure of the particular element against the defined metrics. In due course further application specific will need to be able to associate devices with the levels of performance needed to provide privacy and security relevant to the applications for which the devices are to be used.

4.3.4 PIA standards

As outlined in clauses 7 and 8 and defined in more detail in clause 9 the PIA is key to the organisational treatment of privacy issues using technology. This is required to be specific to the RFID technology and its applications but has to be within a wider PIA framework.

- Definition of the PIA detailed Process.
- Method, conformance and application guidance.

The lead body for this standardisation effort should be CEN to allow direct access to ISO (through the Vienna agreement mechanism).

NOTE 1: A submission of a PIA framework has been made to the Article 29 Data Protection Working Party [i.23]. The PIA framework has to be taken into account in the course of phase 2 of M436 and the development of the PIA process and associated guidance.

NOTE 2: Whist PIA standards are essential there is an associated need for "good practice frameworks" to support them that is expected to be addressed once the base PIA standards are in place.

4.3.5 RFID Penetration testing standards

As outlined in clause 10 and in more detail in Annex D there is a very important role for Penetration testing in support of risk assessment (see Annex C). The lead body for this work is expected to be ETSI TISPAN WG7 with coordination through ETSI MTS and the relevant RFID groups including ETSI ERM TG34 and TC 225.

- EN to specify the method for Penetration testing.
- EN defining a checklist for application of the Penetration testing method.

NOTE: The RFID ecosystem is comprised of frontend and backend parts. Penetration testing methods already exist to support RFID backend systems and thus the standardisation effort in this area will be on defining a checklist for application of existing methods to RFID.

4.3.6 Standards in the security domain

As outlined in clauses 7, 8 and10 and in Annexes C and F, the RFID security system is poorly understood and the means to protect data in an RFID environment impact all parts of the RFID ecosystem. The lead body of this work is expected to be ETSI TISPAN WG7 with support from ETSI MTS, and the relevant RFID groups including ETSI ERM TG34 and CEN TC225.

- EN to specify the method of "Design for Assurance".
- EN defining a checklist for application of "Design for Assurance" method.

NOTE 1: Design for assurance is a paradigm that is not restricted to RFID and thus the standardisation effort in this area should not be considered only for RFID but rather the requirements of RFID should be considered in the standardisation.

- EN to specify the a framework for proof of consent in an RFID environment.

NOTE 2: This may be similar to a non-repudiation framework but is defined to extend the role of consent in the use of personal data in the RFID environment.

- Guide to selection of privacy enhancing technologies for RFID applications.

NOTE 3: The generally accepted view in security threat analysis is that broadcast technologies such as radio are open to interception as that is their intended mode of operation. In order to protect data transferred over the radio interface in RFID systems there are a number of steps that should be taken depending on the nature of the content and the value that an unintended recipient can attach to the intercepted data. In simple terms where tag data contains static personal data (c.f. the left hand side of the ontology (concept relationship diagram) presented in clause 7) the transmission should be encrypted (i.e. the attacker should not be able to gain knowledge of the content of the data from observation of the intercepted data or its triggering signal).

4.4 Gaps in current standards

4.4.1 Overview

The standards gaps analyses have uncovered critical gaps and there is a need for standardisation activities in a number of fields to bridge these gaps. Of these the most essential challenges are:

a) current technology comprising the privacy by design best practice standards;

b) lack of RFID privacy impact assessment standards; and

c) lack of conformance assurance measures and regulations on how to inform the public.

Each of these is necessary to build consumer confidence and each should be founded on the privacy by design principles and RFID privacy impact assessment. Work has commenced within ISO (ISO/IEC JTC1/SC31) to develop a global system for security of data carried by RFID tags. This will enable the security of RFID systems to be adjusted appropriately to meet the needs of individual applications. It is expected that the ESOs will adapt this global work for use within a European context.

NOTE 1: The present document recognises that the deployment of such technologies may take considerable time once the standards are available and that by themselves standards will not address the concerns raised.

There is a further requirement to specify the metrics by which different RFID devices can be compared. This is directly related to the development of the catalogues that need to be able to illustrate common metrics. In particular to maximise the ability of consumers to be aware of RFID device capability attention has to be paid to the set of metrics to catalogued and should include consumer preferred metrics.

NOTE 2: For many aspects of RFID operation metrics already exist (e.g. sensitivity level, data storage space).

4.4.1.1 Summary of main gaps

A simplified summary of the main gaps in standardisation identified in the present document are given in Table 1.

Table 1: RFID standards gaps summary

Technical issues	Gaps to be filled
Personal information inferred from "non personal" data	Guidance on the application of the EU Data Protection definitions to improve their interpretation in relation to RFID applications. RFID privacy categorization that identifies whether identified items are intended to be in the possession of people. Those applications with purposes that are not for personal possession can then be treated less onerously than those that are (see clause 4.2.1).
Tags always readable with associated fears of unauthorized reading. This impacts upon the data to be held on the tag, read distances and the security measures on the tag.	Privacy by design standards for tag data through security throughout the rest of the system. Interrogators, back end systems and applications all need to be addressed to minimize privacy and security risks. Define classification of device types (see clause 4.2.1) using data obtained from penetration testing and user input. Where practical and appropriate, the enhanced on-tag user control of readability including user determined kill or disable capability.
Multipurpose tags. (I.e. tags where multiple valid purposes exist such as production, sales, service and end of life).	Data Protection guidance and standards which ensure that for multiple purpose tags each purpose is correctly addressed. Tag and interrogator standards ensuring suitable authentication and access control by each application/purpose. Consumer notification and informed consent process standards especially when one purpose ends and the next starts. Consumer information standards for items intended for multiple purposes. Interoperability standards for applications which make use of interrogators provided by a number of operators for multiple purposes. (See note.)
Lack of interaction capability.	Application management and operational standards.
RFID characteristics in tota.l	Application management and operation standards accommodating the full range of technology issues given above.
NOTE: This activity is partly covered by development of the 18000 series ISO standards [i.9].	

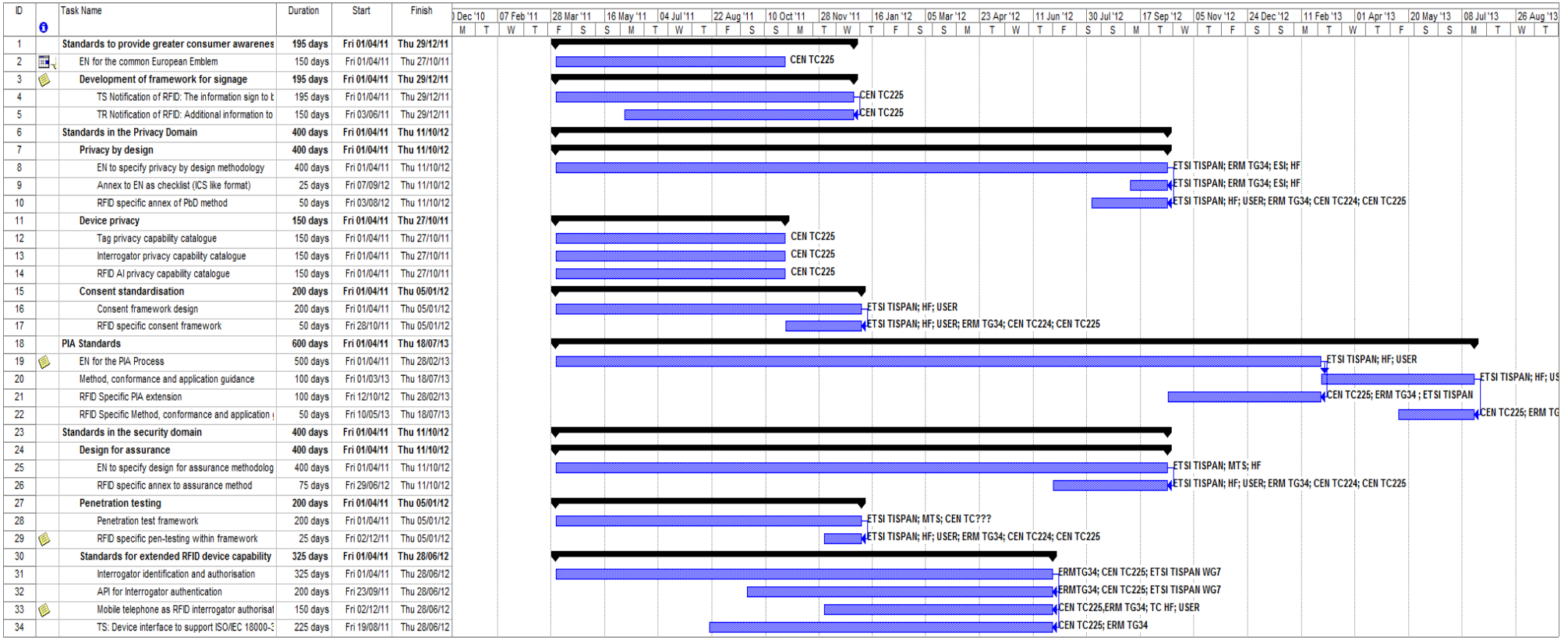
NOTE: Not all of the gaps require to be filled by technical means but means may be provided through process and procedure.

4.4.2 Gantt chart for addressing gaps in Phase 2 of M/436

Table 2 summarises the tasks and the ESO bodies involved in development of standards to address the gaps identified in the main body of the present document. The Gantt chart displays elapsed times for completion of each of the tasks.

Table 2: RFID standardisation activity for phase 2 to close identified gaps

	Task or subtask	ESO bodies to be involved
A	**Standards to provide greater consumer awareness**	
A.1	EN for the common European Emblem	CEN TC225
A.2	***Development of framework for signage***	CEN TC225
A.2.1	TS Notification of RFID: The information sign to be displayed in areas where RFID interrogators are deployed	CEN TC225
A.2.2	TR Notification of RFID: Additional information to be provided by operators	CEN TC225
B	**Standards in the Privacy Domain**	
B.1	***Privacy by design***	
B.1.1	EN to specify privacy by design methodology	CEN WS/DPP, ETSI TISPAN; ERM TG34; ESI; HF
B.1.2	Annex to EN as checklist (ICS like format)	CEN WS/DPP, ETSI TISPAN; ERM TG34; ESI; HF
B.1.3	RFID specific annex of PbD method	ETSI TISPAN; HF; USER; ERM TG34; CEN TC224; CEN TC225
B.2	***Device privacy***	
B.2.1	Tag privacy capability catalogue	CEN TC225
B.2.2	Interrogator privacy capability catalogue	CEN TC225
B.2.3	RFID AI privacy capability catalogue	CEN TC225
B.3	***Consent standardisation***	
B.3.1	Consent framework design	ETSI TISPAN; HF; USER
B.3.2	RFID specific consent framework	ETSI TISPAN; HF; USER; ERM TG34; CEN TC224; CEN TC225
C	**PIA Standards**	
C.1	EN for the PIA Process	CEN (including the CEN WS/DPP) with support of ETSI TISPAN; HF; USER and coordination with ISO SC27
C.2	Method, conformance and application guidance	ETSI TISPAN; HF; USER; ERM TG34; CEN TC225
C.3	RFID Specific PIA extension	CEN TC225; ERM TG34 ; ETSI TISPAN
C.4	RFID Specific Method, conformance and application guidance	CEN TC225; ERM TG34 ; ETSI TISPAN
D	**Standards in the security domain**	
D.1	***Design for assurance***	
D.1.1	EN to specify design for assurance methodology	ETSI TISPAN; MTS; HF
D.1.2	RFID specific annex to assurance method	ETSI TISPAN; HF; USER; ERM TG34; CEN TC224; CEN TC225
D.2	***Penetration testing***	
D.2.1	Penetration test framework	ETSI TISPAN; MTS; CEN TBA
D.2.2	RFID specific pen-testing within framework	CEN TC225; ETSI TISPAN; HF; USER; ERM TG34;
E	**Standards for extended RFID device capability**	
E.1	Interrogator identification and authorisation	ERMTG34; CEN TC225; ETSI TISPAN WG7
E.2	API for Interrogator authentication	ERMTG34; CEN TC225; ETSI TISPAN WG7
E.3	Authorisation of a mobile telephone when used as an RFID interrogator	CEN TC225,ERM TG34; TC HF; USER
E.4	TS: Device interface to support ISO/IEC 18000-3 [i.9] Mode 1 and Mode 3 tags	CEN TC225; ERM TG34



ID	Task Name	Duration	Start	Finish
1	**Standards to provide greater consumer awarenes**	**195 days**	**Fri 01/04/11**	**Thu 29/12/11**
2	EN for the common European Emblem	150 days	Fri 01/04/11	Thu 27/10/11
3	**Development of framework for signage**	**195 days**	**Fri 01/04/11**	**Thu 29/12/11**
4	TS Notification of RFID: The information sign to t	195 days	Fri 01/04/11	Thu 29/12/11
5	TR Notification of RFID: Additional information to	150 days	Fri 03/06/11	Thu 29/12/11
6	**Standards in the Privacy Domain**	**400 days**	**Fri 01/04/11**	**Thu 11/10/12**
7	**Privacy by design**	**400 days**	**Fri 01/04/11**	**Thu 11/10/12**
8	EN to specify privacy by design methodology	400 days	Fri 01/04/11	Thu 11/10/12
9	Annex to EN as checklist (ICS like format)	25 days	Fri 07/09/12	Thu 11/10/12
10	RFID specific annex of PbD method	50 days	Fri 03/08/12	Thu 11/10/12
11	**Device privacy**	**150 days**	**Fri 01/04/11**	**Thu 27/10/11**
12	Tag privacy capability catalogue	150 days	Fri 01/04/11	Thu 27/10/11
13	Interrogator privacy capability catalogue	150 days	Fri 01/04/11	Thu 27/10/11
14	RFID AI privacy capability catalogue	150 days	Fri 01/04/11	Thu 27/10/11
15	**Consent standardisation**	**200 days**	**Fri 01/04/11**	**Thu 05/01/12**
16	Consent framework design	200 days	Fri 01/04/11	Thu 05/01/12
17	RFID specific consent framework	50 days	Fri 28/10/11	Thu 05/01/12
18	**PIA Standards**	**600 days**	**Fri 01/04/11**	**Thu 18/07/13**
19	EN for the PIA Process	500 days	Fri 01/04/11	Thu 28/02/13
20	Method, conformance and application guidance	100 days	Fri 01/03/13	Thu 18/07/13
21	RFID Specific PIA extension	100 days	Fri 12/10/12	Thu 28/02/13
22	RFID Specific Method, conformance and application	50 days	Fri 10/05/13	Thu 18/07/13
23	**Standards in the security domain**	**400 days**	**Fri 01/04/11**	**Thu 11/10/12**
24	**Design for assurance**	**400 days**	**Fri 01/04/11**	**Thu 11/10/12**
25	EN to specify design for assurance methodolog	400 days	Fri 01/04/11	Thu 11/10/12
26	RFID specific annex to assurance method	75 days	Fri 29/06/12	Thu 11/10/12
27	**Penetration testing**	**200 days**	**Fri 01/04/11**	**Thu 05/01/12**
28	Penetration test framework	200 days	Fri 01/04/11	Thu 05/01/12
29	RFID specific pen-testing within framework	25 days	Fri 02/12/11	Thu 05/01/12
30	**Standards for extended RFID device capability**	**325 days**	**Fri 01/04/11**	**Thu 28/06/12**
31	Interrogator identification and authorisation	325 days	Fri 01/04/11	Thu 28/06/12
32	API for Interrogator authentication	200 days	Fri 23/09/11	Thu 28/06/12
33	Mobile telephone as RFID interrogator authorisat	150 days	Fri 02/12/11	Thu 28/06/12
34	TS: Device interface to support ISO/IEC 18000-3	225 days	Fri 19/08/11	Thu 28/06/12

5 Addressing consumer aspects

5.1 Awareness

Consumer awareness embraces:

- the increased customer awareness of the presence of tags is required because by their nature tags are intended to be readable without user intervention (i.e. the user does not control the activation of tags);
- emblems, signs and information accessibility;
- consumer information providing an understanding of the benefits arising from specific RFID applications;
- the provision of sufficient consumer information to allow informed consent to data collection;
- consumer information is also needed to provide an understanding of how to undertake other actions that are part of the Data Protection Directive requirements; and
- the consumer management of residual risks (e.g. keeping RFID credit cards in the shielded wallets provided).

These concerns should be addressed by the following actions:

- emblem and sign standards;
- PIA standards enabling residual risk analysis to input into the provision of information to consumers when any such risks are significant; and
- the provision of standards specifying consumer information.

NOTE: Such standards should fill the operational and management gaps relating to RFID applications.

5.2 Personal data security

Two main personal data security concerns expressed by consumers related to the security of personal data are:

- Whole system personal data security:
  - This concern particularly addresses the linkability of tag data to personal details arising from data collected for legitimate purposes.
- Security of RFID tag / interrogator personal data (direct personal information and inferred personal data) when data may be collected using illicit means for illicit purposes.

These concerns should be addressed through the following actions:

- Whole system personal data security:
  - Privacy by design standards which will raise the level of system security design and system implementation.
  - RFID operational and management standards which can be utilised alongside privacy by design standards. The operational performance and management standards includes those people and process management good practices necessary to address the risks arising from unmanaged human weaknesses that can contribute to a lessening of the security of personal data within the system.

- Illicit tag data collection:
  - Illicit tag interrogation and eavesdropping with current RFID standards requires privacy risk analysis and deployment of appropriate mitigation actions "outside the chip".

NOTE: Such mitigation always remains subject to human error in applying the extra protection, or the impracticability of introducing privacy enhancing technology on grounds of cost and or unsuitability to the application. Privacy by design standards will identify best practice to minimise such risks using current technology.

5.3 Data Protection Requirements

The technical characteristics of RFID present a challenge to the operators of RFID applications when fulfilling their obligations under European personal data protection legislation.

Appropriate RFID operations and management standards facilitate good practice. Specific areas that such standards address are described in the following clauses.

5.3.1 Purpose

A single tag may be used for a number of distinct and specific purposes. The consumer should be informed when a purpose stops and a new purpose begins. In each case consent may be required and the system should not assume that consent is transferable between purposes.

NOTE: The consumer may elect to define a new purpose (e.g. using a food supply chain tag in the domestic food store (fridge)).

5.3.2 Deactivation

The consumer expects to be able to de-activate the tag or the capability of the tag to be read. The right to deactivate is dependent on the relationship of the tag to the user (i.e. as tag owner or keeper there is a greater expectation of control of deactivation). In addition there may be a requirement to reactivate a tag in order to use the tag for a new purpose (or a new instance of the original purpose). This latter requirement implies a need for both permanent and temporary deactivation (need for reactivation under consumer control).

NOTE 1: Deactivation of the tag should be linked to removal or deactivation of data in the wider system.

NOTE 2: Existing and future planned regulation in Europe may not support the concerns on deactivation and purpose identified in this clause (e.g. in some cases such as Government issued passports deactivation will not be allowed by the tag holder).

NOTE 3: Shields may be used to limit the visibility of tags by restricting the ability of a tag to be activated under user control. However at the point of purpose the shield has to be removed and the full range of attacks are exposed.

5.3.3 Consent

According to the Data Protection Directive, personal data may only be processed if the data subjects (i.e. individuals) have unambiguously given their consent. Next to being explicit, consent should also be informed and thus meaningful. The logos and signs examined in the present document play an important role in creating awareness and informing consumer consent.

An example where consent is required is that of RFID tags in consumer products. At the point of sale, individuals should be asked whether they want the tag to remain readable after purchase. Individuals may also wish to revoke previously given consent. This could mean that chips should have the capability to be "switched off"', as defined in German BSI TG 03126 [i.31]

Since it is not considered feasible or realistic to ask consent for each tagged item, the industry is expected to provide solutions, as defined in German BSI TG 03126 [i.31]. Opt out regimes are not likely to meet the definition of consent under the Directive.

5.3.4 Personal data record access and data correction

Whether personal data is held on tags, which currently have no interaction capability, or it is behavioural personal data held centrally (such as travel journey records with respect to the London Underground), consumers have the right to ask for copies of such data to check and correct any errors (such as identifying those journeys recorded and charged for which arise from a cloned RFID travel card).

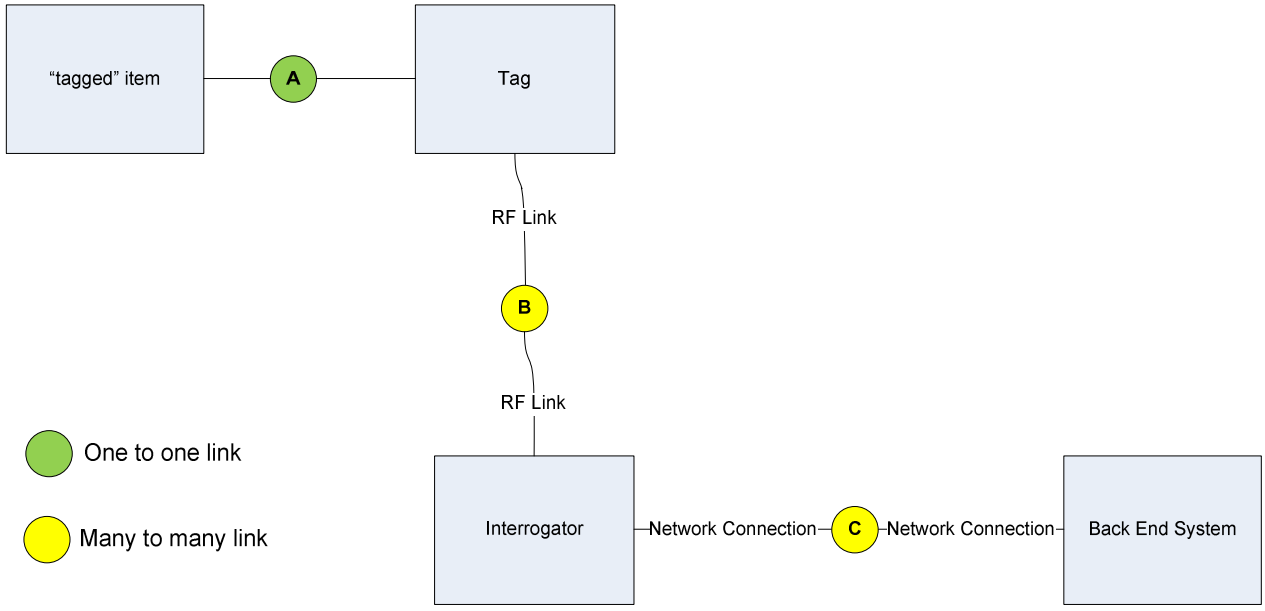
5.4 Accessibility of applications and consumer information

Accessibility requirements under the design for all initiative are to be considered in each of the new standards where accessibility is appropriate to that standard. For example this requires that access to information should not be discriminatory.

