

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



Reference

DTR/TISPAN-07044

Keywords

RFID; Security; Privacy**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 ☐ implemment 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/chaicor/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 yyyy.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTETM is a Trade Mark of ETSI currently being registered for the benefit of its Members and of the 3GPP Organizational Partners.

Logos on the front page

FINAL EDIT TO INCLUDE ALL ESO LOGOS ON FRONT PAGE

Contents

<i>Logos on the front page</i>	3
Intellectual Property Rights	7
Foreword.....	7
Introduction	7
1 Scope	9
2 References	9
2.1 Normative references	9
2.2 Informative references	10
3 Definitions, symbols and abbreviations	13
3.1 Definitions	13
3.2 Abbreviations.....	14
4 Summary of findings and recommendations.....	14
5 Consumer aspects including interaction.....	16
5.1 Awareness.....	16
5.2 Purpose	16
5.3 Deactivation.....	17
6 The RFID ecosystem.....	17
6.1 Overview	17
6.2 Types of RFID Tags	18
6.3 RFID Tag Characteristics	18
6.4 Stakeholders.....	19
6.5 Open and closed system applications.....	19
6.6 RFID and IoT.....	20
6.7 Regulatory protection of Identity	20
7 Analysis.....	23
7.1 RFID system architecture	23
7.2 RFID system and privacy	23
7.2.1 Modelling the role of RFID in privacy.....	25
7.3 Data Protection Objectives and Requirements.....	28
7.3.1 Statement of objectives for Data Privacy Protection.....	29
7.3.2 Statement of objectives for Security.....	35
7.4 Role of Privacy Enhancing Technologies (PETs).....	35
8 Security risk analysis of RFID systems.....	36
8.1 Security analysis and requirements derivation.....	36
8.2 Weaknesses and threats in RFID systems.....	36
8.3 Vulnerabilities in RFID systems.....	38
8.4 Attacks on RFID and associated systems	40
8.4.1 Identity spoofing	40
8.4.2 Tampering with data.....	40
8.4.3 Repudiation	40
8.4.4 Information disclosure.....	41
8.4.5 Denial of service	41
8.4.6 Elevation of privilege	41
8.4.7 Other RFID security threats	41
8.4.7.1 RF eavesdropping	41
8.4.7.2 Collision attack	42
8.4.7.3 Tracking.....	42
8.4.7.4 De-synchronization.....	42
8.4.7.5 Replay.....	42
8.4.7.6 Virus	42

9	Privacy Impact and Data Protection Assessment (PIA) outline	44
9.1	Role of PIA	44
9.2	Overview of RFID-related features with an impact on privacy	45
9.3	RFID PIA Framework	46
9.4	PIA Methodology Requirements	46
9.4.1	Assets and the RFID PIA	47
9.4.2	Scope of the PIA	47
9.4.3	General methodological requirements.....	47
9.4.4	Data Protection and Privacy requirements of the RFID PIA.....	48
9.4.4.1	Data protection requirements.....	48
9.4.4.2	Privacy requirements	49
9.4.4.3	Emerging issues and requirements related to emerging or future applications, technologies, and other issues	49
10	Common European RFID Emblem/Logo/Sign	56
10.1	Approach	57
10.2	Summary of RACE network RFID Report	58
10.3	Requirements specification	58
10.4	RFID Emblem/Logo classified requirements	59
10.4.1	General Requirements Specification	59
10.4.2	Location & Placement	63
10.4.3	Other Requirements.....	65
10.5	RFID Sign classified requirements	65
10.5.1	General Requirements Specification	65
10.5.2	Location & Placement	68
10.5.3	Other Requirements.....	70
11	Environmental aspects of RFID tags and components.....	70
11.1	Health and safety considerations	70
11.2	RFID hardware end of life considerations	71
11.3	Data end of life considerations	71
12	Standardization Gaps Analysis and Summary	71
12.1	Context for the Standards Gap analysis	71
12.1.1	Technology.....	71
12.1.2	Market growth.....	71
12.2	Gaps in current standards.....	72
12.2.1	Overview	72
12.2.2	Summary of main gaps.....	73
12.3	RFID systems structure.....	74
12.3.1	Notes on standards gaps associated with this structure	74
Annex A: Summary of status of RFID standardization.....		77
Annex B: Summary of tag capabilities		80
B.1	Command set.....	80
B.2	Security functionality	80
B.2.1	Tag embedded capabilities.....	80
Annex C: RFID Penetration Testing Standardization		83
C.1	Short Introduction to PEN testing	83
C.2	PEN testing methodologies and standards	84
C.3	RFID PEN testing standardization issues and roadmap	84
C.4	Conclusion and Recommendations	88
Annex D: Gap analysis in standardisation		89
Annex E: Bibliography.....		96
E.1	Books.....	96

E.2	GRIFS database extract.....	96
E.3	Sign Related Standards.....	96
E.3.1	In development	96
E.3.2	Published	98
History	101

Intellectual Property Rights

This clause is always the first unnumbered clause.

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.

Foreword

This Technical Report (TR) has been produced by the M436 coordination group of the European Standards Organisations (ESO) where the work item has been hosted by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) under EC/EFTA Contract reference SA/ETSI/ENTR/436/2009-02.

Introduction

RFID technology and related applications, including their application in the broader context of the Internet of Things, have been estimated to have significant potential in terms of economic and productive development, enhancing the quality of processes and services, reducing production costs and creating new employment and business opportunities.

One of the reasons that this report has been prepared is the perception of the limited attention paid to the social impact of RFID technology, including concerns over the privacy afforded to users and holders of RFID enabled objects. These concerns relate directly to the ability of RFID systems to process data, including personal data, leading to the possibility of identifying directly or indirectly individuals; to the potential of data collection and processing to take place without the individual concerned being aware of it; and to the potential use to monitor individuals via RFID tagged items in their possession.

The above mentioned concerns are likely to be exacerbated by new developments rendering the tags virtually invisible (e.g. embedded tags, subcutaneous or implanted RFID) as well as the broad range of potential application areas in both the public and private sectors. Increased tag and interrogator volumes need to be considered. The cumulative number of tags produced since the inception of the industry has been estimated at 5-6 billion with an associated installed base of interrogators. There are industry forecasts for the next 10 years (IDTechEx) showing global growth to 700 billion tags per annum which implies a cumulative number of tags globally in business public and personal use of 2-3 trillion over the next 10 years. There is some industry scepticism about this rate of growth. None the less standards underpinning privacy will have to cope with the challenge of bridging from the current technology to evolved RFID technology which will be present in our society in volumes up to 500 times greater than today's levels (based on high end estimates).

Consequently, the further development of RFID technology and the adoption of RFID-enabled applications will be linked intrinsically