6 The RFID ecosystem

6.1 Overview

As noted in the introduction to the present document and shown in Figure 1 the RFID ecosystem consists of tagged items, tags, interrogators, a back end processing system and the interconnecting networks. This clause outlines some of the technology behind these components.



NOTE: The technology links (B, C) are many to many in scope but may be restricted by implementation using Privacy Enhancing Technologies (PETs) and basic security technologies to be one-to-one, many-to-one or one-to-many.

Figure 1: RFID ecosystem

The tag is the primary data containing element of RFID and has a wide range of capabilities. The RF link between the interrogator and tag also has a very wide range of capabilities and this is described in the following clauses.

NOTE: The Open Systems Interconnection model defined in ITU-T Recommendation X.200 [i.8] is the template for design of most modern communications systems. RFID technology is not OSI compliant and as such cannot be deployed in an OSI network as a replacement of any other OSI compliant technology.

6.2 Types of RFID Tags

ISO/IEC 19762 [i.13] defines the following type of RFID tags:

- Active tag:
  - RFID device having the ability of producing radio signal;
  - active tags always have a their own power source.
- Passive tag:
  - RFID device which reflects and modulates a carrier signal received from an interrogator;
  - passive tags do not contain a power source. As such, they are completely dependent on power from the RFID interrogator to activate them.
- Battery assisted tags:
  - battery assisted passive tags use the same physical communication principle as passive tags. However, they contain a power source which is used to maintain data in the tag between activations from the RFID interrogator and/or to increase the sensitivity of the tag's input circuit.
- Read only or read/write:
  - read only tags: are factory programmed, or can be initialized (i.e. programmed with data) only one time;
  - read/write tags: can be updated (i.e. reprogrammed) multiple times.

NOTE: Even if the tag is writeable an interrogator may be restricted to perform read operations only by design or by policy in the deployment environment.

6.3 RFID Tag Characteristics

RFID characteristics include:

- Memory size: determines how much information can be stored.
- Frequency: a variety of frequencies have been designated for RFID. The frequency selected is determined by the application.
- Size: ranges from a pinhead to a brick.
- For passive tags, antenna size determines, together with the power of the interrogator, the range at which the tag can be read. The antenna design also defines the beam pattern.

NOTE 1: Emission levels are specified by national administrations.

NOTE 2: Antenna size is also dependent on the frequency of operation and often expressed as a function of wavelength thus higher frequency operation requires a physically smaller antenna for a given performance.

For further details on RFID tag characteristics, please refer to Annex C and Table B.2.

The RF characteristics of the air interface between tag and interrogator are standardized in ISO 11784 [i.34], ISO 11785 [i.35], ISO 14223 [i.36], ISO/IEC 14443 [i.5], ISO/IEC 15693 [i.6] and additionally in ISO/IEC 18000-n [i.9], where n denotes the part of the ISO/IEC document according to operating frequency. Whilst it is tempting to compare the RFID to other radio technologies this is not instructive other than by recognising the diverse range of radio technology application and the strain of different technologies on the available radio spectrum. However a radio receiver may be designed to give approximately 30 dB more sensitivity to radio signal detection than an RFID interrogator in the same frequency range to achieve its design goal. This capability may be used by a hostile attacker to identify the presence of interrogators and tags.

6.4 Stakeholders

The main actors in RFID include the following and their role in the technology is summarised here (note that this list is not exhaustive and other actors and stakeholders may exist):

- Consumers and members of the public:
  - Holders of items with RFID tags.
- RFID manufacturing sector:
  - Responsible for the manufacture of RFID devices and their associated sub-systems (antennas, interrogators, smart-labels and so forth).
- RFID deployment sector (including systems integrators):
  - Responsible for the RFID systems integration and/or deployment. RFID Systems may contain tags, antennas, interrogators, back-end systems and application software. Integration and deployment is usually performed against an application requirement from one of the other sectors (e.g. government or industry).
- Government:
  - Responsible for the safeguarding of citizens.
  - Responsible for provision of the legal framework for safeguarding of citizens.
  - Responsible for the provision of the legal framework that regulates the deployment of applications and deployment of technology.
  - Use of RFID in passports and ID cards.
- Industry and government organisations (when acting as system operators) - those who operate RFID applications and services:
  - Different industries deploy the RFID technology to provide a range of benefits to the industry, examples include the following:
    - Supply chain: Use of RFID to manage the transfer of goods from factory to retail outlet.
    - Tourism: Use of RFID for ticketing and for object hyperlinking (where an item is tagged to act as a key or pointer to detail information from the internet, used in museums and at Points of Interest).
    - Travel: Use of RFID enabled ticketing (e.g. the Transport for London Oyster card).
    - Border control: Use of RFID enabled smartcards in passports.

6.5 Open and closed system applications

It is important to distinguish between open and closed systems and between systems built from open standards and those built using proprietary technologies. In addition it is important to recognise that many published standards allow for a wide set of options to be selected by the system designer. The result is that where a standard is published with options a claim of compliance to the standard does not guarantee interoperability of the resulting equipment as the implemented capabilities may be different. An illustration is given in clause B.1, which shows that both mandatory and optional commands exist in a single standard. The same degree of freedom of selection of features is also applied to memory size, memory locking capabilities, and antenna design.

In the RFID world there are also many proprietary RFID technologies covering encoding schemes, radio interfaces and connection of interrogators to back end systems. It is recognised that proprietary technologies, in terms of both the installed base and new applications, will have a diminishing share of the market. Nevertheless the ability to introduce new proprietary features in standard products represents a particular challenge in the context of the present document.

The current framework and level of regulation of the RFID market does suggest that proprietary RFID technologies will continue to be developed.

6.6 RFID and IoT

The text in this clause is only a brief summary on the IoT and RFID. More detailed information is available from http://www.rfidglobal.eu/.

The Internet of Things (IoT) has been described as an open architecture for sensor based network platforms that integrate with business platforms. An RFID tag is not a sensor but may be integrated with a sensor, with the sensor and other integrated electronics updating the RFID tag contents. Such examples will mostly deploy active or battery assisted read-write tags as the tag data is intended to be a system variable. In such cases the link between Device and Tag becomes active in the RFID ecosystem.

The concept of the IoT, as determined within the IoT European Research Cluster (IERC) is embraced within the following definition:

DEFINITION: The Internet of Things is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. In the IoT, "things" are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information "sensed" about the environment, while reacting autonomously to the "real/physical world" events and influencing it by running processes that trigger actions and create services with or without direct human intervention. Interfaces in the form of services facilitate interactions with these "smart things" over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.

It is noted that the IoT explicitly excludes people and the role of people in networking. A consumer concern that thus arises is that the definition of personal data includes the association of objects to people as a means to indirectly identify a person and the explicit exclusion fails to address the requirements of data protection and privacy regulation.

7 Analysis in support of recommendations

NOTE: This clause summarizes the analysis of privacy and data protection in the context of RFID ecosystems from the perspective of OECD Guidelines for personal data protection [i.17] and the EC Data Privacy directives [i.16], and [i.52]. The security risk analysis is summarized in Annex C.

7.1 RFID system architecture

Implementation of the RFID ecosystem may take many forms including the following scenarios:

- Scenario 1: all key elements (tagged items, tags, interrogators, network connections and back end systems) are under the management of a single entity.
- Scenario 2: Interrogators and back end system under the management of a single entity.
- Scenario 3: All elements under the management of discrete entities.

For the purposes of this report the degree of standardisation is also considered:

- Air Interface (AI) standardised.
- AI not standardised (proprietary).
- Data model compliant to international standard.
- Data model proprietary.

- Other interfaces standardised.
- Other interfaces not standardised (proprietary).

The degree of interoperability and interconnectivity between system components is considered further in this report.

7.2 RFID system and privacy

Many of the privacy concerns raised by consumers regarding the use and deployment of RFID technology surround the uncertainty of the system design, its operation and its intent. First of these is uncertainty with respect to the presence of tags or interrogators. Making the presence of both tags and interrogators visible has been suggested as likely to defuse immediate concerns on the basis that visibility allows action to be taken (it being difficult to take action against an invisible force). It is noted that in many cases visibility is not readily possible.

The actions undertaken in the present document to catalogue requirements for emblems, and for signs, are intended to address some of the user concerns related to visibility of the RFID technology, and have been written in a manner to allow their direct use in future standardisation.

A second privacy concern is that of the system's capability to track individuals. This is more difficult to address as even when visibility is addressed it is in general not clear if all interrogators can read all tags and if the data is seen or can be correlated to be seen by a single group.

The ability to provide protection against tracking requires the system to support the functional capability of "unlinkability". Whilst unlinkability can be achieved by the bearer of the tag (provided he knows that he carries a tag and how to shield it) such shielding may invalidate the primary purpose of the tagged item (i.e. it is not practical to hide a watch in an opaque shielded envelope) and as an addition to the system may not be relied on to be active and thus giving protection. Unlinkability has to be deployed in the back end system and in the interconnection networks, or more fully in any device in the RFID ecosystem able to identify multiple tags and/or to correlate the presence of tags to individuals. Provision of such measures is not likely to be immediately visible to the general public and thus would have to be made visible through assurance marking of some sort.

A related privacy concern is the range at which tags can be identified on a person, or on articles held by a person where typical interrogation ranges are shown in Table 3.

Table 3: RFID Frequencies, Typical uses, and Typical Read Range

Frequency	Type	Typical application	Typical read range
125 KHz to 135 KHz	Passive	Animal tracking (ISO 11784 [i.34] and ISO 11785 [i.35]), Production control, Manufacturing Automation· Access control, parking lots, garages· Automotive: car access, antitheft Industrial machinery and tooling Transport, chemicals handling, dangerous goods processing Waste management Semiconductor chip processing, packaging, manufacturing flow	Up to 1 m Typically 2 cm to 30 cm
13,56 MHz Medium range	Passive	ISO/IEC 15693 [i.6] Library management hands free access control (Ski resort) Logistics (ISO 18000-3 [i.9]) - Item tagging	Up to 60 cm
13,56 MHz Short range	Passive	ISO/IEC 14443 [i.5] passports, ID cards, payment cards access control, ticketing (Near Field Communication (NFC) is battery powered, active)	typically 2 cm to 5 cm

Frequency	Type	Typical application	Typical read range
433 MHz	Active	Cargo handling Container locations Real Time Location Systems Asset tracking	Up to 100 m
860 MHz to 960 MHz	Passive	Logistics chain, Pallet ID etc. Item tagging Integrated RFID and EAS applications Manufacturing process control and product tracking Cargo handling Airline baggage Location systems Asset tracking	Up to 4 m
2 446 MHz to 2 454 MHz	Passive and battery assisted	Chip processing, Automotive manufacturing Toll identification Proximity sensors Location tracking Asset tracking	Up to 10 m
NOTE 1: The use of the term read range as used in the industry and associated press assumes that the antennas for tag activation and for receiving the tags' return signal are at the same physical location, often using the same antenna. NOTE 2: The range at which an interrogator can activate a tag and receive the tag response is often described as the read range. In practice an activated tag can be detected and the data it is transmitting read over a longer range, if using a tuned receiver with sufficient sensitivity to receive the signal (see eavesdropping) and an appropriate decoder.			

7.2.1 Modelling the role of RFID in privacy

The analysis of RFID with respect to privacy requires rigorously considering the manner in which any data, collected or collectable, can be utilised to identify individuals, their behaviour and possessions. Privacy is most often concerned with the controlled release of information relating to a person by that person, or by permission of release of that data through a third party. It is essential therefore to look at how tagged items in the RFID world are associated to the person and how observations of the tag impact the privacy of the person holding the tag or associated with it.

The following assumptions have been made as input to the analysis:

- The association of tag to tagged item is managed by the tagged item value chain.
- The tag value chain is different to the associated tagged item value chain.
- The association of tag to tagged item modifies the value chain of the tagged item.

EXAMPLE 1: Adding an RFID tag may add value to the tagged item by allowing additional purposes to be applied to the item, for example allowing degradable goods to be monitored in the home environment after exiting the retail chain.

- The tagged item and tag costs are independent.
- A tag acts as an identifier by association to a tagged item.;
- The tagged item may be identified in other ways so the tag identifier is not uniquely associated to the tagged item identity.

EXAMPLE 2: A jacket may be tagged and identified remotely by its tag but is also identified visually by its cut, material and other non-tagged attributes.

The existing privacy regulation (the right of the individual to have his identity and agency protected from any unwanted scrutiny and interference) tends to view static data whereas it is common practice to examine behavioural data to make assertions about the behaviour of individuals or groups. This is consistent with the definition of personal data in the data protection directive [i.52] and is shown for the purpose of further analysis as a concept relationship diagram in Figure 2. In this case there is a clear link between behaviour and the person.

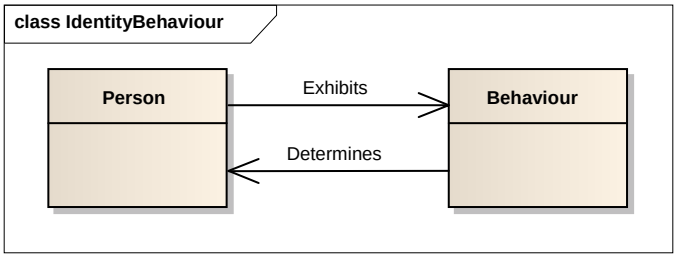


Figure 2: Very simplified concept relationship diagram of identity

The simplified concept relationship diagram can then be expanded on each side, shown in Figure 3 for behaviour. In this view three new items are introduced: Action; Time and Location. In the RFID context actions may be interpreted by the BES and the time and location may be determined by the read action of the interrogator itself.

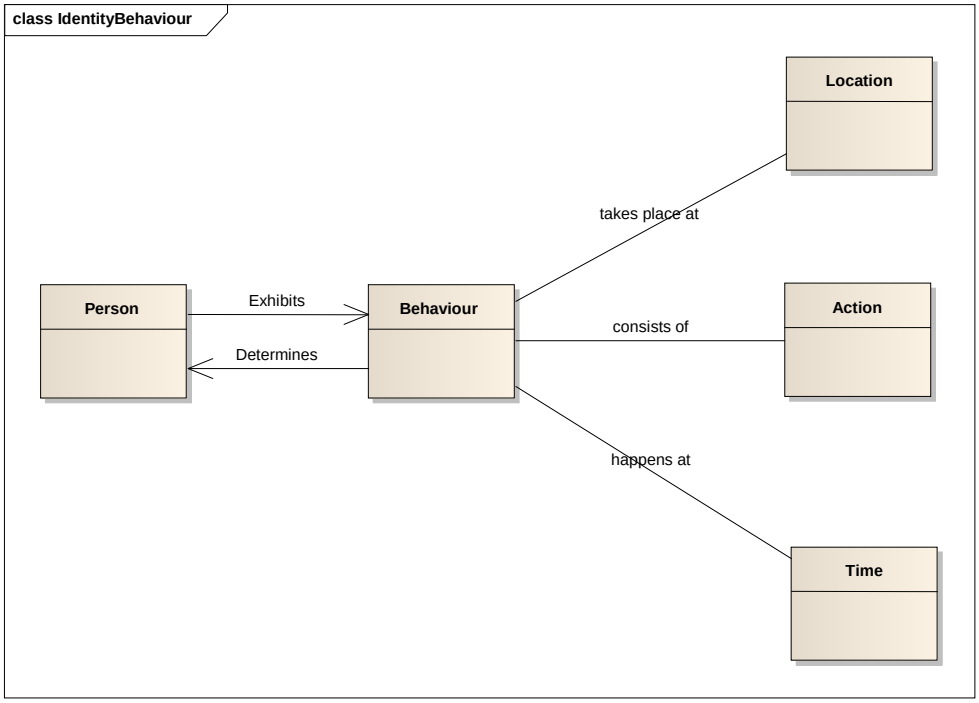


Figure 3: Expansion of simple concept relationship diagram with respect to behaviour

Extending this further with consideration of how RFID tagged items are used and how they influence the privacy domain is shown in Figure 4. In the model the person is assumed to control release of personal data. What the model attempts to show is that observations of the data on a tag, which may or not be explicit personal data, allows circumstantial data to be built up that may be sufficient to determine the person without having to observe the explicit personal data.

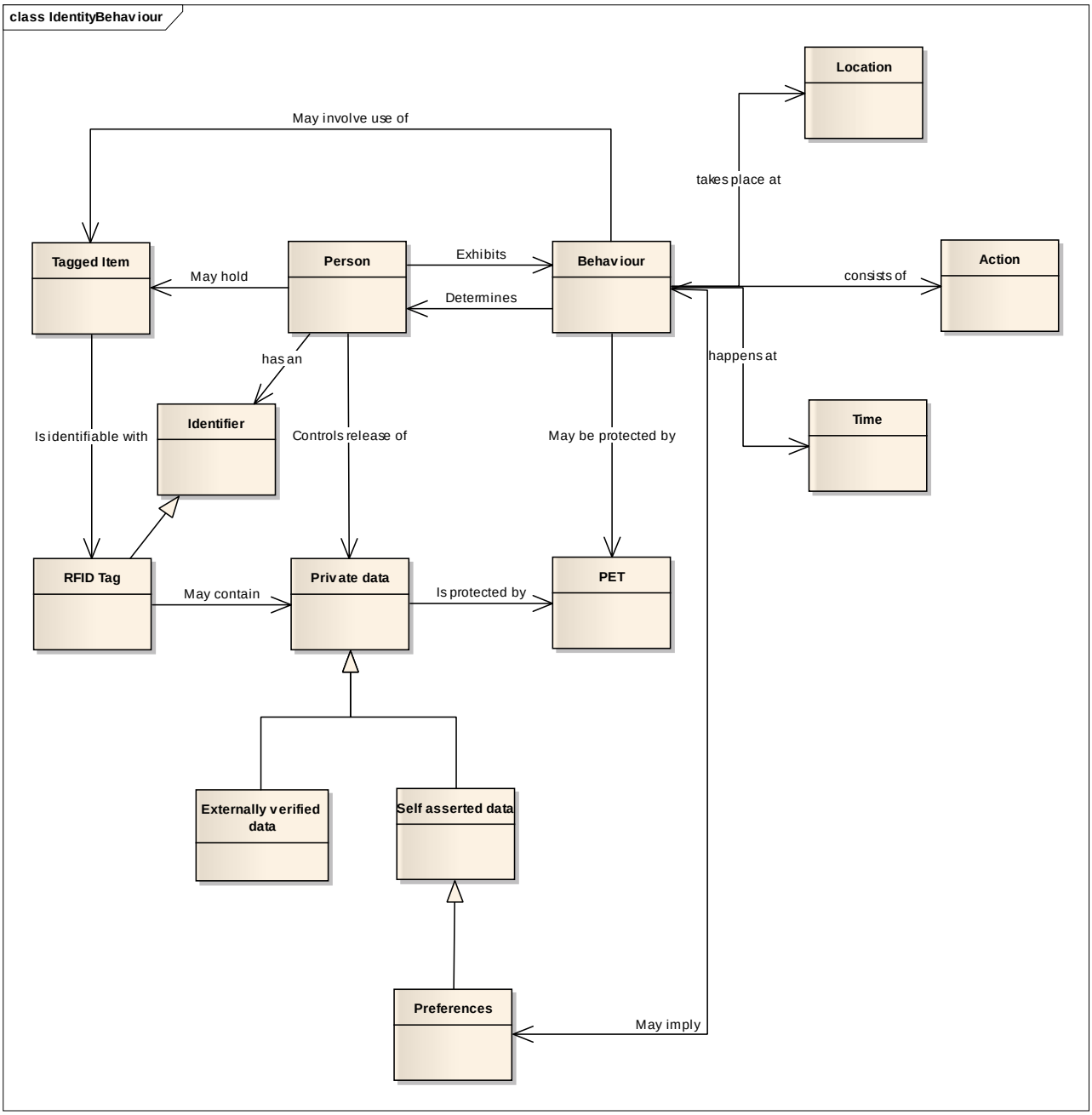


Figure 4: Concept relationship diagram for privacy in RFID

In an RFID system each time a tag is a read the content of the tag is made available and the data recovered may then be extended by assertions made by the interrogator (e.g. time of day that the read operation occurred, location of the interrogator at the time of the read operation). For the purposes of assuring privacy these asserted claims have to be protected in like manner to the static data of the user holding the tagged item. Assertions of user preferences may also be made by the back end systems thus establishing a link between behaviour and individuals.

NOTE 1: For security purposes the links between recovered data and asserted data has to give the same assurance of security to each, and to their combination.

NOTE 2: The interrogator provides data to the back end system and it is trusted to have received that data from a tag. As the tag has been read the audit trail needs the back end system to record the time of reading and the data recorded as well and to mark if the data has been processed.

The consequence of this model is that privacy protection has to be offered not just to the explicit personal data but also to the processes that make such data open by interpretation of behaviour. The Privacy Enhancing Technology should not be applied only to the data on the tag but to the static data held on the system, observations of behaviour in the system and any release of post processed data. The control of release of personal data by the affected party is crucial to system support of privacy and needs to allow for informed consent.

7.3 Principles for handling personal data in RFID systems

The OECD Guidelines for personal data protection [i.17] and the EC Data Privacy directives [i.16], and [i.52] introduce a number of basic principles to be implemented by RFID operators when personal data are involved. These principles are summarised in Table 4.

Table 4: Generic principles arising from an analysis of OECD guidelines and EC Data Protection and Privacy directives.

Root principle	Subsidiary principle	Impact on RFID
Collection limitation	Limits to data collection	Before collecting personal data - for example, when contracting with the data subject - an RFID operator should obtain the prior and unambiguous consent of the data subject **or** inform him/her of the collection of personal data and the indicated purposes of use according to domestic regulations (see note).
		From the viewpoint of the RFID operator, consent is always required when personal data is used in commercial services. However, in cases of safety and public services, prior explicit consent may not be required although implicit consent is likely to have been given as part of the user's contractual agreement with the service provider (see note).
	Data collection methods	An RFID operator should not acquire personal data by fraudulent or other dishonest means.
	Data collection without consent	The limits to data collection do not apply to cases in which the handling of personal data is restricted by national regulation.
	Exclusion of data capable of identifying an individual from collected data	An RFID operator should take reasonable measures to avoid collecting data from which an individual could be identified by referring to a database in cases where such a possibility exists.
	Confirmation of a data subject's consent about data collection	An RFID operator should take suitable measures to confirm the consent of a data subject about data collection (see note).

Root principle	Subsidiary principle	Impact on RFID
Collection limitation	Limits to data collection	Before collecting personal data - for example, when contracting with the data subject - an RFID operator should obtain the prior and unambiguous consent of the data subject **or** inform him/her of the collection of personal data and the indicated purposes of use according to domestic regulations (see note).
		From the viewpoint of the RFID operator, consent is always required when personal data is used in commercial services. However, in cases of safety and public services, prior explicit consent may not be required although implicit consent is likely to have been given as part of the user's contractual agreement with the service provider (see note).
	Data collection methods	An RFID operator should not acquire personal data by fraudulent or other dishonest means.
	Data collection without consent	The limits to data collection do not apply to cases in which the handling of personal data is restricted by national regulation.
	Exclusion of data capable of identifying an individual from collected data	An RFID operator should take reasonable measures to avoid collecting data from which an individual could be identified by referring to a database in cases where such a possibility exists.
	Confirmation of a data subject's consent about data collection	An RFID operator should take suitable measures to confirm the consent of a data subject about data collection (see note).
Data quality		An RFID operator should endeavour to keep personal data accurate and up to date within the scope necessary for the achievement of the purposes of use.
Purpose specification	Specification of the purposes of use	When handling personal data, the RFID operator should specify the purposes of use of personal data.
	Limits on changing the purposes of use	An RFID operator should not change the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes.
	Change of the purposes of use required prior consent	Before an RFID operator changes the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes, it should inform a data subject of the change or obtain prior and unambiguous consent (see note).
Use limitation	Use limitation	An RFID operator should not handle personal data, without obtaining the prior consent of the data subject, beyond the scope necessary for the achievement of the specified purposes of use (see note).
	Restriction of disclosure to third parties	An RFID operator should not provide personal data to a third party without obtaining the prior consent of the data subject (see note).

Root principle	Subsidiary principle	Impact on RFID
Collection limitation	Limits to data collection	Before collecting personal data - for example, when contracting with the data subject - an RFID operator should obtain the prior and unambiguous consent of the data subject **or** inform him/her of the collection of personal data and the indicated purposes of use according to domestic regulations (see note).
		From the viewpoint of the RFID operator, consent is always required when personal data is used in commercial services. However, in cases of safety and public services, prior explicit consent may not be required although implicit consent is likely to have been given as part of the user's contractual agreement with the service provider (see note).
	Data collection methods	An RFID operator should not acquire personal data by fraudulent or other dishonest means.
	Data collection without consent	The limits to data collection do not apply to cases in which the handling of personal data is restricted by national regulation.
	Exclusion of data capable of identifying an individual from collected data	An RFID operator should take reasonable measures to avoid collecting data from which an individual could be identified by referring to a database in cases where such a possibility exists.
	Confirmation of a data subject's consent about data collection	An RFID operator should take suitable measures to confirm the consent of a data subject about data collection (see note).
	Use without consent	The provisions of the preceding two paragraphs do not apply to cases in which the handling of personal data is based on domestic laws. The RFID operator should grant access only to law enforcement authorities as authorized by a domestic court order or equivalent legal instrument.
Security safeguards		Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
Openness		There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data collector.

Root principle	Subsidiary principle	Impact on RFID
Collection limitation	Limits to data collection	Before collecting personal data - for example, when contracting with the data subject - an RFID operator should obtain the prior and unambiguous consent of the data subject **or** inform him/her of the collection of personal data and the indicated purposes of use according to domestic regulations (see note).
		From the viewpoint of the RFID operator, consent is always required when personal data is used in commercial services. However, in cases of safety and public services, prior explicit consent may not be required although implicit consent is likely to have been given as part of the user's contractual agreement with the service provider (see note).
	Data collection methods	An RFID operator should not acquire personal data by fraudulent or other dishonest means.
	Data collection without consent	The limits to data collection do not apply to cases in which the handling of personal data is restricted by national regulation.
	Exclusion of data capable of identifying an individual from collected data	An RFID operator should take reasonable measures to avoid collecting data from which an individual could be identified by referring to a database in cases where such a possibility exists.
	Confirmation of a data subject's consent about data collection	An RFID operator should take suitable measures to confirm the consent of a data subject about data collection (see note).
Individual participation		An individual may have the right to: a) obtain from an RFID operator, or otherwise, confirmation of whether or not the operator of the RFID system has data relating to him; b) have communicated to him, data relating to him; (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; c) be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
Accountability		An RFID operator should be accountable for complying with measures which give effect to the principles stated above.
Equality of regime		An RFID operator should not transfer personal data across borders unless the destination has at least the same privacy regime as the origin.

Root principle	Subsidiary principle	Impact on RFID
Collection limitation	Limits to data collection	Before collecting personal data - for example, when contracting with the data subject - an RFID operator should obtain the prior and unambiguous consent of the data subject **or** inform him/her of the collection of personal data and the indicated purposes of use according to domestic regulations (see note).
		From the viewpoint of the RFID operator, consent is always required when personal data is used in commercial services. However, in cases of safety and public services, prior explicit consent may not be required although implicit consent is likely to have been given as part of the user's contractual agreement with the service provider (see note).
	Data collection methods	An RFID operator should not acquire personal data by fraudulent or other dishonest means.
	Data collection without consent	The limits to data collection do not apply to cases in which the handling of personal data is restricted by national regulation.
	Exclusion of data capable of identifying an individual from collected data	An RFID operator should take reasonable measures to avoid collecting data from which an individual could be identified by referring to a database in cases where such a possibility exists.
	Confirmation of a data subject's consent about data collection	An RFID operator should take suitable measures to confirm the consent of a data subject about data collection (see note).
Anonymity		An RFID operator should provide the means for users to transact anonymously.
NOTE: The authorisation framework to support consent does not need to be technical but may be procedural and may be both explicit (e.g. by acknowledgement of data transfer) and implicit (e.g. by means of signs and logos).		

Root and subsidiary principles are treated as objectives for the purpose of the present document and the comments in the "impact on RFID" column are treated as functional or operational requirements in RFID systems.

7.4 Role of Privacy Enhancing Technologies (PETs)

Privacy Enhancing Technologies (PETs) are those security technologies and processes that when deployed protect the privacy of persons. As already identified in deliverables from ETSI on Identity Management (e.g. TR 187 010 [i.7]) the Common Criteria defined in ISO/IEC 15408−2 [i.21] identify 4 key attributes that relate to privacy.

- Anonymity.
- Pseudonymity.
- Un-Linkability.
- Un-Observability.

Of these measures as PETs the primary aims in RFID are to support Pseudonymity and Un-Linkability. However the consent element of control of personal data also requires that the authorisation framework for access to data, including the initialisation of authority, transfer of authority and deletion of authority, has to be given consideration.

NOTE: The authorisation framework to support consent does not need to be technical but may be procedural and may be both explicit (e.g. by acknowledgement of data transfer) and implicit (e.g. by means of signs and logos).

Whilst the "Design for Assurance" and "Privacy by Design" approaches in standardisation tend to concentrate on technical means to provide security and privacy it should be noted that procedural means are also considered. The role of the Privacy Impact Assessment in this is considered in more detail later in the present document.

8 Data Protection, Privacy and Security Objectives and Requirements

NOTE: Each proposed implementation requires that a risk analysis is carried out to ensure that the risks are properly identified and any countermeasure to be applied is proportionate to the risk. A report on tests that investigated the risks associated with the illicit reading and eavesdropping of tags is provided in TR 101 543 [i.32].

8.1 Distinguishing objectives and requirements

As identified in TR 187 011 [i.25] there is distinction to be made between objectives and requirements and this distinction has been followed in the analysis presented in the present document:

- An objective is the expression of what a {security} system should be able to do in very broad terms whereas a requirement is a more detailed specification of how an objective is achieved. Objectives may be considered to be desires rather than mandates. {Security} requirements are derived from the {security} objectives and, in order to make this process simpler, requirements can be further subdivided into functional requirements and detailed requirements.

- Functional {security} requirements identify the major functions to be used to realize the {security} objectives. They are specified at a level which gives an indication of the broad behaviour expected of the asset, generally from the user's perspective.

- Detailed {security} requirements, as their name implies, specify a much lower-level of behaviour which would, for example, be measurable at a communications interface. Each functional requirement is realized by a number of implementation requirements.

8.2 Data protection and privacy objectives

Table 4 identifies the core objectives arising from the OECD guidelines [i.17] and EC Data Protection and Privacy directives which are re-stated in Table 5 as labelled objectives for RFID. The rationale for each of the objectives is defined in Table 4.

NOTE: The requirements stated in Table 5 are summarised from the OECD guidelines and the Data Protection regulations described in clause 7.3 and do not constitute a specification or standard but are intended as input to the future standardisation process.

Table 5: Data protection and privacy objectives statement for RFID

Ref.	Objective	Comments
DPP0-1	Privacy by design	Privacy and security friendly technologies are to be designed to ensure that applications respect the fundamental right to privacy and the data protection legislation.
DPPO-2	Accountability principle	The data controller is accountable for complying with measures which give effect to the DPP principles. The data controller is ultimately responsible for the personal data gathered through the application in question. RFID privacy compliant standards should ensure that data controllers processing personal data through RFID technology have the necessary tools to implement the requirements contained in the data protection Directive.
DPPO-3	Data Collection limitation: Information and transparency on RFID use	Operators should develop and publish concise, accurate and easy to understand information for each of their applications.
DPPO-4	Data collection limitation: Consent through signs	RFID operators should take steps to inform individuals of the presence of interrogators on the basis of a common European sign to be developed.
DPPO-5	Data collection limitation: Consent.	Before collecting personal data - for example, when contracting with the data subject -an RFID operator should obtain the prior and unambiguous consent of the data subject **or** inform him/her of the collection of personal data and the indicated purposes of use according to appropriate national and regional regulations.
DPPO-6	Data collection limitation: Data collection methods	Data collection methods. An operator should not acquire personal data by fraudulent or other dishonest means. Data collection without prior consent may be argued to be dishonest.
DPPO-7	Data collection limitation: principle of purpose limitation	As established in DPPO-3, when handling personal data, a RFID operator should specify the purposes of use of personal data.
DPPO-8 (note 1)	Right of access, rectification, deletion to personal data including tag content	RFID tags containing personal data: data subjects, using means easily accessible, should be entitled to know the information contained in the tag and in the back-end system together with any processing related to that information.
DPPO-9 (notes 2,3 and 4)	Right of deletion: Tags disablers (right to 'silence of the chips')	Individuals should be able to disconnect from their networked environment at any time.
DPPO-10	Data quality principle to be applied	This requires personal data to be relevant and not excessive for the purposes for which they are collected. Thus, any irrelevant data should not be collected and if it has been collected it cannot be retained.
DPPO-11	Anonymisation and minimization	RFID operators should minimize the processing of personal data using anonymous or pseudonymous data where possible.
DPPO-12	Security safeguards	Personal data, including unique identifiers, should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

NOTE 1: Some applications (e.g. RFID enabled passports) will not grant the holder the right to discard, disable or remove a tag.

NOTE 2: Tag deactivation is equivalent to tag content deletion as per Article 12 b of the Data Protection Directive. Examples of tag content deletion include: permanent deactivation, temporary deactivation, overwriting of the data, physical shielding, removal of the tag from its associated object etc.

NOTE 3: Tag content rectification (Article 12 b data protection Directive): to embed a feature into the tag that will erase or scramble the item serial number and let only the item class type description completely or partially available (the contrary is also possible but with different privacy implications).

NOTE 4: (DPPO-9) In some RFID applications, when the individual exercises his/her rights under Article 14 a and the subsequent right to disable the tag, both manufacturers and deployers of RFID technology should ensure that such operation of disabling the tag is easy to carry out. In other words, for the data subject the task of disabling the tag should be easy although this may cause conflict with the use of RFID tags for EAS.

8.3 Statement of objectives for Security

Table 6 outlines the security objectives statements for RFID and their derived security functional requirements. The result from the security risk analysis (Annex C) was used as input to the security objectives identification, which was refined into security functional requirements using the guidelines in TR 187 011 [i.25].

NOTE 1: TR 187 011 [i.25] provides guidelines on how to apply ISO-15408-2 [i.21] (Common Criteria) requirements to ETSI standards.

NOTE 2: The threat analysis described in Annex C covers all general threats and specific threats may not apply in specific applications of RFID.

Table 6: Security objectives statements and security functional requirements for RFID

SO No.	Security Objective	Sec. Functional Requirements
SO-1	Data that can directly or indirectly identify an individual recorded on or by RFID tags should not be revealed to any party not authorised to receive the information.	Access control; Identification of parties; Authentication of parties; Data confidentiality
SO-2	Data that can directly or indirectly identify an individual recorded on or by RFID tags should be visible by the use of legitimate means only.	Access control; Identification of parties; Authentication of parties
SO-3	Data that can directly or indirectly identify an individual sent to or from any component in the RFID ecosystem should not be revealed to any party not authorised to receive the information.	Access control; Identification of parties; Authentication of parties; Data confidentiality
SO-4	Data that can directly or indirectly identify an individual held within one or more components of the RFID ecosystem (see Figure 1, clause 6.1) should be protected from non-legitimate access from within the RFID ecosystem.	Access control; Identification of parties; Authentication of parties
SO-5	Data that can directly or indirectly identify an individual held within one or more components of the RFID ecosystem (see Figure 1, clause 6.1) should be protected from non-legitimate access from outside of the RFID ecosystem.	Access control; Identification of parties; Authentication of parties
SO-6	Data that can directly or indirectly identify an individual held within one or more components of the RFID ecosystem (see Figure 1, clause 6.1) should be protected from unauthorised modification.	Integrity control; Access control
SO-7	Data that can directly or indirectly identify an individual held within one or more components of the RFID ecosystem (see Figure 1, clause 6.1) should be protected from unauthorised deletion/removal.	Integrity control; Access control; Resilience
SO-9	Access to, and the operation of, components of the RFID ecosystem (see Figure 1, clause 6.1) by legitimate users should not be prevented by malicious activity within the RFID ecosystem.	Resilience; System integrity; Identification; Authentication (prevention of masquerade)
SO-10	Access to, and the operation of, components of the RFID ecosystem (see Figure 1, clause 6.1) by authorised users should not be prevented by malicious activity from outside of the RFID ecosystem.	Resilience; System integrity; Identification; Authentication (prevention of masquerade)
SO-11	The identity of an user should not be compromised by any action of the system.	Restriction of functionality of the system; System integrity
SO-12	No action of the system should make a user liable to be the target of identity theft.	Restriction of functionality of the system; System integrity; Resilience

NOTE 3: Repudiation is not considered in Table 6 as repudiation requires user determination and control to invoke, and this is considered as unreasonable in the RFID systems examined in the present document.

9 Privacy and Data Protection Impact Assessment (PIA) outline

NOTE: The European Commission Recommendation of 12 May 2009 [i.10] on the implementation of privacy and data protection principles in applications supported by radio-frequency identification assigned the task of developing a framework for privacy and data protection impact assessments to the industry. The industry undertook the task in collaboration with relevant civil society stakeholders. A final version of the industry PIA framework was submitted to the Article 29 Data Protection Working Party [i.23] at the beginning of December 2010. It is anticipated that the Commission will publish the PIA framework in the first quarter of 2011.

The original Mandate M/436 issued by the European Commission, backed by the Member States, to the European Standards Organizations (ESOs) to deliver a co-ordinated response on the subject of Radio Frequency Identification Devices (RFID) in relation to data protection, information security and privacy has been amended. Consequently, with regard to the Privacy and data protection Impact Assessment (henceforth PIA), the work reflected in the present document has consisted of defining the general requirements for a PIA. On the basis of the requirements thus defined, the present document presents a gap analysis identifying related standardization needs not yet addressed.

Upon publication of the PIA framework for RFID by the European Commission it will be necessary to review the contents of this clause to ensure that there are no conflicts between the 2 documents.

9.1 State of the art and standardization gaps

The need for systematic analysis of privacy and data protection impacts has been brought about by several developments including digitization and the development of the information society; the central role and increased use of personal data for defining and delivering digital products and services; changes in the data protection legislation; the international character of digitally-mediated transactions; and consumer/citizen issues.

The beginnings of impact assessments focusing specifically on privacy can be traced back to the 1990s. New Zealand, Australia, Canada and the USA are amongst those countries which pioneered the concept of PIA.

The importance of assessing the impact on privacy and data protection of various initiatives, whether private or public, has permeated through the European Union. The European Commission, the European Data Protection Supervisor and Article 29 Data Protection Working Party [i.23] recommend that PIAs be performed at the design stage of any project involving the processing of personal data, and link it to the privacy by design principle. The United Kingdom and Germany are examples of Member States with an active policy in this field. Both countries have formulated and are now able to provide detailed guidance for performing PIAs, ranging from generic frameworks to more detailed guidance (e.g. sector- or domain-specific).

However, despite the recommendations and initiatives mentioned above, there is no EU-broad harmonized or standardized approach to privacy and data protection impact assessments. Moreover, there is no agreed methodology for performing - PIA - methodologies currently in use being based upon, or borrowing from environmental, social, policy or security assessment methodologies.

From a content point of view, and despite their name, most PIAs have a narrow focus, namely data protection rather than privacy protection. The result is that many PIAs are restricted to legal compliance checks and do not include societal aspects. That is reflected in the form of some PIAs which are limited to checklists. Increasingly, however, PIA methodologies include narrative descriptions of the systems assessed and the environments in which they will operate, which helps to understand better the potential privacy and data protection risks.

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

From the point of view of the domain of the PIA, most guidance available is of a generic nature. However certain technologies and applications might require specifically defined PIAs. Increasingly, such specific assessment methodologies are being defined, as is the case of RFID, biometrics, the financial and medical sectors, etc.

Internationally, the most notable standardization activities in the field of privacy are carried out by ISO. Initiatives include a privacy framework which was proposed as a work item in 2006. Work is still underway and is expected to be finalized in 2011. Other relevant ISO initiatives include a proposal for a privacy capability maturity model; the published standard for a privacy impact assessment for financial services; and the consumer privacy-protection protocol for mobile RFID services.

All of the above highlight standardization gaps in this area, ranging from standard methodological approaches to domain-and application-specific PIAs. For RFID, these needs will be addressed after the industry PIA will have been finalized and during the second phase of Mandate 436 [i.1]. Standardization gaps identified thus far include:

- Standard RFID-specific PIA methodologies, built around the functional capabilities and physical characteristics of the major RFID standards that specify air interface protocols.
- Standard RFID-specific PIA methodologies built around the RFID system architecture.
- Domain and sector-specific PIA methodologies, templates and guidance

NOTE: There is scope for standardisation to reduce the costs of the PIA processes .The impact of potential cost savings and more effective processes in PIA work arising from privacy-by-design standards, PIA formats and processes standards and even standard PIAs for SMEs should be examined.

The following clauses will provide the foundation for this future work plan by outlining the main requirements the (RFID) PIA will have to fulfil. The requirements have been defined based on a study of existing PIA methodologies, and relevant good practices, and should be read in conjunction with clause 8.1, Personal Data and Privacy Protection Objectives.

9.2 Role of the PIA

Privacy is defined, for the purposes of the present document, as the right of the individual to have his identity, agency and action protected from any unwanted scrutiny and interference. It reinforces the individual's right to decisional autonomy and self-determination.

The RFID Privacy and Data Protection Impact Assessment (henceforth PIA) is the thorough and systematic assessment of privacy (and security) risks posed to individuals by RFID-enabled systems and the means to mitigate these risks. The PIA examines all relevant technological, organizational and regulatory risks. A PIA should be conducted prior to implementing new RFID systems and subsequently prior to any changes in existing RFID systems or in the environment in which they are used.

The intent of the PIA is to identify, in a timely manner, risks posed to the individual's privacy by the system in which RFID is deployed and from which services are offered; and to identify and devise appropriate solutions either by process or in the design and deployment of the technology in order to minimize privacy risks. Subsequent PIAs are to be performed after an RFID system has become operational, at regular intervals, and throughout its entire lifecycle. The main purpose of the subsequent PIAs is to identify any new threats and risks, and ways to mitigate them.

NOTE 1: It is a consequence of the volatility of technology and environmental change that the PIA is seen as a management process in like manner to the management of quality or security in an organisation for which process standards exist in ISO 9000 [i.37] (Quality) and ISO/IEC 27000 [i.18] (Security).

A PIA should be performed for all types of RFID systems processing data, which can be used to identify individuals directly or indirectly.

The PIA should be conducted for RFID systems in both the public and the private sectors and should be an integral part of the design methodology for such systems and should be applied on any change to the system or its environment.

RFID systems not processing information that can be used to identify individuals directly or indirectly will not require a PIA.

NOTE 2: It is always necessary to conduct a prior assessment (sometimes called a threshold assessment) to be able to determine accurately if the system is processing information that can be used to identify individuals directly or indirectly. The key issue is whether items that are tagged are intended to be in the possession of individuals.

EXAMPLE: Pure inventory control applications will not require a PIA.

The PIA includes but is not limited to a security risk assessment. Moreover, the PIA challenges current security paradigms, such as the perimeter defence model, in that it includes privacy risks arising from certain types of activities conducted by organizations such as legitimate insiders (e.g. through their use of profiling and behavioural targeting, or through their selling, sharing or renting of data pertaining to the individual with/to partner organizations and third parties). A number of premises for employing such a methodology for privacy and data protection risk analysis and risk management are described in the following paragraphs.

The RFID PIA takes a systemic approach in two respects. Firstly, it assesses all technological, organizational and regulatory risks relevant to a (proposed) RFID system. Secondly, given the highly networked communication systems and the fluidity of data, (proposed) RFID systems should be assessed in relation to other systems with which they will connect and with which they will interact.

Further premises of the RFID privacy and data protection impact assessment include:

- that RFID is to be understood as an enabling technology rather than a purpose in itself;
- that RFID systems should favour a user-centred design, whereby the requirements of citizens/consumers (including privacy and data protection requirements) are taken into consideration when designing RFID-enabled systems;
- that the use of RFID-enabled systems should not place any unnecessary or unwanted burden on the citizen/consumer;
- that the design of RFID systems should aim to strike an even balance between the interests of enterprise/government efficiency; product or application usability; user convenience, rights and trust;
- that privacy should be an integral part of the design of new RFID systems (privacy by design) rather than added at a later stage.

Performing a PIA cannot eliminate all privacy risks. A PIA should, however, help design privacy-preserving systems, for example by adopting the privacy-by-design paradigm.

NOTE 3: The privacy by design paradigm is not formally specified thus proof of conformance to the paradigm requires further standardisation. It is further noted that the paradigm is not specific to RFID but may contain specific extensions for RFID.

Although a PIA cannot eliminate all privacy risks, it should provide an analysis of residual risks (i.e. risks that cannot be mitigated by means of technical, organizational, etc. solutions). The analysis should then be used for consent processes.

It can be expected that performing a PIA will incur costs. The costs will vary depending on a variety of factors, such as the size of the organization, the complexity of the system assessed, and the need for external expertise. Furthermore, depending on the results of the PIA, additional investment might be required to finance the privacy-preserving solutions identified as necessary for the system.

9.3 Overview of RFID-related features with an impact on privacy

Certain current features of RFID technology and RFID-enabled applications pose risks to individual privacy and other fundamental rights, and to data protection. Among them:

- RFID has the potential to be a disruptive technology in that it changes the way in which individuals interact with each other and with their environment;

NOTE 1: Disruptive technologies may have both positive (i.e. life affirming) and negative connotations (i.e. degrading quality of life).

- the multitude of envisaged RFID-enabled applications and the vast range of domains in which they can be used could render RFID ubiquitous;

- RFID is a technology relatively unknown to the larger public;

NOTE 2: The 2005 pan-European survey on "RFID and Consumers - What European Consumers Think About Radio Frequency Identification and the Implications for Business" [i.12] indicated that individuals' awareness was low and perceptions were mixed. 82 % of the European citizens were not aware of RFID technology; of the 18 % aware of the technology, more than half were concerned about tracking via product purchases, targeting via direct marketing, use of data by unauthorized third parties and the possibility of distance reading of tags.

NOTE 3: More recent consumer surveys maintain the assertion that the technology of RFID is relatively unknown.

- the RFID technology and related applications enjoy various levels of maturity, resulting in fragmented understanding of related risks;
- RFID tags include unique identifiers which may make it possible to reference them back (directly or indirectly) to their owners (tracking);
- RFID can enable real-time tracking;
- RFID has the ability to operate unnoticeably, in a way that the ability of the individual to observe and be aware of the ongoing functionality of the device;
- RFID has the ability to operate without the knowledge and consent of the person carrying a tag;
- RFID tag data and reading have no interface for the individual; this renders them virtually invisible or inscrutable, thereby limiting the individual's scope of choice and consent;
- tags may become practically and virtually invisible through miniaturization, embedding (e.g. woven tags; subcutaneous or implanted tags) or just through their ubiquity;
- RFID tag lifetime usually exceeds its useful purpose or data protection legal prescriptions;
- The majority of RFID tags do not include standard privacy features (e.g. no standard encryption of data on tags, no standard authentication-based access to data, etc.).

NOTE 4: It is recognised in some applications that security features in the tag may be counter to the purpose to which RFID is put. In such cases assurance of privacy has to be determined across the entire system.

NOTE 5: Any statement in the preceding list taken in isolation may not apply to specific applications.

9.4 RFID PIA Framework

The following clauses define the methodological requirements for conducting a PIA. Subsequently, the privacy and data protection requirements are defined. The data protection requirements are derived from current data protection legislation. The privacy requirements are defined along the four dimensions of privacy and formulated to take into consideration citizen/consumer concerns.

9.5 PIA Methodology Requirements

As mentioned above, certain current features of RFID technology and RFID-enabled applications may pose risks to individual privacy and other fundamental rights, that extend beyond data or informational privacy (for example RFID used to monitor patients can have an impact on the bodily integrity of the patients; RFID used by parents to monitor the whereabouts of their children can infringe on children's spatial and temporal privacy; RFID used in the retail sector to track the behaviour of customers in time and space can have an impact on the customers' behavioural privacy). Therefore, in defining the PIA requirements the broader concept of privacy has been considered, including:

- data or informational privacy;
- spatial (location) and temporal privacy;
- bodily privacy; and
- behavioural privacy.

In addition, the contextual character of privacy has been taken into consideration, as well as consumer requirements insofar as documented. This approach has several merits over current practice for the following reasons:

- The current relevant regulatory framework is concerned primarily with the first dimension of privacy, namely data or informational privacy.

- The current privacy regulatory framework does not cover the broader impact that a disruptive technology such as RFID can have on the privacy and other fundamental rights of individuals.

NOTE: At the time of the preparation of the present document both the European data protection legislation and the OECD privacy principles are in the processes of being revised to reflect these and other developments.

- For the larger part, self-regulatory initiatives in the field of RFID privacy have focused on the retail sector. Privacy issues specific to the use of RFID in other sectors (e.g. medical sector, public sector, etc.) are not addressed systematically.

As mentioned in clause 9.1, Privacy is defined, for the purposes of the present document, as the right of the individual to have his identity and agency protected from any unwanted scrutiny and interference. It reinforces the individual's right to decisional autonomy and self-determination.

In order to conduct a PIA, an operational definition of privacy is required as well. Such a definition is not included in the current data protection legislation. Consequently, for the purpose of the present document, we are introducing the concept of reasonable expectation of privacy. In this context, the reasonable expectation of privacy is defined as the generally accepted and shared norms with regard to privacy. One drawback of the operational definition should be noted: using it in performing a PIA will imply a certain amount of discretion in discerning privacy risk.

Although the current document defines only the main general requirements for a RFID PIA, more specific requirements for certain domains or applications might be necessary. For example, the use of RFID in the health sector, for which additional privacy and data protection requirements might be necessary given the sensitivity of data processed and consumer perceptions. Or similarly, additional and more specific privacy and data protection requirements might be necessary for the use of RFID in the public sector given the type of data processed and limited choice a citizen has in adopting such applications (for instance RFID-enabled passports and other travel documents). This hypothesis will need to be tested in the standards gaps analysis.

The PIA methodology will include both generic requirements (such as the sequence of steps to be undertaken in performing a PIA process) and RFID-specific requirements (such as those derived from the technical features of RFID with an impact on privacy, or the context or domain in which RFID systems are employed).

9.5.1 Assets and the RFID PIA

Assets refer to the object being protected in a risk analysis. The main assets at risk in the context of RFID are the personal data and privacy of the individual. Loss of these assets can result in risk for secondary assets such as the reputation of the individual, (e.g. in the case of identity theft), the right to be left alone (e.g. via direct marketing), trust in organizations deploying RFID, financial assets, etc.

9.5.2 Scope of the PIA

The RFID PIA should incorporate both risk assessment and risk management:

- risk assessment: a scientific and technologically based process consisting of four steps, threat identification, threat characterisation, exposure assessment and risk characterisation;

- risk management: the process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and if need be, selecting appropriate prevention and control options.

9.5.3 General methodological requirements

As mentioned above, the RFID PIA will include a number of generic requirements related to the steps to be undertaken in performing a PIA process. Among them are:

- Determining the PIA domain, scope and subject.
- Determining and appointing the PIA roles. These roles could be defined according to a responsibility assignment matrix (RACI): responsible roles, accountable roles, consulted roles, informed roles.
- Identifying the required expertise to perform a PIA.
- Drawing up a PIA plan.
- Conducting the actual PIA. This will not be limited to a questionnaire, but will include necessarily a detailed narrative description of technological, organizational and regulatory environment in which the system assessed is to function; the flows of information.
- Determining and insofar as possible quantifying privacy risks and defining means to mitigate them (see Annex C on risk assessment for a summary of the forms of threat that may apply).
- Determining notification protocols in the event of a privacy breach.
- Determining redress protocols in the event of a privacy breach.
- Documenting the process in a PIA report.
- Incorporating the PIA outcomes in decision-making and at an operational level.
- Ensuring the periodicity of the PIA process (linked to the life cycle of the system assessed).
- Ensuring the integration of the PIA in internal audit processes.
- Achieving a level of independence for a PIA with a view to a PIA audit.
- Ensuring accountability to an independent supervisory body (e.g. the Data Protection Authority).
- Making the results of the PIA both internally and publicly available (whilst taking into consideration organization confidentiality requirements).

9.5.4 Data Protection and Privacy requirements of the RFID PIA

Three categories of privacy and requirements for data protection have been defined for the PIA based on:

- current data protection and privacy legal requirements (see also clause 5.7);
- broader concepts of privacy and consumer/citizen issues;
- and insofar as documented, new and emerging issues.

9.5.4.1 Data protection requirements

This clause addresses primarily general issues of data/information privacy; issues of compliance with European, national, regional, local and sector-specific legislation. The detailed analysis of RFID-specific data/information privacy is presented below.

NOTE: See also clause 7.3 for the analysis of RFID data protection requirements.

The data protection requirements include:

1) Purpose specification - referring to limiting the collection of (personal) data exclusively for implementing a specific purpose whereby the re-use for an incompatible purpose is not permitted.

2) Collection and use limitation/minimization - referring to the length of time during which the (personal) data are kept, which should not exceed the period of time necessary to fulfil the purpose for which it was collected.

3) Data quality - referring to the obligation to ensure that personal data is accurate and, where necessary, kept up to date; and referring to the obligation to take every reasonable step to ensure that data, which are inaccurate or incomplete having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

4) Transparency and openness - referring to the individual's right to know that a product contains a tag; that the tag may store personal data; when a tag is being read and why; that data relating directly or indirectly to an individual is being stored in a database.

5) Accountability - referring to the assignment of responsibility for compliance with overall privacy and data protection requirements; measurement and monitoring of the fulfilment of these responsibilities and potential compliance; and defining redress measures.

6) Rights of data subjects (i.e. individuals in their quality of citizens or/and consumers) right to information, correction, removal and availability of contact information. Additional attention should be paid to issues of:

   a) Citizen/consumer awareness surveys indicate that only a modest percentage of the population is aware of the technology.

   b) Citizen/consumer consent - the extent to which consent is informed, meaningful, explicit and unambiguous.

   c) Citizen/consumer behaviour concerned with the privacy paradox, i.e. the disjunction between opinions held regarding privacy and actual behaviour (e.g. the trade-off between privacy and convenience).

   d) Protection of minors and other vulnerable groups - currently not specifically addressed by the data protection legislation although covered by other legislation not specifically covered under the scope of mandate M/436.

7) Security safeguards - referring to the appropriate measures to be taken by RFID service providers to safeguard the security of their systems (prevent unauthorized access to data, secure use and disposal, security awareness and training, etc.).

8) Third party transfer/processing - referring to the sharing and disclosure of information/personal data with/to third parties if necessary to fulfil the purpose(s) identified above.

9) Third country transfer - referring to restrictions or additional measures to be taken when transferring (personal) data outside the EU where (comparable) privacy standards and safeguards might not be available.

9.5.4.2 Data protection requirements

This clause addresses broader privacy requirements, which cover issues related to citizen/consumer awareness and behavioural issues; the contextual character of privacy in its several meanings; as well as issues related to other dimensions of privacy beside data privacy, namely: spatial, temporal, bodily and behavioural privacy.

The detailed analysis of RFID-specific data/information privacy is presented in Table 5.

1) Spatial (or location) and temporal privacy referring to the location of an individual at a discrete point in time and over a continuous period of time.

2) A subset of the temporal dimension of privacy refers to the quality of data to acquire new meanings or change meaning over time.

3) Bodily privacy referring to the integrity of the individual's body.

4) Behavioural privacy referring to the individual's activity and preference patterns, both explicit and implicit.

5) Contextual character of privacy referring to the fact that:

   a) citizen/consumer privacy perceptions depend strongly on the context: surveys indicate that certain types of personal data are likely to be regarded as more sensitive than others (financial data and medical data);

   b) compounded (personal) data can acquire a different value and meaning;

   c) (personal) data can acquire a different value and meaning if used in a different context than the one for which it was originally processed.

9.5.4.3 Emerging issues and requirements related to emerging or future applications, technologies, and other issues

New technological developments and new applications can bring about new categories of challenges to individual privacy and data protection. They might include one or a combination of the categories mentioned above and should be addressed by an RFID PIA. A non-exhaustive list of RFID-related emerging issues and requirements identified thus far include those referring to:

- data mining and profiling;
- smart technologies/applications - referring to technology convergence (e.g. RFID used in conjunction with GPS, sensor technology, etc.);
- internet of things/ambient intelligence - referring to things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental and user contexts;
- protection and rights of vulnerable individuals, including minors;
- workplace privacy - in relation to using RFID to track and/or trace activities of employees;
- tracking by proxy - referring to the possibility of inferring the identity of an individual through a RFID- tagged item belonging to the individual;
- corporate espionage - where the misuse of personal data acquired by means of RFID tampering or illegal access is not the purpose, but rather the means to acquire other economic, competitive advantage, etc.

10 RFID Penetration (PEN) Testing Outline

Penetration (PEN) testing takes a technology viewpoint to privacy, data protection and security of RFID systems and may be used to support a PIA. The need for developing standards for PEN testing of RFID systems are based on the results of the general RFID risk assessment (Annex C) and the PIA work.

NOTE 1: The security objectives and the technological implications inherent from the DPP objectives has been used as the basis for evaluating the need for RFID PEN testing standards and to develop the requirements for such.

NOTE 2: The PIA does not offer methodology to analyse the DPP and security implications of the RFID technologies and applications involved in a specific RFID system.

Risk assessment (security risk analysis) is an essential part of both PEN testing and PIA (clause 9) and should be carried out prior to or as the first activity of a PEN test. If a PIA has already been carried out, it includes a risk assessment. The goal of a risk assessment is to do a targeted and specific analysis of the applications and technologies of the RFID system under analysis. The general threats and vulnerabilities described in Annex C can be used as input to such analysis, as they outline the general threats to RFID systems, where some of these general threats may be relevant and some may not be relevant.

Risk assessment is a critical component of the system and information security lifecycle, producing lists of potential threats, inherent weaknesses in the system or the way the system is used and their realizations as vulnerabilities, including the identification of countermeasures. The identified set of countermeasures make up the countermeasure framework as defined in TVRA [i.16] and their common goal is to remove or protect against the vulnerabilities which they target, reducing the security risk level posed to the RFID system. The list of general RFID systems vulnerabilities is given in clause C.3. The countermeasure framework for these general vulnerabilities will be developed as part of phase 2.

NOTE 3: Countermeasures may be security mechanisms, security protocols, security procedures or detailed security requirements.

NOTE 4: In cases where the countermeasure framework consists of a set of detailed security requirements, it is the fulfilment of the inherent security properties of these requirements that is the subject for the PEN test.

The goal of a PEN test is to check whether the countermeasure framework is complete, consistent and indeed protects the RFID system under analysis and should be carried out on the actual implementation of the RFID system with the countermeasure framework deployed, if possible. A PEN test is carried out in a series of structured activities against the identified vulnerabilities from the risk assessment and additional vulnerabilities discovered as part of the PEN test analysis activities in an effort to exploit these vulnerabilities either by means of malicious and invasive software (malware, attacker tools, attack code, attack scripts, etc.) or manually, involving the gathering of information leading to a vulnerability exploit or disclosure of personal information.

NOTE 5: Countermeasures aim at removing or masking weaknesses in a specific RFID system and as a result vulnerabilities should be removed. A PEN test checks whether the vulnerabilities are indeed removed.

An introduction to PEN testing and an overview of existing PEN testing methodologies and standards are given in Annex D.

10.1 PEN testing standards and methodologies

There are mainly three standardization efforts of relevance for RFID PEN testing. These are the Open Source Security Testing Methodology Manual (OSSTMM) [i.49], National Institute of Standards and Technology (NIST) discusses penetration testing in SP800-115 [i.28] and the Information Systems Security Assessment Framework (ISSAF) [i.29]. OSSTMM is a comprehensive peer-reviewed methodology for performing security tests and metrics.
NIST SP800-115 [i.28] is less comprehensive than the OSSTMM, but more likely to be accepted by regulatory agencies. For this reason, NIST refers to the OSSTMM. The ISSAF is a peer reviewed structured framework from the Open Information Systems Security Group that categorizes information system security assessment into various domains and details specific evaluation or testing criteria for each of these domains. It aims to provide field inputs on security assessment that reflect real life scenarios. More information on the three methodologies is given in clause D.2.

The RFID ecosystem is comprised of a frontend part including tags and interrogators, the backend system and the network connection between the frontend and backend. OSSTMM has been examined and it has been concluded that OSSTMM covers the needs of the RFID backend system. Some of the structure in OSSTMM is also valid for PEN testing of the RFID frontend part. This will be further examined in phase 2 as part of standardising PEN testing of tag and interrogator communication. Preliminary PEN testing procedures have been developed and tested as part of phase 1. These are to be standardised as part of phase 2 work. The conclusion is that a tailored version of OSSTMM should satisfy most requirements of PEN testing of the network connection between the interrogator and the backend system. This is to be verified as part of phase 2.

NOTE: The RFID backend system is similar to other backend systems and existing methodologies therefore fulfils the needs of PEN testing standardisation of the RFID backend system.

10.2 RFID PEN testing standardization roadmap

The RFID ecosystem comprises tagged items, tags, interrogators, the RF link, network connection and the backend system (Figure 1). As a consequence, the responsibility for preserving privacy and protecting an RFID system is not limited to stakeholders producing or integrating RFID technology (system integrators), but also those providing the backend system. For this reason, the work has focused on PEN testing for all components of the RFID ecosystem, categorized into the frontend part (tagged items, tags and interrogators), backend system and the network connection between the frontend and backend. This also means that security measures or the placement of personal information can be distributed amongst the components in the RFID ecosystem. For example, if the tag cannot support the overhead and performance consequences introduced by some security mechanism (e.g. cryptographic operations), it should be investigated whether this information could be placed elsewhere in the RFID ecosystem and only provided on a strictly need-to-know basis.

PEN test guidelines should be developed for all components of the RFID ecosystem (for some of the components it will be possible to reuse existing PEN testing methodology as discussed in clause 8) and to analyse the specific RFID application deployment (system integration PEN testing).

There will be multiple RFID sectors and RFID applications or ecosystems within each sector that may have varying level of privacy and security needs. These should be identified and analysed for specific requirements derivation. The general privacy, data protection and security objectives for RFID are outlined in clause 8. The identified vulnerabilities (clause C.3) is linked to one or more of the objectives (clause 8) and the threats (clause C.2) describe ways to exploit the RFID system and by that violate one or more of the privacy, data protection and/or security objectives. The seriousness of such a breach depends on the required level of privacy and security of a specific RFID system. This level should be used to select the scope of an RFID PEN test for a specific RFID system.

10.3 PEN testing requirements and method outline

The analysis of existing PEN testing methodologies (clause D.2) resulted in the development of requirements for RFID PEN testing procedures and standardization activities.

The identified requirements and standardization activities for RFID PEN testing are:

- **Establish the scope and purpose of the RFID PEN test:** An RFID test should start with defining the scope of the PEN test tailored for the specific RFID system. This includes defining the following parameters: RFID system boundaries, DPP and security objectives of relevance and the validation of procedures (the success criteria). An RFID PEN testing standard should include guidelines on how to define scope and purpose of an RFID PEN test.

- **PEN tester skills and responsibilities:** A successful and effective PEN test relies on skilled and experienced personnel to perform the PEN test. Recommendations already exist to support the development of a framework for establishing the PEN testing environment and to specify the requirements for PEN testers. No standardization activities are needed in this area. In summary, the existing recommendations includes how to evaluate a PEN tester along the following dimensions:

  - Legally capable.

  - Experienced.

  - Ethically responsible.

- **Choose adequate set of tests:** Manual and automated tests will most probably yield the best balance of costs and benefits for RFID PEN tests. This means that an RFID PEN testing standard should provide guidelines on how to employ and combine black, white and grey box PEN testing.

- **Follow a methodology:** PEN testing should follow a structured process. An RFID PEN testing standard should specify the method and process of PEN testing of the frontend part (tag, interrogator and RF-link) and the network connection between the frontend and backend. Methodologies already exist for PEN testing of the RFID backend system but guidelines on applying these for RFID is needed.

- **Findings and recommendations:** This is a very important part of a PEN test. The final PEN test report has to clearly state the findings and map the findings to the potential risks. This should be accompanied by a balanced remediation roadmap based on RFID security best practices. An RFID PEN testing standard should include report templates for the various types of PEN tests supported by the standard.

11 Common European RFID Emblem and Sign

The requirements to be met by signs and emblems are summarised here with the analysis of a number of candidates proposed given in Annex E. The recommendation from the analysis is that the ISO RFID Emblem option expressing "RFID" as it is defined today (in ISO/IEC 29160 [i.33]) is adopted for the purpose of notifying the public of the presence of tags in retail environments and optionally elsewhere. Detailed analysis of the requirements for the emblem is given in Annex E.

An EN will be developed to perform the role of a "reader" sign reflecting the requirements of the Recommendation (in previous paragraph) and the wider stakeholder input as outlined in the requirements specification and summarised in Annex E. The Common European RFID sign will contain information required by the Data Protection and Privacy directives to inform the consumer in a retail environment, and optionally elsewhere, where interrogators are deployed of the purpose of the RFID system. The signage will include the following:

- the emblem;
- the purpose (application dependent); and
- the contact details of the data controller (content will be determined by the specific application).

Detailed requirements analysis for the sign is given in Annex E.

It is noted that consumers, on acquisition of items that contain an RFID tag may require more information than that provided in public signage to allow them to understand and manage their participation in the one or more applications associated with the tagged item(s) in their possession and thus the signage and emblem should be seen as only one means of providing the consumer with information.

12 Environmental aspects of RFID tags and components

12.1 Health and safety considerations

In 1999 the European Council issued Council Recommendation 1999/519/EC of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) [i.38]. This was in answer to general concerns relating to EMF exposure and was based around the Guidelines for limiting exposure to time-varying electric, magnetic and electromagnetic fields (up to 300 GHz) produced the year previously by the International Commission on Non-Ionizing Radiation Protection (ICNIRP). Following the publication of the Recommendation, the European Commission issued a mandate, M/305 [i.39], to the European Standards Organisations. This mandate was for the production of standards to limit human exposure to electromagnetic fields under the Low Voltage and RTTE Directives, using the EC Recommendation 1999/519/EC [i.38]. The horizontal coordination of this standards activity was undertaken by CENELEC TC106X, although it was possible for other relevant committees within ESOs to produce specific standards to fulfil the mandate.

CENELEC TC106X produced two standards in 1991 which specifically cover the human exposure to fields generated by RFID systems. CENELEC EN 50357 (2001) [i.40] provided the methods of assessment and CENELEC EN 50364 (2001) [i.42] was the harmonised standard which linked the methods of assessment to limits from the EC Recommendation 1999/519/EC [i.38]. The reason for producing two standards was so that the CENELEC EN 50357 [i.40] could be later forwarded to IEC for globalisation, without different regional limits around the globe becoming a problem.

Globalisation was successfully achieved in 2009 with the publication of IEC 62369-1, produced by IEC106. This standard was derived from the CENELEC EN 50357 [i.40], updated to include the latest state of the art. This was then also published in Europe as CENELEC EN 62369-1 [i.11]. The updated CENELEC EN 50364 (2010) [i.42] has since also been published to utilise the methods of assessment from the new standard.

In addition CENELEC TC106X has produced, and is still producing, standards for human exposure to EMF in the workplace under mandate M/351 for the Physical Agents (EMF) Directive, 2004/44/EC [i.54]. Although this Directive has had its implementation delayed until some aspects of its provisions are reviewed and updated, the standardisation work has continued where possible. CENELEC EN 50499 (2008) [i.43] and any specific standard it calls up, is the general procedure for the assessment of the exposure of workers to electromagnetic fields, which would include RFID. Work in this area continues and is planned to include a specific standard for assessment of RFID in the workplace, once the final provisions of the Physical Agents (EMF) Directive [i.54] are clearer.

CENELEC continues to monitor new developments and knowledge and also continues to work together with IEC and other ESOs to develop standards for human exposure to EMF. There are standards already in place to address concerns over human exposure to the EMF from RFID and this work will continue to further address exposure in the workplace; and to monitor, review and update existing standards where necessary.

Suppliers of RFID interrogators and tags are expected to comply with existing and developing standards covering human safety in the presence of electromagnetic fields. (These standards should cover safety in the presence of both continuous emission and pulsed emissions).

12.2 RFID hardware end of life considerations

RFID components are expected to comply with the existing end of life laws and organisations may reasonably be expected to have implemented ISO 14000 [i.55] structures to manage these aspects and any existing sector specific regulations (e.g. Waste Electrical and Electronic Equipment (WEEE) directive [i.44]).

12.3 Data end of life considerations

There may be a conflict between end of purpose and the end of the lifetime of data on a tag. Data held on a tag that is either personal or which acts as a pointer to personal data should be destroyed at the end of the purpose unless the purpose is explicitly changed and consent to retain the data on the tag for the new purpose is recorded.

SCENARIO: In the fashion industry clothes are generally sold for a season (winter/summer/spring/autumn) and have a short purpose life (say 6 months). In contrast the data on the tag may reasonably be expected to be able to be retrieved for periods of up to 50 years (if access is only by RF the antenna circuit may degrade at a faster rate restricting access more quickly).

Annex A:
Summary of status of RFID standardization

Figure A.1 outlines the main components of an RFID system based on existing and emerging standards. Where a standard does not exist similar functions are currently achieved using proprietary solutions. The purpose of the colour coding is to group together similar types of components. The relevant standardisation activities and the status for each component are discussed in Table A.1.

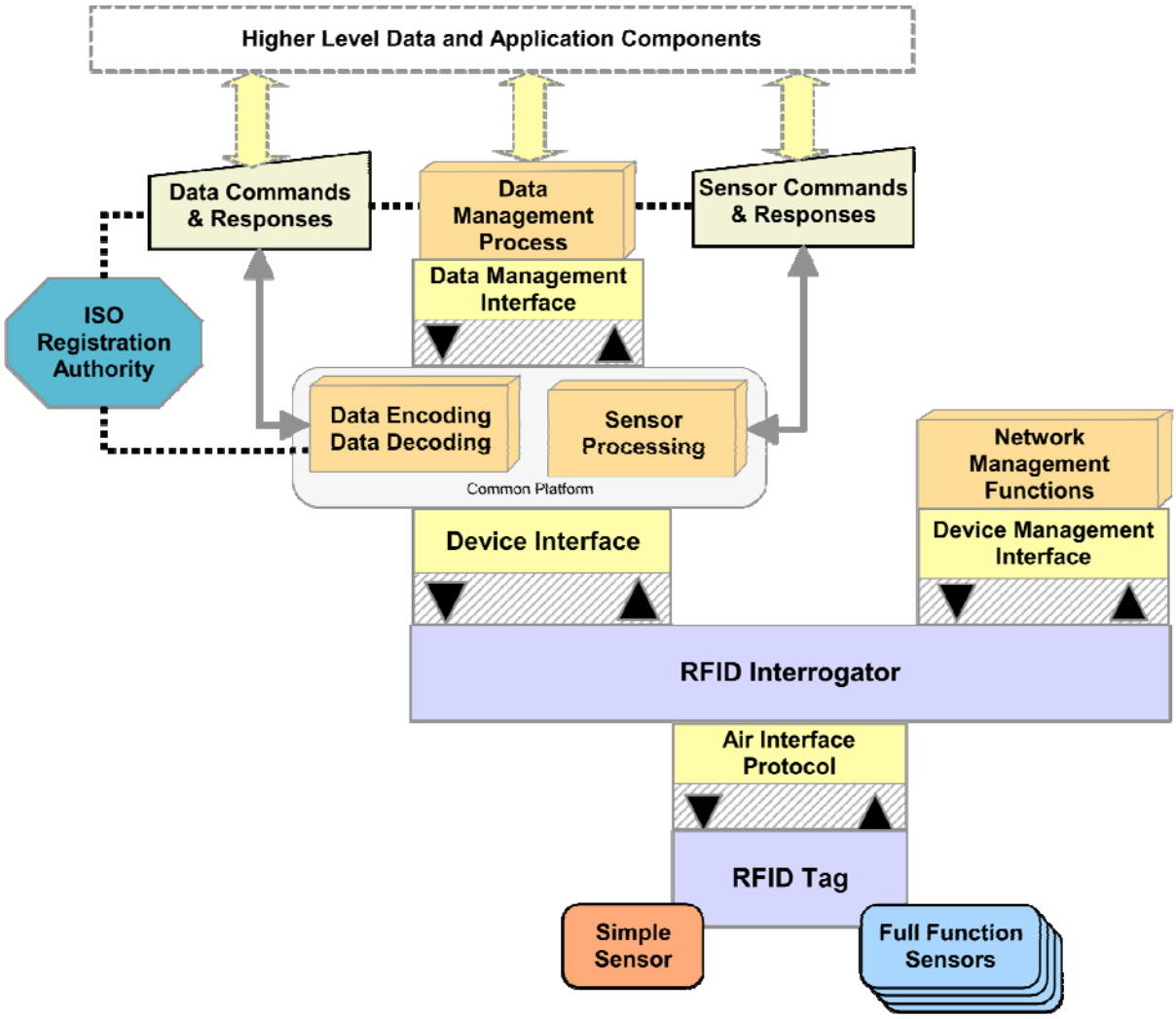


Figure A.1: Schematic diagram outlining the main components in an RFID application

Table A.1: Summary of technology standardisation for each component

Component	SDO	Specification	Comments and status
RFID Tag	None	None	There are no standards that specify the requirements for the tag. The tag is expected to be designed in such a way that it supports the air interface and the data encoding specifications.
Sensors	ISO/IEC	ISO/IEC 18000-6 [i.9]	Sensors of interest in an RFID context are those that are attached to RFID tags communicating with the application over the RFID air interface protocol. The identified standard describes extensions for Type C and D tags for sensor functionality.
Air Interface Protocol	ISO/IEC	ISO/IEC 18000-x [i.9]	Each part of the ISO/IEC 18000 [i.9] series is focused on the communication frequency and may specify more than one RFID technology.
NOTE: Manufacturers have great flexibility in implementing the ISO/IEC 18000-x [i.9] specifications that has resulted in numerous different product variants all compliant with the standard.			
The Interrogator	None	None	There are no standards that specify the requirements for the interrogator. The interrogator is expected to be designed in such a way that it supports the air interface and the data encoding specifications.
Device Interface	ISO/IEC	ISO/IEC 24791-5 [i.45]	The device interface is the communication point between the interrogator and the application. The EPCglobal "Low Level Reader Protocol" standard [i.56] has been extended by ISO in the identified standard.
Device Management Interface	ISO/IEC	ISO/IEC 24791-3 [i.46]	The identified specification only applies to 18000-6 [i.9] Type C tags and is an extension of EPCglobal's Discovery, Configuration and Initialisation (DCI) standard [i.56].
Network Management Functions	None	None	There are no standardisation activities for the network management functions.
Data Encoding and Decoding	ISO/IEC	ISO/IEC 15962 [i.3] ISO/IEC 15961 [i.2]	The identified specification is derived from the EPCglobal Tag Data Standard [i.57] that converts the EPC Manager, Product and Serial Number into the bit string encoded on the RFID tag.
Sensor Processing			This is concerned with configuring sensors and decoding the observed data. As for sensors, the risks are mostly related to tampering of data. The ISO/IEC 18000-6C air interface protocol supports an access password, which has been proposed for used by those authorised to configure and re-configure a sensor. Reading the sensor data is less of a concern and is compatible with the open system nature of providing sensor data. Apart from the configurable fields, all the "writing of data" is carried out automatically by the sensor, and there are no commands to write data to the monitoring and history records.
ISO Registration Authority	ISO/IEC	ISO/IEC 15961-2 [i.2]	
Data Management Interface	ISO/IEC	ISO/IEC 24791-2 [i.47]	Whilst the identified specification exists it is noted that many proprietary solutions apply in this area.
Data Management Process	None	None	This is effectively the edge of the business operating system, be it a warehouse management system, library management system, retail store system, hospital patient registration system, baggage handling system, transport ticketing system and so forth. The type of personal data and the retention of that data should already be the subject of data protection regulations.
Data Commands and Responses	ISO/IEC	ISO/IEC 15961-1 [i.2]	

Annex B:
Summary of tag capabilities

B.1 Command set

The following example is taken from the ISO 18000-6 [i.9] type C tag specification and is offered as an example of the typical command set available across the RF link.

NOTE: Other tags will have different command encoding, different mandatory status, and different protection modes applied.

Protection is used to refer to the protection given to the data returned. If for example "unique command length" is indicated, the response is rejected if the length of the response does not match the expected length. Similarly if "CRC-5" or "CRC-16" is indicated the tag response contains a Cyclic Redundancy Check (CRC) to allow some forward error correction. It should be noted that a CRC does not provide proof of integrity but does provide protection from transmission errors.

Table B.1: ISO 18000-6 type Type C Air interface command set

Command	Length (bits)	Mandatory	Protection
QueryRep	4	Yes	Unique command length
ACK	18	Yes	Unique command length
Query	22	Yes	Unique command length and a CRC-5
QueryAdjust	9	Yes	Unique command length
Select	> 44	Yes	CRC-16
NAK	8	Yes	Unique command length
Req_RN	40	Yes	CRC-16
Read	> 57	Yes	CRC-16
Write	> 58	Yes	CRC-16
Kill	59	Yes	CRC-16
Lock	60	Yes	CRC-16
Access	56	No	CRC-16
BlockWrite	> 57	No	CRC-16
BlockErase	> 57	No	CRC-16
BlockPermalock	> 66	No	CRC-16

B.2 Security functionality

B.2.1 Tag embedded capabilities

The following capabilities are offered across a number of the ISO specifications as an illustration of the capabilities available within the CIA paradigm for RFID tags and interrogators. It should be noted that the Password enabled functions and the memory locking functions are not considered as security functions that present a high assurance capability to the end user. In particular as the password solution may be silicon embedded and a single password may be shared amongst many devices using only a 32 or 48 bit solution password guessing attacks may be considered as trivial (or if countered by failure lock out mechanisms will be a vector for denial of service attacks (i.e. if only n attempts can be made to unlock data on the tag then an attacker only has to make n+1 attempts to prevent any future unlock occurring).

Table B.2: CIA capabilities in RFID tags

ISO Reference	Frequency	Memory locking	Supports Access Password	Supports Kill Password	Standardised security	CIA capability (See Note 1)
ISO 11784 [i.34]/85	<135 kHz			No	No	Integrity: CRC
ISO 14223 [i.36]	<135 kHz			No	No	Integrity: CRC
ISO/IEC 14443 [i.5]	13,56 MHz	Yes	Yes	No	ISO/IEC 14443-4 [i.5]	Confidentiality: by passwords or keys, various solutions exist on top of the basic air interface standards ISO/IEC 14443-1, -2 and -3 [i.5] Integrity: CRC and additional means Authentication: Mutual authentication Authorization: multiple keys
ISO/IEC 15693 [i.6]	13,56 MHz			No	No	Confidentiality: only as proprietary solutions
ISO/IEC 18000-2 [i.9]	<135kHz			No	No	Integrity: CRC
ISO/IEC 18000-3 [i.9] Mode 1	13,56 MHz	permanently lock any block	No	No	No	Confidentiality: only as proprietary solutions Integrity: CRC
ISO/IEC 18000-3 [i.9] Mode 2	13,56 MHz	all words up to lock pointer, which can be reset to a higher value	Yes, 48-bit password may be invoked	No	No	Integrity: CRC
ISO/IEC 18000-3 [i.9] Mode 3	13,56 MHz	Locking is based on password control for permanently locking or for unlocking and relocking. For MB01, 01, 10 locking applies to the complete memory block; MB11 can be selectively locked	Optional 32 bit password	Optional 32 bit password	ISO/IEC 29167-1 [i.30] and ISO/IEC 29167-3 [i.30] under development	Confidentiality: Access password Integrity: CRC and additional means in ISO/IEC 29167-3 [i.30] Authentication: Mutual authentication Authorization: multiple keys
ISO/IEC 18000-4 [i.9] Mode 1	2,45 GHz	Selectively by individual 8-bit block	No	No	No	Integrity: CRC
ISO/IEC 18000-4 [i.9] Mode 2	2,45 GHz	No	No	No	No	Integrity: CRC
ISO/IEC 18000-6 [i.9] Type -	860 MHz to 960 MHz	Selectively by block	No	No	No	Integrity: CRC
ISO/IEC 18000-6 [i.9] Type -	860 MHz to 960 MHz	Selectively by individual 8-bit block	No	No	No	Integrity: CRC

ISO Reference	Frequency	Memory locking	Supports Access Password	Supports Kill Password	Standardised security	CIA capability (See Note 1)
ISO/IEC 18000-6 [i.9] Type -	860 MHz to 960 MHz	18000-6 AMD1: complete MB. Later version: Locking is based on password control for permanently locking or for unlocking and relocking. For MB01, 01, 10 locking applies to the complete memory block; MB11 can be selectively locked	Optional 32 bit password	Optional 32 bit password	ISO/IEC 29167-1 [i.30] and ISO/IEC 29167-6 [i.30] under development	Confidentiality: Access password Integrity: CRC and additional means in ISO/IEC 29167-6 [i.30] Authentication: Mutual authentication Authorization: multiple keys
ISO/IEC 18000-6 [i.9] Type -	860 MHz to 960 MHz	Selectively in 16-bit, or 32-bit, or 64bit sequences depending on the IC manufacture	No	No	No	
ISO/IEC 18000-7 [i.9]	433 MHz	Yes	Yes	No	ISO/IEC 29167-6 [i.30] planned	Confidentiality: Access password
ISO/IEC 18092 [i.48]	13,56 MHz				Various additional standards related to ISO/IEC 18092 [i.48]	Confidentiality: extensive measures exist Integrity: CRC and additional means Authentication: Mutual authentication Authorization: multiple keys
NOTE 1: The CIA capability covers Confidentiality, Integrity, Authentication, Authorisation and Identification. Capabilities that are not covered are not mentioned. NOTE 2: The state of the art for cryptanalysis is generally taken as the time that an attacker without access to the key is able to recover the plain text of an encrypted message.						

Annex C:
Summary of risk assessment of RFID systems

C.1 Security analysis and requirements derivation

The analysis followed the ETSI standard for risk assessment, the Threat, Vulnerability and Risk Analysis as specified in TS 102 165-1 [i.15]. TVRA comprises seven steps, including identification of weaknesses, threats and vulnerabilities. RFID systems come in a wide variety of applications and comprise a number of technologies. As risk estimation and evaluation requires context and specific application information, such activities were not carried out as part of the analysis. The goal of the analysis was not to establish the specific risks but to identify the main vulnerabilities of RFID systems. The list of vulnerabilities is given in clause C.3 and has been used as input to the derivation of privacy, data protection and security objectives and requirements (clause 8).

NOTE 1: This Annex reviews some attacks many of which are not specific to RFID and the vulnerability being exposed may be exposed in other, non-RFID, systems. However it is essential to address such vulnerabilities in the evaluation.

One of the main purposes of RFID is to identify and track objects by means of their attached RFID tag. A primary characteristic of RFID is for tags to be read remotely by interrogators at known locations, where in some cases the interrogator is able to extract additional information including the location and time of the read. Such information can be used to track tagged items. In addition to tracking objects in a logistics environment, RFID tags are also used for access control (e.g. for transport systems), and for linking data to objects (e.g. in object hyperlinking).

NOTE 2: The involuntary reading of proximity and vicinity tags is improbable without detection due to the required proximity of the attacker to the victim, while the involuntary reading of long range systems is possible without detection.

Threats are potential events that can cause a system to respond in an unexpected or damaging way. It is useful to categorize threats to determine effective and deployable mitigation strategies. The identification and analysis of RFID relevant security threats (general and application specific) have been carried out according to the STRIDE model [i.27], which include the following categories:

- Spoofing of identity (masquerade).
- Tampering with data (manipulation).
- Information disclosure.
- Denial of service.
- Elevation of privileges.

The following clauses describe the threats in general terms and illustrate the threat in the RFID context by scenarios. The scenarios are not considered as exhaustive and they are not, at this stage, ranked in terms of viability or impact on the system.

NOTE 3: Attack classes are not specific to a technology but some technologies have greater or lesser inherent weaknesses that lead to greater or lesser development of attack vectors.

C.2 Weaknesses and threats in RFID systems

TVRA [i.16] separates between weaknesses, threats and vulnerabilities. In the context of RFID systems, weaknesses describe problem areas in RFID systems. Threats are potential events that can cause damage to the RFID system and vulnerabilities are the combination of a threat and a weakness describing how the threat may exploit the weakness and the potential output. The result of the threat identification was categorized into privacy and data protection (DPP) related threats and security specific threats.

NOTE 1: The privacy and data protection (DPP) related threats have been used as input to DPP objectives specifications in clause 8.

NOTE 2: The security specific threats have been used as input to security objectives specifications in clause 8.

NOTE 3: The extent and magnitude of the specific threats listed below will vary by technology and the design of the RFID system.

Privacy and Data Protection (DPP) related threats:

- T1-Identify theft;
- T2-Profiling;
- T3-Data linkability;
- T4-Tracking;
- T5-Exclusion of the data subject from the data processing process due to disabling of RFID tag;
- T6-Procedures / instructions not followed leading to tags being used past end of purpose;
- T7-Large-scale and/or inappropriate data mining and/or surveillance;
- T8-Non-compliance with data protection legislation other than those covered in T1 to T7;

Security threats:

- T9-Denial of service attack (flooding, blocking, buffer overflow, etc.);
- T10-Collision attack;
- T11-De-synchronization;
- T12-Replay;
- T13-Man-in-the-middle attack;
- T14-Theft;
- T15-Unauthorised access to / deletion / modification of data (in tags, interrogators, backend system);
- T16-Cloning of credentials and tags (RFID related);
- T17-Worms, viruses and malicious code;
- T18-Side channel attack;
- T19-Masquerade (attacker illicitly acting as a legal user to gain access to data or equipment);
- T20-Traffic analysis/scan/probe;
- T21-RF eavesdropping.

C.2.1 Privacy and Data Protection (DPP) related threats

C.2.1.1 Identify theft

Identity theft is a form of fraud in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. The victim of identity theft (here meaning the person whose identity has been assumed by the identity thief) can suffer adverse consequences if he or she is held accountable for the perpetrator's actions. Organizations and individuals who are duped or defrauded by the identity thief can also suffer adverse consequences and losses, and to that extent are also victims.

C.2.1.2 Profiling

Anonymous profiling is used in retail for targeted sales and commercials. Profiling as long as it is done with a priori consent and agreement from the affected individuals or anonymized is not considered a problem in the context of this report. The problem is cases where information collected and distributed over RFID systems can be used to identify behaviour patterns and other personal data, which can be used to build a profile without a prior consent.

C.2.1.3 Data linkability

Figure 4 in clause 6 shows how behavioural and other non-personal information can be linked to derive personal information. Data linkability refers to cases where data collected and processed in RFID systems can be aggregated into information which may be used to derive personal information.

C.2.1.4 Tracking

Tracking is a threat directed to the privacy of users. RFID interrogators in strategic locations can record sightings of unique tag identifiers (or "constellations" of unique and/or non-unique tag identities), which are then associated with personal identities. The problem arises when individuals are tracked involuntarily. Subjects may be conscious of the unwanted tracking (e.g. school kids, senior citizens and company employees), but that is not always necessarily the case.

NOTE: Some technologies, such as mobile phones, require that the device is always reachable which can be considered as tracking. However this is often perceived as a desirable trade-off and is consensual. If a mobile phone user wishes to be invisible they can choose to switch off their phone and tracking will stop.

C.2.1.5 Exclusion of the data subject from the data processing process due to disabling of RFID tag

This threat deals with procedures and practices requiring the tag to remain active to gain access to specific services. For example, retail stores may restrict the ability of consumers to return items for which the tag has been disabled.

C.2.1.6 Procedures/instructions not followed leading to tags being used past end of purpose

Consent is most often given for a specific purpose or use of data. As most RFID systems do not exhibit an interface towards the consumer, the purpose of data collection and processing are given a priori. This specifies the purpose of the tags and the lifetime of the data collected. When tags are used past the initial purpose, data can be linked and personal information may be derived.

C.2.1.7 Large-scale and/or inappropriate data mining and/or surveillance

This threat refers to cases where a significant number of items carry tags and where tags are used to collect data in a number of contexts. The data from various RFID systems may be aggregated, particularly in RFID backend systems, deriving personal information. The combination of RFID systems may also result in the ability to profile and track individuals resulting in surveillance.

C.2.1.8 Non-compliance with data protection legislation

In addition to the above privacy and data protection related threats, there are threats arising from non-compliance with data protection legislation outside of consent and purpose. Details are given in clauses 7 and 8. An example is function creep.

C.2.2 Security threats

C.2.2.1 Denial-of-Service attack

Denial-of-Service attacks are events resulting in reduced or no service to valid users. Denial-of-Service attacks are relatively easy to accomplish and difficult to guard against. The below scenarios are some ways in which Denial-of-Service attacks may be carried out in RFID systems.

SCENARIO#1: An attacker may kill tags in the supply chain, warehouse or store disrupting business or to prevent check-out of a particular item.

SCENARIO#2: An attacker removes or physically destroys tags attached to objects. This is used by an attacker to avoid tracking. A thief destroys the tag to remove merchandise without detection.

SCENARIO#3: An attacker shields the tag from being read.

SCENARIO#4: An attacker with a powerful signal generator could jam the return signal from the tag although such an action would most probably cause the interrogator to raise an alarm.

C.2.2.2 Collision attack

Collision attacks violate the way in which the interrogator single out a specific tag for communication. Interference with other radio transmitters may prevent an interrogator from discovering and polling tags. Tag collision occurs when more than one tag responds to the interrogator's interrogation at the same time. Without any coordination amongst the interrogator and the tags, the responses from the tags will become illegible to the interrogator. The attacker acts as one or more tags to respond to the query from the interrogator at the same time hence a collision happens. Collision attack is a variant of DoS attacks.

C.2.2.3 De-synchronization

De-synchronization refers to the threat of de-synchronizing the identity between a back-end database server and a RFID tag, which may render the tag useless. There are two kinds of operation between the tag and the interrogator, read and write. The main function of write is to write data into the tag. The intention of a de-synchronization attack is to destroy the operation of the write process. In addition, the write operation (like updating identities) may fail in cases where the attacker successfully destabilizes the connection between the tag and the interrogator or the network.

NOTE: To slow down the interrogation process it would be necessary to use multiple tags with different IDs.

C.2.2.4 Replay

Replay attacks aims to consume the computing resources of the tag and the interrogator. For example, in an attack against an RFID interrogator, the attacker may gain access to the identity of an RFID tag from previous communication and then replays this identity or communication to the interrogator forcing it to respond to an outdated communication request.

C.2.2.5 Man-in-the-middle attack

The man-in-the-middle attack (often abbreviated MIM) is a form of active eavesdropping in which the attacker makes independent connections with tags, interrogators and/or the RFID backend system and relays messages between them, making them believe that they are talking directly to each other, when in fact the entire conversation is controlled by the attacker. The attacker has to be able to intercept messages going between the two victims and inject new ones, which may be possible in some RFID systems.

A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other.

C.2.2.6 Theft

Theft is not a specific security problem, but a problem area of RFID systems as tags and some interrogators may be detached and removed from the intended or original premises.

C.2.2.7 Unauthorised access to/deletion/modification of data (in tags, interrogators, backend system)

Unauthorised access to, deletion or modification of equipment occurs when an attacker modifies, adds, deletes, or reorders data. The impact of such attacks range from serious threats such as an attacker modifying the data in a passport to modifying the product code/identity on tags in the supply chain, warehouse or similar disrupting business operations and causing a loss of revenue. For a user, tampering of data may lead to failure to enter a country (passport attacks), wrong identity, somebody masquerading as the user, loss of service, loss of reputation, financial loss and identity fraud.

SCENARIO: Altering the data encoded on a tag at tag personalisation such that it mislabels a tagged item.

CONCERN: An observed problem with the "kill" command is that this feature can be misused by an attacker as a consequence of the password distribution being difficult to secure or because of failure to implement a password. In either case the attacker may kill tags with a number of consequences ranging from diversion of items, through loss or theft of items, to business failure (the level of impact depends on the dependency of the impacted business on the RFID technology working properly).

C.2.2.8 Cloning of credentials and tags (RFID related)

Most tags possess no explicit anti-cloning features. Also standards do not exist that prescribe mechanisms for interrogators to authenticate the validity of the tags they scan. A tag emits its response promiscuously and interrogators accept the validity of the tags they scan by default. The result is that tags are vulnerable to elementary cloning attacks. An attacker can learn a tag's essential data, simply by scanning it or by gaining access to an appropriate tag database. If the unique tag identifiers are not random, e.g. if they are sequential, then an attacker that sees the tagged item identity can guess or fabricate another valid item identity.

C.2.2.9 Worms, viruses and malicious code

Software infections, commonly referred to as a virus, can be used to manipulate, disclose or maliciously prevent communication between tags, interrogators, network connections and the backend system. It may be possible for the payload of an RFID tag to carry either a virus or the trigger for or link to one. This may be of particular relevance in object hyper-linking scenarios. Details and descriptions of scenarios are continuously updated at www.rfidvirus.org.

NOTE: The virus problem is not specific to RFID and therefore should be addressed both for the frontend and backend part of RFID systems, where the frontend part comprises the tag and interrogator.

C.2.2.10 Side channel attack

A side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis). For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Many side-channel attacks require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented.

C.2.2.11 Masquerade

Masquerade occurs when an attacker successfully poses as an authorized user of a system. There are many ways in which such an attack can affect RFID systems, ranging from competitors performing unauthorized scanning of inventory to obtain information on types and quantities of items to more serious intrusion of the privacy of individuals. The tag identities can for some tag technologies be emulated, giving rise to the possibility of tag masquerade. This is made possible if a tag cannot distinguish between legitimate and illegitimate interrogators. To the tag, an interrogator is an interrogator. Also, the numbering scheme used for RFID tags contains the tag identity and may include information about the manufacturer and possibly the product number.

C.2.2.12 Traffic analysis/scan/probe

Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. For RFID systems it may be useful simply to observe the locations of tags and interrogators and the frequency of the communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. The result of traffic analysis of RFID systems may lead to knowledge about location and type of tags and interrogators, network connections and the backend system.

C.2.2.13 RF eavesdropping

Eavesdropping is the act of secretly listening to communications without consent. Since an RFID tag is a wireless device, the RF signal between tags and interrogators can be eavesdropped.

NOTE: Several tests have been undertaken and the general observation is that actual read ranges are greater than those specified in the standards, or as claimed by vendors.

If the attacker knows the specification of encoding, the signal picked up can have serious implications - used later in other attacks against the RFID system, such as Spoofing attack, Replay attack and Tracking.

C.3 Summary of vulnerabilities in RFID systems

The approach to risk analysis used in the ESOs is to identify the weaknesses of systems and to identify the threats or threat agents able to exploit the weakness. When a weakness is exploited the system exhibits a vulnerability [i.16].

The below list summarizes the main open issues and problem areas derived from the result of the analysis of privacy, data protection and security related threats to RFID systems. These vulnerabilities have been used as the basis for specifying the privacy, data protection and security needs, which are formulated as objectives according to TS 102 165-1 [i.15] and TR 187 011 [i.25]. The list of objectives and their requirements derivation is given in clause 8.

NOTE: The list of vulnerabilities should not be looked upon as an exhaustive list of privacy, data protection and security weaknesses in RFID systems. Clause 7 extends the list below, including DPP regulatory aspects and PIA specific requirements. The list below is not given in a prioritized order:

- non-compliance with the data minimization and proportionality principles;
- non-compliance with the purpose limitation (finality principle);
- non-compliance with the transparency principle;
- non-compliance with the legitimacy of data processing, e.g. consent;
- non-compliance with the data conservation principle;
- non-compliance with the rights of the data subject (such as the right for rectification, blocking or deletion of data);
- lack of data correction mechanisms (as normally data subjects do not have access to the databases);
- lack of common or harmonized legislation in EU Member States;

- data linkability;
- profiling;
- inappropriate / inadequate identity management;
- inherent features (size, material, etc.): easy to lose, and to steal. Data, but not the UID, may be copied using specialist equipment;
- actual read range longer than the operational norm. Risks are greatest for UHF systems;
- RFID tags do not have a turn-off option;
- inadequate security measures of data storage (e.g. inadequate encryption measures);
- insufficient protection of data communication (weak or no encryption, etc.);
- insufficient protection against DoS attacks.

Annex D:
RFID Penetration Testing

D.1 Short Introduction to PEN testing

This annex gives a short introduction to PEN testing and an overview of existing PEN testing methodologies and standards.

There are three main categories of PEN testing which all may be carried out once or multiple times, on-site or off-site or a combination, and paper-based or in real-time or a combination:

- Whitebox testing.
- Blackbox testing.
- Greybox testing.

White box penetration tests evaluate the efficacy of a system's internal protection, including the way in which the system is used. System or network configurations, protocol specifications, source codes and the occasional password are provided in the white box penetration test. The purpose of providing this information is to reduce the resources invested in PEN testing and to check that the system can withstand security attacks even when some of its security information is made available to attackers or other outsiders. The white box PEN test is usually less expensive than the black box testing as most of the relevant information necessary to exploit the identified vulnerabilities is provided up-front. The goal of a white box test is to check the robustness of a system in its specific system environment where the security information cannot be strictly controlled (several stakeholders involved, exchange of passwords over insecure communication, multiple use of the same password (the same password used across multiple interrogators or tags, etc.)).

In a black box PEN test no information on the system or its security measures are provided up-front simulating the environment of an attacker with no prior knowledge about the specific RFID system. This means that the attacker may have general knowledge about RFID, but not about the specific RFID system being analysed. The tester will use all of the tricks and methodologies at his disposal in an effort to emulate the persistence, knowledge and expertise level of potential attackers. The tester may also use specialized equipment that is normally only available to producers or operators of the RFID system to emulate the power and abilities of professional attackers or attacker networks. A black box PEN testing is usually more expensive than a white box PEN test.

Grey box PEN testing is a combination of white and black box testing. Some security and system information is made available in a grey box test, but not as much as that provided in a white box test. This is to simulate cases where an attacker has some information but not all that is necessary to break into the specific RFID system. The first activity in a grey box test is for the tester to use the available information to acquire more information, potentially leading to the ability to exploit one or more of the system's vulnerabilities.

D.2 PEN testing methodologies and standards

The Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for performing security tests and metrics. The OSSTMM test cases are divided into five channels which collectively test: information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunication networks, wireless devices, mobile devices, physical security, access controls, security processes, and physical locations such as buildings and other physical perimeters.

The OSSTMM focuses on the technical details of exactly which items need to be tested, what to do before, during, and after a security test, and how to measure the results. OSSTMM is also known for its Rules of Engagement which define for both the tester and the client how the test needs to properly run starting from denying false advertising from testers to how the client can expect to receive the report. New tests for international best practices, laws, regulations, and ethical concerns are regularly added and updated.

The National Institute of Standards and Technology (NIST) discusses penetration testing in SP800-115 [i.28]. The NIST methodology is less comprehensive than the OSSTMM; however, it is more likely to be accepted by regulatory agencies. For this reason, NIST refers to the OSSTMM.

The Information Systems Security Assessment Framework (ISSAF) [i.29] is a peer reviewed structured framework from the Open Information Systems Security Group that categorizes information system security assessment into various domains and details specific evaluation or testing criteria for each of these domains. It aims to provide field inputs on security assessment that reflect real life scenarios. The ISSAF should primarily be used to fulfil an organization's security assessment requirements and may additionally be used as a reference for meeting other information security needs. It includes the crucial facet of security processes and their assessment and hardening to get a complete picture of the vulnerabilities that might exist. The ISSAF, however, is still in its infancy.

Annex E:
Summary of requirements and analysis for signs and emblems

E.1 Requirements specification

The common European RFID sign is targeted at raising public awareness to diminish fears and remove barriers to widespread European RFID adoption. Emblems/logos can contribute to this process primarily due to their potential small size, low cost and to transcend language frontiers. This may be largely sufficient but there are concerns that if such an emblem/logo is deployed without an associated common European information sign the emblem/logo may raise unjustified suspicion and negative emotional public response. Examples of such contagious public reaction to poorly conceived RFID pilots have been numerous over the last 8 years and as RFID applications have moved into the public domain. Many RFID and associated technologies have chosen to disassociate themselves with RFID as a result through renaming or rebranding of their initiatives. Furthermore there are proposed requirements of the common European RFID sign which cannot be fulfilled by an emblem alone. It is for these reasons that consideration of an RFID sign has been structured into the initial requirements specification.

NOTE 1: The term emblem is preferred as the term Logo can often imply a trademark.

The following requirements have been collected from preliminary input from CEN TC225 and from the discussion within RACE networkRFID Work Package 5.

NOTE 2: The requirements stated in this annex do not constitute a specification or standard but are intended as input to the future standardisation process.

E.2 RFID Emblem/Logo classified requirements

E.2.1 General Requirements Specification

Ref.		Primary	Secondary	Further Information	Additional Comments
E.1	What is the overall goal the RFID emblem/ logo is setting out to contribute to?	1) Public confidence in RFID applications through notification/awarenes s of the possible (i.e. beyond reasonable doubt that there are no RFID tags or interrogators) presence of tags and interrogator systems (i.e. interrogator antenna and interrogator). 2) Link to signs which explain the RFID application (see RFID sign specification).	Contributing to: 1) Wider, faster paths to RFID adoption in Europe. 2) Broader industrial applications through visibility increasing the confidence of all stakeholders and thereby in reinforcing consistent and uniform European application of privacy and security requirements. 3) Providing access to a broader range of trusted RFID applications serving or interacting with the public. 4) Reinforcing European competitiveness through innovation and efficiency in broader areas of society. 5) Increased security and safety for private individuals and organizations.		Similar requirements are envisaged for other and future wireless technologies. So accommodation of general wireless identification (Wireless ID, Wireless Sensor Networks, IoT) could be a distinct advantage to the public and organizations.

Ref.		Primary	Secondary	Further Information	Additional Comments
E.2	What is the purpose?	1) Public awareness/ notification of possible presence of RFID interrogators or tags. 2) Building trust through providing visibility to something which is invisible (devices small, difficult to identify, located inconsistently, often hidden, etc.). 3) Consistent presentation across EU Member states.	1) Removing the "hidden" and "silent" aspect of RFID which generates fears of vulnerability through a loss of control to unknown 3rd parties. 2) As a deterrent to property theft.	Building trust in: 1) The application(s). 2) The owner/ operator. 3) The technology.	Neither the "hidden" nor "silent" aspects of RFID contribute to most applications. These aspects do sometimes detract from applications e.g. like bar codes without their bar code scan beep.
E.3	Which applications?	1) **Suitable for all.** 2) **Optimized for the following:** **i) Retail environments:** a) On product where RFID tag or RFID interrogator embedded or associated with the product. b) On product packaging (display or transport) where the product or product packaging has an RFID tag or the product has an embedded or associated RFID tag or interrogator. c) On displays or promotional stands. d) On shelves. e) At POS. f) At access doorways, etc. g) On product advertising or promotional material where this is associated with RFID associated products or packaging. **ii) Pharmaceutical:** a) Product packaging. b) POS/dispense. c) Product instructions. d) Notifications /instructions + as retail above. **iii) Libraries:** a) All forms of tagged media. + as retail above. **iv) Passports/ID document**	At places of work where RFID systems or RFID applications are installed, present or operated.		The CE RFID project provided categories of existing RFID applications.

Ref.		Primary	Secondary	Further Information	Additional Comments
		systems/Loyalty Cards. **v) Contactless payment systems.** **vi) Pet vaccination.** a) cards/certificates. + as retail above. **vii) Industrial/Services.** a) access control systems. b) production/process automation. c) logistics. **vi) Access control/Security** a) facility access. b) vehicle access. c) vehicle immobilizers.			
E.4	What are the reference values to be implemented or, with which there is the aim of being associated?	1) Trust. 2) Confidence. 3) Openness/ Transparency. 4) Convenience/User friendliness.		Values with which the RFID emblem/logo (or sign) is **NOT** to be associated: 1) Hazard/Danger/ Threat. 2) Warning. 3) Surveillance/ Monitoring	When legally permitted information generated by RFID applications may be used for the purposes of enriching personal or property surveillance type information but this is to be referenced or explained in the corresponding RFID sign (see RFID sign below).
E.5	Who is the target for the message presented by the emblem/ logo?	1) General Public: i) All ages. ii) All ethnical origins/ nationalities. iii) All European cultures. 2) Employees.	1) General Public and& Employees: i) All abilities.	Where all abilities refer to educational attainment and physical abilities (e.g. blind, etc.). It should be possible for the RFID emblem/ logo through its concept/design to be accessible to this group, although there are no precedents to suggest it is essential.	
E.6	Who is the target for the technical specification/ guidelines?	1) Specification and guidelines - anyone ordering RFID tagged items which are or could be presented to the general public. 2) Specification and guidelines - anyone that manufactures RFID tagged items which are or could be presented to the general public. 3) To be employed by all owners or operators of RFID systems and			Not necessarily for RFID tag manufacturers unless they are delivering RFID tags (converted or otherwise) which are or could be public facing.

Ref.		Primary	Secondary	Further Information	Additional Comments
		applications.			
E.7	**How?**	1) No text, nor additional symbols, nor other elements should be **essential** for the emblem/logo to be capable of raising general public awareness to the (possible) presence of RFID tags or RFID interrogators and linking with the common European RFID sign. 2) The sign has to be clearly recognizable from a minimum distance of 6 metres. 3) The sign has to be designed in such a way that does not detract or divert attention from safety or safety related emblems/logos/signs	1) Text and/or symbols can be present but should then: i) Mention the letters "RFID". ii) Optionally indicate the relationship with the common European RFID application sign through the economic/minimal use of text, symbols or other elements. iii) Not confuse or detract from the application sign. iv) Not confuse or detract from the purpose of the emblem/logo i.e. not include a warning word or message.	Placing emphasis upon an emblem/logo design which is capable of crossing language boundaries.	There is a need for rapid/instant recognition of the emblem/logo without reading text. Provisions for the emblem/logo to appear on simple or small electronic displays which cannot display text within an emblem/logo and yet still read by the majority of the public. Provisions for emblem/logo use for the purpose of public notification for technologies similar to RFID but not RFID.
E.8	What information?	No information provided on the logo/emblem should be **essential** to the logo/emblem meeting the requirements for public notification.	1) Mention of "RFID" is the only possible exception and if necessary. 2) As mentioned above where necessary the addition of a text, symbols or other elements to differentiate between multiple application specific features described through the RFID sign or signs is possible.	Presence of information makes it an RFID sign (See RFID Sign below).	Information on the emblem/logo should be strictly limited to avoid message conflict with the RFID sign. If any information is present on the emblem/logo this has to be present only to create a clearer association with an RFID sign (or element within the sign) e.g. two RFID systems, or different RFID tags, or different applications in the immediate same area where one emblem/logo is differentiated from another to refer to different RFID signs (or different elements of the same sign) describing the two applications.

Ref.		Primary	Secondary	Further Information	Additional Comments
E.9	What communicat-ion medium?	Visual: 1) Printed (all forms of printing). 2) Electronic display. i) Fixed at the location. a) Moderate or high resolution. b) Low resolution. ii) Mobile wireless device.	Touch: 1) Embossed. 2) Braille. Not audible signal.	Need for "Touch" optional as: 1) There is no suitable supporting existing comparable reference. And RFID systems themselves pose no known risk to health. 2) Could be an advantage where RFID is used in an application for visually impaired to assist the individual bring into proximity tag (tagged item) and RFID interrogator e.g. enabling audible RFID sign information about tagged item or tagged shelf "Size S, red T-shirt", etc..	Mobile wireless devices may display an RFID emblem/logo on their electronic screen when an RFID applica This creates a number of demands upon the public in matching emblems/logos with corresponding signs or information elements within one sign, which is complex and demanding for the public to follow easily. tion or RFID device within the mobile wireless device is activated e.g. RFID interrogator and application opened in smart phone (in a similar fashion to "Bluetooth" activation).
E.10	Linking to?	RFID Signs (see below)	Avoiding confusion with existing popular logos/emblems/signs: 1) European Privacy Seal. 2) EPCglobal emblem. 3) ISO RFID Emblem. 4) RFID Passport Logo. 5) NFC Logo. 6) WiFi Logo. Etc.?	It is important that the emblem/logo is: 1) Capable of fulfilling the purpose of notification alone. 2) Distinguishable from other emblems/signs when positioned next to one or more. 3) Maximizing it's positive influence on other related/associated emblems/logos which are likely to be displayed in the vicinity.	

Ref.		Primary	Secondary	Further Information	Additional Comments
E.11	Accessibility of technical specification/ guidance notes?	1) No restrictions to accessibility. i) No licence fee, royalties or, other charges associated with the use of the technical specification, guidance notes or any other similar documents. ii) Unrestricted ready availability of technical specifications / application notes / guidance notes 24h/7d. iii) Available in local languages of individual European Member States.			Should be low cost to promote adoption.
E.12	Quality?	Should be defined in terms of measurable parameters to promote consistency.			Conformance requirements TBD.

E.2.2 Location and Placement

Ref.		Primary	Secondary	Further Information	Additional Comments
EL.1	When?	The signage has to be presented to the general public at any location where an RFID system, RFID device or application is or may be operated, installed or present.		A sign or signs are **not necessary** where an RFID field is measurably present or may be present, where there is no RFID system or application installed or operated in the area. This exception **is not permitted** when there is an association or exchange of information between: 1) The owner/ operator of any RFID system or application which projects an RFID electromagnetic field into the area and, 2) The area owner or lessee of the area.	The exception described in further information is there to avoid an obligation on the operator to places signs in areas where they may have no legal access rights to place an RFID sign. For example where the operation of and RFID interrogator system can activate tags outside the perimeter of the premise the RFID interrogator system is installed in.

Ref.		Primary	Secondary	Further Information	Additional Comments
EL.2	Where?	Europe: The RFID emblem/logo design is intended to be suited to placement at the following locations: 1) All locations whether public or not and, where individuals may encounter or interact with RFID systems or applications. 2) Located at the entrances to facility, buildings or bounded areas where RFID systems, RFID devices or, RFID applications are or maybe present or operated. 3) Located on RFID signs to ensure clear association between the two. See RFID signs for more details. 4) Where product or product component(s) is tagged the RFID emblem/logo is to be present on the product or product attached label or product packaging and any product instruction literature (whether presented electronically or printed). 5) Where product labels or product packaging or product transport packaging is tagged the RFID emblem/logo is to be printed on either or both the product attached label or product packaging. 6) Located on shelves or in the near vicinity of hanger rails where tagged products are to be presented. 7) Located on products, product packaging, product labels or instruction literature (whether presented electronically or printed) where the product contains one or more RFID interrogators. 8) On the Web site of organizations producing or handling or operating RFID devices or applications.	Worldwide: Suitable to encourage: 1) Use of the RFID emblem/logo in a way consistent with Europe. 2) Use on advertising and promotional material where this is associated with tagged product, tagged product packaging, tagged labels or tagged shipping containers.	1) Guidance will be provided to support to consistent locations of product marking. 2) Specifications will be provided for locating emblems/logos on shelves, rails, entrances, walls, etc. 3) Defined measure for proximity to other emblems/logos and signs. 4) Where tagged product, product packaging or product labels are all small (max. size TBA) then the RFID emblem/logo is to be displayed on the associated display shelf only. 5) Any organization embedding RFID devices in products is to ensure that: i) Where they do not provide the product packaging it is important that the transport packaging, all associated paperwork includes an RFID emblem/logo to notify the receiver of the presence of RFID devices within the product. ii) Where they do provide the product packaging that the RFID emblem/logo is included on the product packaging. iii) The product is marked with the RFID emblem/logo.	1) The Common European RFID emblem/logo has to be positioned above or to the left of any other emblem/logo associated with RFID (giving precedence for normal reading direction of left to right, and top to bottom). 2) Has to be placed below or to the right of any: Privacy seal, National or Royal flag or emblem, etc. (in the precedence norm for normal reading direction of left to right, and top to bottom). 3) The RFID emblem/logo may be used to indicate where the RFID tag or, RFID interrogator or, RFID interrogator antenna is located for the purpose of assisting the removal or physical disabling and/or removal of the device. This is **not mandatory,** as there are circumstances where such placement could assist criminals. In fact careful consideration should be given to use of the RFID emblem/logo for such a purpose following "privacy & security by design." 4) Reference to tagged shipping packaging or containers are included to ensure that wholesale or bulk purchased or, re-used boxes, etc., that these are not invisible to the public.
EL.3	How often should the emblem/ logo be repeated?	1) Recommended minimum once on the RFID sign. 2) Recommended no maximum ceiling restriction.	1) Recommended once: i) At entrances (see EL.2, 2 above). ii) In all other situations (see EL.2 1-8 above.	To comply with the RFID Recommendation the RFID sign (below) must be present. The RFID sign must include the RFID emblem/logo.	To be included in the RFID emblem/logo future standard.

E.2.3 Other Requirements

Ref.		Primary	Secondary	Further Information	Additional Comments
EO.1	Maintenance?	It is: 1) The RFID system and/or application operator's responsibility to maintain the RFID emblem/logo ensuring the RFID sign: i) Has the correct references. ii) Accurately associates with the RFID system and RFID application. iii) Is readable and in an adequate state to fulfil the purpose. 2) The responsibility of anyone applying RFID tag labels to ensure that the relevance and quality of the RFID emblem/logo is maintained.		Such maintenance processes should be defined and the activities recorded in support of quality procedures.	All post RFID emblem/logo labelling or packaging processes have to be defined in order not to mask the RFID emblem/logo.
EO.2	Conformance?	It is the responsibility of the producer of the RFID emblem/logo to ensure it conforms to the appropriate standards.		Conformance requirements are to be made clear within the common European RFID related standards.	

E.3 RFID Sign classified requirements

E.3.1 General Requirements Specification

Ref.		Primary	Secondary	Further Information	Additional Comments
S.1	What is the overall goal?	Build public trust through widespread RFID application visibility by: 1) Providing the public an opportunity to be consistently and correctly informed about RFID related applications or the presence of RFID devices. 2) Providing link to and support to RFID emblem/logo.	1) Inform employees: i) For information. ii) Reinforce consistent correct/intended use of the RFID system and RFID application.	Must be understandable to a broad cross section of the general population or cross section of the population coming into regular contact with the RFID sign.	Actions necessary for the public to seek more information about the RFID application must be consistently presented on RFID signs and, detailed in the RFID sign standard.
S.2	What is the purpose?	Delivery of information of public interest related to: 1) Fulfilling RFID Recommendation. 2) Applications associated with RFID systems or RFID system devices. 3) Supporting the RFID Logo/Emblem.	1) Public notification. 2) Public information. 3) A deterrent to property theft.	Building trust in the: 1) Application(s), 2) Owner/operator. 3) Technology. Can be used in place of RFID logo/emblem but the RFID logo/emblem must also be present on the RFID sign.	The RFID sign may for example describe that the presence of tags is associated with no known RFID systems operated within the facility/area.

Ref.		Primary	Secondary	Further Information	Additional Comments
S.3	Who is the target for the message presented by the sign?	1) General Public: i) All ages. ii) All local nationals. iii) All national cultures.	1) General Public: i) All abilities. 2) Employees	Where all abilities refers to educational attainment and physical abilities (e.g. blind, etc.). The RFID sign can be presented in Braille or acoustically so as to be accessible to visually impaired. There is no strict precedent for such an approach to be a mandatory requirement as RFID is not associated with a known hazard or danger to health. However where the application is expressly designed for the visually impaired these approaches should be considered as highly recommended.	
S.4	What information?	1) The RFID emblem/logo must be visibly present on the sign. 2) Name and contact details of the operator of the RFID system or application. 3) Name and contact details of the principle point of contact capable of furnishing further information in situations where there are or may be RFID devices (e.g. tags, or interrogators, interrogator antenna, etc.) present but not used in any RFID system or application at the location. 4) Title of the application(s).	Application related information with mention of or, reference to: 1) Application benefits or motivation supporting the application's adoption. 2) The nature of the information being collected or processed. 3) The Privacy Impact Assessment (PIA) associated with the application. 4) Links to other sources of information relevant to the application. 5) Mention of any potential challenges to individuals and how to avoid or minimize them. 6) Technology explanation. 7) Contact details of local DPA.		The principle objective is to provide the general public information about the application and paths "for individuals to follow in order to obtain the information policy for the application". It is not to make the general public experts in technology.

Ref.		Primary	Secondary	Further Information	Additional Comments
S.5	What communicat-ion medium?	Either or any combination of the following: 1) Printed. i) Fixed sign/poster. ii) Flyer. (Must have permanent back-up). 2) Electronic display. i) Fixed at the location. a) Moderate or high resolution. b) Low resolution. ii) Mobile wireless device. 3) Projection. 4) Sound.	Optionally: 1) Braille. 2) Acoustically delivered verbal message.	Avoiding confusion with existing popular logos/emblems/ signs. There is no strict precedent for the use of Braille for it to be a mandatory requirement as RFID is not associated with a known hazard or danger to health.	Multiple media formats will be necessary and must support intention to inform all.
S.6	What form?	Either or any combination of the following: 1) Text. 2) Diagrams. 3) Video. 4) Acoustically delivered verbal message.	Optionally: 1) Braille. 2) Acoustically delivered verbal message.	Signs should be comprehensive, unambiguous, uniform and standard compliant.	
S.7	What information source?	Either or any combination of the following: 1) Printed sign. 2) Web page. 3) 2D bar code. 3) Electronic memory: i) Contact memory (e.g. USB stick). ii) Contactless electronic memory device (e.g. RFID).	Optionally: 1) Braille. 2) Acoustically delivered verbal message.		2D bar codes allows i-Phone and other Smart Phone users today to upload the information into their phone without connection to the Internet.
S.8	Accessibility of technical specification /guidance notes?	1) No restrictions to accessibility. i) No licence fee, royalties, or other charges associated with the use of the technical specification, guidance notes or any other similar documents. ii) Unrestricted ready availability of technical specifications/ application notes / guidance notes 24h/7d. iii) In local languages of Member States.			Should be low cost to promote adoption.
S.9	Quality?	Should be defined in terms of measurable parameters to promote consistency.		Conformance requirements to be built into RFID sign standard(s).	

E.3.2 Location and Placement

Ref.		Primary	Secondary	Further Information	Additional Comments
SL.1	When?	Must 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.	Can also be present on web sites, literature, etc. of organizations who are or are intending to produce, handle or operate RFID systems, devices or applications.	Not necessary where an RFID field exists or may exist but where there is no RFID system, RFID devices or RFID application installed, present or operated in the area. This exception is not permitted when there is an association or exchange of information between the owner/operator of any RFID system or RFID application projecting into the area and, the area owner or lessee of the area.	
SL.2	Where?	Europe: The RFID sign must be suited to placement at the following locations: 1) All locations whether public or not and, where individuals may encounter or interact with RFID systems or applications. 2) Located within facilities, buildings or bounded areas where RFID systems, RFID devices or, RFID applications are or maybe present or operated. 3) Where product or product component(s) is tagged the RFID sign is to be present on the product instruction literature whether this is presented electronically or printed. 4) Located in the vicinity of shelves or in the near vicinity of hanger rails where tagged products are to be presented to the public. 5) Located on product literature (whether presented electronically or printed) where the product contains one or more RFID interrogators. 6) On the Web site of organizations intending to or in the process of producing or handling or operating RFID devices or applications.	Worldwide: Suitable to encourage: 1) Use of the RFID sign in a way consistent with Europe.	1) Guidance will be provided to support harmony in the selection of RFID sign locations. 2) Specifications will be provided for the layout of information within the RFID sign. 3) Guidance measures for the proximity for RFID signs to RFID emblems/logos.	

Ref.		Primary	Secondary	Further Information	Additional Comments
SL.3	How often should the emblem/ logo be repeated?	1) Minimum once: i) In the vicinity of RFID emblems/logos at locations accessible to the public.		Where there are multiple RFID applications in the area it is considered preferable that the RFID signs describes the multiple applications and, avoids encouraging a different RFID sign for each application. The RFID sign standard needs to provide for the description of multiple RFID applications in a consistent manner.	

E.3.3 Other Requirements

Ref.		Primary	Secondary	Further Information	Additional Comments
SO.1	Maintenance?	It is the RFID system or RFID application operator or owner/lessee of the area to maintain the sign ensuring the RFID sign: 1) Has the correct references. 2) Describes the application accurately. 3) Is readable and in an adequate state to fulfil the purpose.		Such maintenance processes should be defined and the activities recorded in support of quality procedures.	
O.2	Conformance?	It is the responsibility of the owner of the RFID sign to ensure it conforms to the appropriate standards.		Conformance requirements are to be made clear within the common European RFID related standards.	

Annex F:
Review of security analysis issues in PIA

From the list of RFID-related emerging issues identified in the main body of the present document the following additional analysis of issues arising is given. This covers the following areas:

- data mining and profiling;
- smart technologies/applications - referring to technology convergence (e.g. RFID used in conjunction with GPS, sensor technology, etc.);
- internet of things/ambient intelligence - referring to things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts;
- protection and rights of vulnerable individuals, including minors;
- workplace privacy - in relation to using RFID to track and/or trace activities of employees;
- tracking by proxy - referring to the possibility of inferring the identity of an individual through an RFID- tagged item belonging to the individual;
- corporate espionage - where the misuse of personal data acquired by means of RFID tampering or illegal access is not the purpose, but rather the means to acquire other economic, competitive advantage, etc.

Table F.1: Data protection requirements

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure
automatic or manual processing of data	the (technical) means employed to collect, store, use, exchange, collate or otherwise change, destroy data	technical or human errors that might occur in the course of processing data, illicit processing of data, etc.	all	PETs, authentication and authorization, Training of personnel
purpose specification	what information is collected, for what purpose and through which technical means. Collection of personal data exclusive to fulfil a specific purpose. Re-use for an incompatible purpose; (see clause 5 for details)	function creep behavioural targeting	all	explicit notification to and consent from citizen/consumer for data collection and use purpose; renewed notification and consent for every change in the original purpose.
collection and use limitation, minimization	the length of time for which the data is kept and the amount of data should not exceed the period of time necessary to fulfil the purpose for which it was collected	retention period and use of data exceeds the period of time necessary and purpose for which it was collected profiling, etc. see clause A.2 and clause 5.	Backend system	automatic deletion or disabling of information according to fulfilment of some parameter (time, period, action, event)
data quality	the syntactic and semantic quality of the data collected, stored or otherwise processed, including the length of time for which the data is kept	limited user control poor data quality incorrect personal information incorrect aggregation of data	tag, backend database, other components in RFID backend system	data integrity checks and mechanisms to detect and discharge poor quality data based on both syntactical and semantic validations
transparency, openness	the right to know that a product contains a tag; that the tag stores personal data; when a tag is being read and why; that data relating directly or indirectly to an individual is being stored in a database	details are in clause 5	tag, interrogator, backend system	user notification; emblems and signage, etc.
rights of data subjects	the right to information, correction, removal; right to object to the processing of personal data (except when collected to comply with a legal obligation or perform an agreed to contract, or for which informed, meaningful, explicit and unambiguous consent has been given) contact information for queries and complaints;	use of data without consent; inaccurate data stored in backend databases, limited access to products and services	all	regulatory measures
security safeguards	appropriate measures to be taken by service providers to safeguard the security of their systems, prevent unauthorized access to data, prevent misuse of data, etc.	overview of threats are given in Annex C	all	encryption of data on tag, shielding, authentication and authorization, anonymization, etc.

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure
third party transfer/processing	sharing and disclosure of (personal) data with/to third parties only if necessary to fulfil any of the original purposes for which the data was collected in the first place; no transfer, sharing, etc. of data for advertising or direct marketing purposes	details are in Annex C	backend system (databases)	regulation
third-country transfer	transfer to countries outside the EU (i.e. third countries) is subject to special conditions: informed, meaningful, explicit and unambiguous consent of the data subject; for the performance of (pre)contractual obligations; for law enforcement purposes; for the protection of the vital interest of the data subject; transfer from a public register	absence of (comparable) privacy standards and safeguards, etc.	backend system (databases)	regulation
accountability	1. assigning responsibility for compliance with overall privacy and data protection requirements; 2. Measurement and monitoring of fulfilling these responsibilities and potential compliance; 3. Redress measures	failure to notice incidents, failure to notify individuals affected, failure to offer redress solutions, failure to prove compliance, etc.	all	activity logging protocols and practices (authentication, authorization, controls, incident reporting, etc.);audit protocols independent supervisory body

The privacy requirements captured in Table F.2, including requirements related to consumer/citizen issues, cover issues related to citizen/consumer awareness and behaviour issues; the contextual character of privacy in its several meanings; as well as issues related to other dimensions of privacy: spatial, temporal, bodily and behavioural privacy.

Table F.2: Privacy requirements

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure
consumer awareness	low public awareness of RFID technology	no informed, meaningful, explicit and unambiguous consent possible effectively no user control, etc.	tag, interrogator, backend system	information campaign, logos and signage, regulation
consumer behaviour	refers to the privacy paradox: disjunction between opinions held re privacy and behaviour (trade-off privacy-various advantages the consumer/citizen stands to gain in exchange for sharing his personal data)	profiling, tracking. More information in Annex C	all	regulation, use of pseudonyms, encryption, use of session id rather than tag identity, etc.
spatial (location) and temporal dimension of privacy	refers to the location of an individual at a discrete point in time and over a continuous period of time	unwanted disclosure of location; real-time tracking and monitoring; real-time surveillance; association between individuals, etc.	all	regulation, encryption, use of pseudonyms, use of session id rather than tag identity, silence of the chip, etc.
bodily dimension of privacy	refers to the integrity of the individual's body	tags on body and implants monitoring bodily functions, etc.	tag, interrogator	regulation, shielding, controlled readings, encryption, use session id rather than tag identity, etc.
behavioural privacy	refers to individual's activity and preference patterns, both explicit and implicit	Profiling		Regulation of implementaion, pseudonyms, use of session id rather than tag identity etc.
contextual character of privacy - multiple meanings	a) citizen/consumer privacy perceptions depend strongly on the context: surveys indicate that certain types of personal data are likely to be regarded as more sensitive than others (financial data, medical data)	undesirable, possibly harmful, disclosure of sensitive information (more information is given in Annex C)	tag, interrogator, backend database	regulation, encryption, pseudonyms, anonymization, etc.
	b) compounded (personal) data can acquire a different value and meaning	behavioural data used for profiling, etc.	tag, interrogator, backend database	regulation, encryption, pseudonyms, minimizing of data, procedures for deletion and deactivation of information, etc.
	c) (personal) data can acquire a different value and meaning if used in a different context than the one for which it was originally processed	function creep, etc.	interrogator, backend system	regulation, purpose specification, automatic expiry date for data, etc.

Table F.3 presents emerging data protection and privacy issues and requirements related to emerging or future applications, technologies, etc. involving RFID. These new developments are expected to bring about new categories of challenges to individual privacy and data protection and might refer to one or a combination of the categories mentioned in Tables 3, 4 and Annex C.

Table F.3: Emerging issues

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure
data mining and profiling	data mining refers to the use of analytical techniques to reveal patterns, trends and profiles from sets of data. Profiling is "a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics"	details are given in Annex C	backend database, and other backend system components	encryption, anonymisation, deletion and deactivation regulations and procedures, use of pseudonyms, use of session id rather than tag identity, etc.
smart technologies/application	through technology convergence (e.g. RFID used in conjunction with GPS, sensor technology, etc.) new and innovative uses of RFID enabling broader aggregation of information across domains/applications and more detailed profiling	see Annex C	all	randomisation of data, shielding, minimizing of data, control of purpose, consumer awareness, logos and signage, etc.
internet of things/ambient intelligence	things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts	limited or no individual autonomy and control, lack of consumer awareness, can lead to undesired disclosure of information personal data	all	consumer awareness, encryption, authentication and authorization, pseudonyms, etc.
protection of minors	the current legislation does not include explicit provisions for the protection of privacy and data of children	children's rights issues (e.g. in relation to parental RFID track and trace tagged items), etc.	all	consumer awareness, regulations, parental control, encryption, anonymization, pseudonyms, etc.
workplace privacy	1) onsite: use of RFID for employee identification and access purposes, computer use, etc. 2) offsite: in the context of a growing mobile workforce and home workers	blurring of the boundaries between the private and public spheres, tracking and tracing, disclosure of personal data, profiling, etc.	all	consumer/citizen awareness, regulations, signs and logos, use of pseudonyms, etc.
corporate espionage	unauthorized access to customer performance	unauthorized access to customer performance, etc.	all	security safeguards, architecture solutions (privacy by design), etc.

Annex G: Bibliography

G.1 Books

The following books give some background to the topics of privacy and security in the use and deployment of RFID.

"Security in RFID and Sensor Networks (Wireless Networks and Mobile Communications)"; Editor(s): Yan Zhang, Paris Kistos; Publisher: Auerbach Publications; ISBN-10: 1420068393, ISBN-13: 978-1420068399.

"How to Cheat at Deploying and Securing RFID"; Author(s): Paul Sanghera, Brad Haines; Publisher: Syngress; ISBN-10: 1597492302, ISBN-13: 978-1597492300.

"RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Identification and NFC (Near Field Communication)"; Author: Dr. Klaus Finkenzeller; Publisher: WileyBlackwell; ISBN-10: 0470695064, ISBN-13: 978-0470695067.

G.2 GRIFS database extract

NOTE: The extract from GRIFS below was made on November 29th 2010 and is accurate as of that date.

Title	Area of application	Publisher	Status	Date of publication
1999/519/EC	Health and Safety regulations	European Council Recommendation	Published	1999
2002/58/EC	Data protection and privacy regulations	EC Directive	Published	2002
2002/95/EC [Draft note: ETSI has this as 2002/96/EC, which is correct]	Environmental regulations (e.g. WEEE, packaging waste)	EC Directive	Published	2002
2002/96/EC [Draft note: ETSI has this as 2002/95/EC, which is correct]	Environmental regulations (e.g. WEEE, packaging waste)	EC Directive	Published	2002
2004/40/EC	Health and Safety regulations	EC Directive	Published	2004
2005/83/EC	Frequency regulations	EC Directive	Published	2005
2006/771/EC	Frequency regulations	Commission Decision	Published	2007
2006/804/EC	Frequency regulations	Commission Decision	Published	2007
2007/344/EC	Frequency regulations	Commission Decision	Published	2007
2007/346/EC	Frequency regulations	Commission Decision	Published	2007
494-522; Health Physics 74 (4)	Health and Safety regulations	ICNIRP	Published	2005
ALE-v1.1 - Part 1: Core	Data encoding and protocol standards (often called middleware)	EPCglobal	Published	2008
ALE-v1.1 - Part 2: XML and SOAP bindings	Data encoding and protocol standards (often called middleware)	EPCglobal	Published	2008

Title	Area of application	Publisher	Status	Date of publication
AN ACT Relating to electronic communication devices; addingInew...	Data protection and privacy regulations	Washington State Legislature, USA	Published	2008
Class 1 Generation 2 UHF Air Interface Protocol Standard v1.2.0	Air interface standards	EPCglobal	Published	2008
DCI Standard	Device interface standards	EPCglobal	In development	
Dynamic Test: Conveyor Portal Test Methodology, version 1.1.4	Conformance and performance standards	EPCglobal	Published	2006
Dynamic Test: Door Portal Test Methodology, version 1.1.9	Conformance and performance standards	EPCglobal	Published	2006
EN 50357	Health and Safety regulations	CENELEC	Published	2001
EN 50357:2001	The European Harmonisation procedure	CENELEC	Published	2001
EN 50364	Health and Safety regulations	CENELEC	Published	2001
EN 50364:2001	The European Harmonisation procedure	CENELEC	Published	2001
EPC Information Services Standard v1.0.1	Data exchange standards and protocols	EPCglobal	Published	2007
ETSI EN 300 220-1 V2.1.1 (2006-04)	Frequency regulations	ETSI	Published	2006
ETSI EN 300 220-2 V2.1.1 (2006-04)	Frequency regulations	ETSI	Published	2006
ETSI EN 300 330-1 V1.5.1 (2006-04)	Frequency regulations	ETSI	Published	2006
ETSI EN 300 330-2 V1.3.1 (2006-04)	Frequency regulations	ETSI	Published	2006
ETSI EN 300 440	Frequency regulations	ETSI	Published	2009
ETSI EN 300 440	Frequency regulations	ETSI	Published	
ETSI EN 300 674	Frequency regulations	ETSI	Published	2004
ETSI EN 300 761	Frequency regulations	ETSI	Published	2001
ETSI EN 300 761	Frequency regulations	ETSI	Published	2001
ETSI EN 301 489	Frequency regulations	ETSI	Published	2002
ETSI EN 301 489	Frequency regulations	ETSI	Published	2008
ETSI EN 302 208-1 V1.1.2 (2006-07)	Frequency regulations	ETSI	Published	2006
ETSI EN 302 208-2 V1.1.1 (2004-09)	Frequency regulations	ETSI	Published	2004
ETSI ETS 300 683	Frequency regulations	ETSI	Published	1997

Title	Area of application	Publisher	Status	Date of publication
ETSI TR 101 445	Frequency regulations	ETSI	Published	2002
ETSI TR 102 378	Frequency regulations	ETSI	Published	2005
ETSI TR 102 436 V1.1.1 (2005-12)	Frequency regulations	ETSI	Published	2005
ETSI TR 102 649-1	Frequency regulations	ETSI	Published	2007
ETSI TS 102 190	Frequency regulations	ETSI	Published	2003
ETSI TS 102 562	Frequency regulations	ETSI	Published	2007
European Parliament and Council Directive 94/62/EC	Environmental regulations (e.g. WEEE, packaging waste)	EC Directive	Published	1994
Guidelines for Using RFID Tags in Ontario Public Libraries	Data protection and privacy regulations	Information and Privacy Commissioner, Ontario, Canada	Published	2004
IEC 60601-1-2	Health and Safety regulations	IEC	Published	2007
IEC 62369	Health and Safety regulations	IEC	Published	2008
IEC 62369	Health and Safety regulations	IEC	Published	2008
IEC 62369-1 Ed.1	The European Harmonisation procedure	IEC	Published	2008
IEEE 1451.5-2007	Wireless Network Communications	IEEE Standards Association	Published	2007
IEEE802.15.4-2006	Wireless Network Communications	IEEE Standards Association	Published	2006
IEEE802.15.4a-2007	Wireless Network Communications	IEEE Standards Association	Published	2007
IEEE802.15.4c	Wireless Network Communications	IEEE Standards Association	In development	
IEEE802.15.4d	Internet Standards	IEEE Standards Association	In development	
IETF BCP 115 (= RfC 4395)	Internet Standards	The Internet Society	Published	2006
IETF BCP 40 (= RfC 2870)	Internet Standards	The Internet Society	Published	2000
IETF BCP 65 (= RfC 3405)	Internet Standards	The Internet Society	Published	2002
IETF BCP 66 (= RfC 3406)	Internet Standards	The Internet Society	Published	2002
IETF RFC 2181	Internet Standards	The Internet Society	Published	1997
IETF RFC 2671	Internet Standards	The Internet Society	Published	1999
IETF RFC 3044	Internet Standards	The Internet Society	Published	2001
IETF RFC 3061	Data exchange standards and protocols	The Internet Society	Published	2001
IETF RFC 3187	Internet Standards	The Internet Society	Published	2001
IETF RFC 3188	Internet Standards	The Internet Society	Published	2001
IETF RFC 3403	Internet Standards	The Internet Society	Published	2002
IETF RFC 3650	Data exchange standards and protocols	The Internet Society	Published	2003
IETF RFC 3651	Data exchange standards and protocols	The Internet Society	Published	2003
IETF RFC 3652	Data exchange standards and protocols	The Internet Society	Published	2003
IETF RFC 4122	Internet Standards	The Internet Society	Published	2005

Title	Area of application	Publisher	Status	Date of publication
IETF RFC 4729	Internet Standards	The IETF Trust	Published	2006
IETF RFC 4919	Wireless Network Communications	The IETF Trust	Published	2007
IETF RFC 4944	Wireless Network Communications	The IETF Trust	Published	2007
IETF RFC 5134	Data exchange standards and protocols	The IETF Trust	Published	2008
IETF STD 1 (= RfC 5000)	Internet Standards	The Internet Society	Published	2008
IETF STD 13 (= RfC 1034)	Internet Standards	The Internet Society	Published	1987
IETF STD 13 (= RfC 1035)	Internet Standards	The Internet Society	Published	1987
IETF STD 62 (= RfC 3411)	Internet Standards	The Internet Society	Published	2002
IETF STD 62 (= RfC 3412)	Internet Standards	The Internet Society	Published	2002
IETF STD 62 (= RfC 3413)	Internet Standards	The Internet Society	Published	2002
IETF STD 62 (= RfC 3414)	Internet Standards	The Internet Society	Published	2002
IETF STD 62 (= RfC 3415)	Internet Standards	The Internet Society	Published	2002
IETF STD 62 (= RfC 3416)	Internet Standards	The Internet Society	Published	2002
IETF STD 62 (= RfC 3417)	Internet Standards	The Internet Society	Published	2002
IETF STD 62 (= RfC 3418)	Internet Standards	The Internet Society	Published	2002
IETF STD 66 (= RfC 3986)	Internet Standards	The Internet Society	Published	2005
Interoperability Test System for EPC Compliant Class-1 GenItion-2...	Conformance and performance standards	EPCglobal	Published	2006
ISO 17363:2007	Application standards	ISO	Published	2007
ISO CD 26324	Data exchange standards and protocols	ISO	In development	
ISO-IEC 9834-1	Data exchange standards and protocols	ISO	Published	2005
ISO-IEC 9834-9	Data exchange standards and protocols	ISO	Published	2008
ISO/DIS 17364	Application standards	ISO	In development	
ISO/DIS 17365	Application standards	ISO	In development	
ISO/DIS 17366	Application standards	ISO	In development	
ISO/DIS 17367.2	Application standards	ISO	In development	
ISO/DIS 28560-1	Application standards	ISO	In development	
ISO/DIS 28560-2	Application standards	ISO	In development	
ISO/DIS 28560-3	Application standards	ISO	In development	
ISO/IEC 15434:2006	Data standards	ISO/IEC	Published	2006
ISO/IEC 15961:2004	Data encoding and protocol standards (often called middleware)	ISO/IEC	Published	2004
ISO/IEC 15962:2004	Data encoding and protocol standards (often called middleware)	ISO/IEC	Published	2004
ISO/IEC 18000-1:2008	Air interface standards	ISO/IEC	Published	2008
ISO/IEC 18000-2:2004	Air interface standards	ISO/IEC	Published	2004
ISO/IEC 18000-3:2004	Air interface standards	ISO/IEC	Published	2004
ISO/IEC 18000-4.1	Air interface standards	ISO/IEC	Published	2008
ISO/IEC 18000-4:2004	Air interface standards	ISO/IEC	Published	2004

Title	Area of application	Publisher	Status	Date of publication
ISO/IEC 18000-6:2004	Air interface standards	ISO/IEC	Published	2004
ISO/IEC 18000-6:2004/Amd 1:2006	Air interface standards	ISO/IEC	Published	2006
ISO/IEC 18000-7:2008	Air interface standards	ISO/IEC	Published	2008
ISO/IEC 18046-3	Conformance and performance standards	ISO/IEC	Published	2007
ISO/IEC 21481	Mobile RFID	ISO	Published	2005
ISO/IEC 24730-1:2006	Real time location standards	ISO/IEC	Published	2006
ISO/IEC 24730-2:2006	Real time location standards	ISO/IEC	Published	2006
ISO/IEC 28361	Mobile RFID	ISO	Published	2007
ISO/IEC CD 15961-1	Data encoding and protocol standards (often called middleware)	ISO/IEC	In development	
ISO/IEC CD 15961-2	Data encoding and protocol standards (often called middleware)	ISO/IEC	In development	
ISO/IEC CD 15961-3	Data encoding and protocol standards (often called middleware)	ISO/IEC	In development	
ISO/IEC CD 18046-1	Conformance and performance standards	ISO/IEC	In development	
ISO/IEC CD 18046-2	Conformance and performance standards	ISO/IEC	In development	
ISO/IEC CD 24730-5	Real time location standards	ISO/IEC	In development	
ISO/IEC CD 24753	Sensor standards	ISO/IEC	In development	
ISO/IEC CD 24791-2	Data encoding and protocol standards (often called middleware)	ISO/IEC	In development	
ISO/IEC CD 24791-3	Device interface standards	ISO/IEC	In development	
ISO/IEC CD 24791-5	Device interface standards	ISO/IEC	In development	
ISO/IEC CD 29160	Data protection and privacy regulations	ISO/IEC	In development	
ISO/IEC CD TR 18047-7.1	Conformance and performance standards	ISO/IEC	In development	2010
ISO/IEC DIS 18000-6	Air interface standards	ISO/IEC	In development	
ISO/IEC DTR 18047-6.2	Conformance and performance standards	ISO/IEC	In development	
ISO/IEC DTR 24769	Conformance and performance standards	ISO/IEC	In development	

Title	Area of application	Publisher	Status	Date of publication
ISO/IEC DTR 24770	Real time location standards	ISO/IEC	Published	2008
ISO/IEC FCD 15962	Data encoding and protocol standards (often called middleware)	ISO/IEC	In development	
ISO/IEC FCD 18000-2.1	Air interface standards	ISO/IEC	In development	
ISO/IEC FCD 18000-3.2	Air interface standards	ISO/IEC	In development	
ISO/IEC FCD 18000-6	Air interface standards	ISO/IEC	In development	
ISO/IEC FCD 18000-7.2	Air interface standards	ISO/IEC	In development	
ISO/IEC FCD 24730-5	Real time location standards	ISO/IEC	In development	
ISO/IEC FCD 24791-1	Device interface standards	ISO/IEC	In development	
ISO/IEC FCD 24791-1	Data encoding and protocol standards (often called middleware)	ISO/IEC	In development	
ISO/IEC FCD 24791-5	Device interface standards	ISO/IEC	In development	
ISO/IEC FCD 24791-6	Security standards for data and networks	ISO/IEC	In development	
ISO/IEC FCD 24791-6	Device interface standards	ISO/IEC	In development	
ISO/IEC FCD 29143	Mobile RFID	ISO/IEC	In development	
ISO/IEC FDIS 29160	Data protection and privacy regulations	ISO/IEC	In development	
ISO/IEC NP 15961-4	Data encoding and protocol standards (often called middleware)	ISO/IEC	In development	
ISO/IEC NP 15961-4	Sensor standards	ISO/IEC	In development	
ISO/IEC NP 24791-2	Data encoding and protocol standards (often called middleware)	ISO/IEC	In development	
ISO/IEC PDTR 18047-6.2	Conformance and performance standards	ISO/IEC	In development	
ISO/IEC PDTR 18047-7.1	Conformance and performance standards	ISO/IEC	In development	
ISO/IEC TR 18047-2:2006	Conformance and performance standards	ISO/IEC	Published	2006
ISO/IEC TR 18047-3:2004	Conformance and performance standards	ISO/IEC	Published	2004
ISO/IEC TR 18047-3:2004/Cor 1:2007	Conformance and performance standards	ISO/IEC	Published	2007
ISO/IEC TR 18047-3:2004/Cor 2:2008	Conformance and performance standards	ISO/IEC	Published	2008
ISO/IEC TR 18047-4:2004	Conformance and performance standards	ISO/IEC	Published	2004

Title	Area of application	Publisher	Status	Date of publication
ISO/IEC TR 18047-6:2006	Conformance and performance standards	ISO/IEC	Published	2006
ISO/IEC TR 18047-7:2005	Conformance and performance standards	ISO/IEC	Published	
ISO/IEC TR 24729-4	Security standards for data and networks	ISO/IEC	Published	2009
ISO/IEC TR 24769	Real time location standards	ISO/IEC	Published	2008
ISO/IEC TR 24770	Conformance and performance standards	ISO/IEC	In development	
ITU-T F.771	Application standards	ITU-T	Published	2008
ITU-T H.621	Application standards	ITU-T	Published	2008
ITU-T H.IDscheme	Data standards	ITU-T	In development	
ITU-T H.IRP	Data exchange standards and protocols	ITU-T	In development	
ITU-T X.668 | ISO/IEC 9834-9	Data standards	ISO/IEC	Published	2008
ITU-T X.oid-res | ISO/IEC 29168	Data exchange standards and protocols	ISO/IEC	In development	
LLRP Version 1.0.1	Device interface standards	EPCglobal	Published	2007
NFC Forum RTD-URI 1.0	Mobile RFID	NFC Forum	Published	2006
NFC Forum TS-Type-1-Tag 1.0	Mobile RFID	NFC Forum	Published	2007
Object Naming Service (ONS) Standard	Data exchange standards and protocols	EPCglobal	Published	2008
prEN 50XXX-1	Health and Safety regulations	CENELEC	Published	
Revision of EN 302 208-1	Frequency regulations	ETSI	Published	2008
Revision of EN 302 208-2	Frequency regulations	ETSI	Published	2008
Revision of TR 102 436	Frequency regulations	ETSI	Published	2008
RM Standard v. 1.0.1	Device interface standards	EPCglobal	Published	2007
Tag Performance Parameters and Test Methods, Version 1.1.3	Conformance and performance standards	EPCglobal	Published	2008
UHF Class 1 Gen 2 Conformance Requirements Standard v 1.0.4	Conformance and performance standards	EPCglobal	Published	2006
[none]	Data protection and privacy regulations	Information and Privacy Commissioner, Ontario, Canada	Published	2006

G.3 Sign Related Standards

G.3.1 In development

Reference	Title
ISO 20712-1	Water safety signs and beach safety flags Part 1: Specifications for water safety signs used in workplaces and public areas.
ISO 20712-1 A2	Water safety signs and beach safety signs Part 1: Specifications for water safety signs used in workplaces and public areas.
ISO 20712-3	Water safety signs and beach safety flags Part 3: Guidance for use.
ISO 20712-1 A3	Water safety signs and beach safety signs Part 1: Specifications for water safety signs used in workplaces and public areas.
ISO 20712-1/A18	Water safety signs and beach safety signs Part 1: Specifications for water safety signs used in workplaces and public areas.
ISO 24409-1	Ships and marine-technology - Design, location, and use of shipboard safety-relted signs - Part 1: Design principles.
ISO 24409-3	Design, location, and use of shipboard safety signs - Part 3 Code of practice for means of escape, life-saving appliances, and fire-fighting equipment signs.
ISO 24502	Ergonomics - Accessible design - Specification of age-related relative luminance in visual signs and displays.
ISO 7010	Graphical symbols - Safety colours and safety signs - Safety signs used in workplaces and public areas.
ISO 7010:2003+A5	Graphical symbols - Safety colours and safety signs - Safety signs used in workplaces and public areas.
ISO 3864-2:2004/CD COR 1	Graphical symbols - Safety colours and safety signs Part 2: Design principles for product safety labels - Technical Corrigendum 1.
ISO 3864-4	Graphical symbols - Safety colours and safety signs Part 4: Colorimetric and photometric properties of safety sign materials.
ISO 11684	Tractors, machinery for agriculture and forestry, powered lawn and garden equipment - Safety signs and hazard-pictorials - General principles.

G.3.2 Published

Reference	Comment
IEC 8046-1: 2008	Provides basic principles and guidelines for the creation of graphical symbols for registration, and provides the key principles and rules for the preparation of title, description and note(s).
ISO 13200: 1995	Establishes general principles for the design and application of safety signs and hazard pictorials permanently affixed to cranes. Describes the basic safety sign formats, specifies colours for safety signs and provides guidance on developing the various panels that together constitute a safety sign.
ISO 15870: 2000	Powered industrial truck - Safety signs and hazar-pictorial - General principles.
ISO 16069: 2004	Also does not include the special considerations of possible tactile or audible components of SWGS, nor does it include requirements concerning the emergency escape route lighting, especially the design and application of emergency escape route lighting, unless illumination is used to mark safety equipment or special features of the escape route like the emergency exit doors or stairs.
ISO 20712-1: 2008	Includes water safety signs which require that supplementary text signs be used in conjunction with these water safety signs to improve comprehension.
ISO 22727: 2007	Is for use by all those involved in the commissioning and the creation and design of public information symbols. It is not applicable to safety signs, including fire safety signs, or to traffic signs for use on the public highway.
ISO 23601: 2009	Establishes design principles for displayed escape plans that contain information relevant to fire safety, escape, evacuation and rescue of the facility's occupants. These plans may also be used by intervention forces in case of emergency.
ISO 2575: 2004	Establishes symbols (i.e. conventional signs) for use on controls, indicators and telltales applying to passenger cars, light and heavy commercial vehicles and buses, to ensure identification and facilitate use. It also indicates the colours of possible optical tell-tales, which inform the driver of either correct operation or malfunctioning of the related devices.
ISO 3864-2: 2004	Establishes additional principles to ISO 3864-1 for the design of safety labels for products, i.e. any items manufactured and offered for sale in the normal course of commerce, including but not limited to consumer products and industrial equipment. The purpose of a product safety label is to alert persons to a specific hazard and to identify how the hazard can be avoided.
ISO 7010:2003	Is generally applicable to safety signs in workplaces and all locations and all sectors where safety-related questions may be posed. However, it is not applicable to the signalling used for guiding rail, road, river, maritime and air traffic and, in general, to those sectors subject to a regulation which may differ with regard to certain points of ISO 7010: 2003 and of ISO 3864-1.
ISO 9186-1: 2007	Specifies methods for testing the comprehensibility of graphical symbols. It includes the method to be used in testing the extent to which a variant of a graphical symbol communicates its intended message and the method to be used in testing which variant of a graphical symbol is judged the most comprehensible.
ISO 17724: 2003	Defines terms relating to graphical symbols, principally symbols for public information and use on equipment and safety signs. It does not include terms related to graphical symbols for diagrams (technical product documentation (tpd) symbols).
ISO 3864-1: 2002	Establishes the safety identification colours and design principles for safety signs to be used in workplaces and in public areas for the purpose of accident prevention, fire protection, health hazard information and emergency evacuation. It also establishes the basic principles to be applied when developing standards containing safety signs.
ISO 17398: 2004	Specifies requirements for a performance-related classification system for safety signs according to expected service environment, principal materials, photometric properties, means of illumination, fixing methods and surface. Performance criteria and test methods are specified in ISO 17398: 2004 so that properties related to durability and expected service life can be characterized and specified at the time of the product's delivery to the purchaser.
ISO/IEC 29160: 2010	Specifies the design and use of the RFID Emblem: an easily identified visual guide that indicates the presence of radio frequency identification (RFID). It does not address location of the RFID Emblem on a label. Specific placement requirements are left to application standards developers. It also specifies an RFID Index, which can be included in the RFID Emblem and which addresses the complication added by the wide range of RFID tags (frequency, protocol and data structure). The RFID Index is a two-character code that provides specific information about compliant tags and interrogators. Successful reading of RFID tags requires knowledge of the frequency, protocol and data structure information provided by the RFID Index.
ISO/IEC Guide 53:2005	Outlines a general approach by which certification bodies can develop and apply product certification schemes utilizing requirements of an organization's quality management system. The provisions given are not requirements for the accreditation of a product certification body and do not substitute the requirements of ISO/IEC Guide 65.

Reference	Comment
ISO/IEC Guide 74: 2004	Does not cover road traffic signs and graphical symbols for use in technical documentation.
ISO/TS 14823: 2008	Presents a system of standardized codes for existing signs and pictograms used to deliver traffic and traveller information (TTI). The coding system can be used to form messages to be handled by respective media systems, graphic messages on on-board units, and media system information on TTI dissemination systems [variable message signs (VMS), personal computers (PC), public access terminals (PAT), etc.] (including graphic data).

G.4 Other references

ETSI TS 187 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Protection (Protection Profile)".

ETSI TS 102 359: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Equipment Information in the Management Information Base (MIB)".

ETSI TS 102 209: "Telecommunications and Internet converged Services and Protocols for Advancing Networks (TISPAN); Telecommunication Equipment Identification".

ITU-T Recommendation M.1400 (2004): "Designations for interconnections among operators' networks".

ITU-T Recommendation M.3320: "Management requirements framework for the TMN X-Interface".

Terms of Reference for Specialist Task Force STF 396 (CEN/CENELEC/ETSI) "Response to Phase 1 of EC mandate M/436 (RFID)"SA/ETSI/ENTR/436/2009-02.

EC, Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. (Text with EEA relevance).

UK Home Office; R. V. Clark; "Hot Products: understanding, anticipating and reducing demand for stolen goods", ISBN 1-84082-278-3.

ISO/IEC 27002 (2005): "Information technology - Security techniques - Code of practice for information security management".

ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

AS/NZS 4360: "Risk Management".

Directive 2002/21/EC of the European Parliament and of the council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal service and users' rights relating to electronic communications networks and services (Universal Service Directive - OJ L 108, 24.04.2002).

European Commission communication (2010) "A Digital Agenda for Europe".

ISO/IEC Guide 76 Development of service standards - Recommendations for addressing consumer issues.

Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (19.03.2010).

EC: "Charter of Fundamental Rights of the European Union".

The Royal Academy of Engineering: "Dilemmas of Privacy and Surveillance - Challenges of Technological Change", March 2007.

EP ITRE Draft report on the Internet of Things, Rapporteur: Maria Badia i Cutchet (24.02.2010).

German BSI TG 03126 - Technical Guidelines for the Secure Use of RFID.

German BSI TR 03126-2 Application area "eTicketing for events", version 1.0.

German BSI TR 03126-3 Application area "NFC based eTicketing", version 1.0.

German BSI TR 03126-4 Application area "trade logistics", version 1.0.

German BSI TR 03126-5 Application area "Electronic Employee ID Card".

German BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents - EAC, PACE, and RI, Version 2.05.

German BSI Technical Guideline TR-03111 Elliptic Curve Cryptography.

NOTE: German BSI documents are available from www.bsi.bund.de.

NIST SP 800-98 "Guidelines for Securing Radio Frequency Identification (RFID) Systems" April 2007.

International Journal of Smart Home Vol.4, No.1, January, 2010 Review: Security Threats for RFID-Sensor Network Anti-Collision Protocol.

ENISA (2010) Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology.

Giovanni Buttarelli, Assistant European Data Protection Supervisor, "Internet of things: ubiquitous monitoring in space and time", European Privacy and Data Protection Commissioners" Conference Prague, Czech Republic, 29 April 2010.

Linden Consulting, Inc., Privacy Impact Assessments: International Study of their Application and Effects, Prepared for Information Commissioner's Office United Kingdom October, 2007.

Bodea, Gabriela; Welfing, Dick and Hoepman, Jaap-Henk (2009) Towards a generic framework for Privacy Impact Assessment - an exploratory study, TNO report, Delft, 2009.

History

Document history		
V1.1.1	May 2011	Publication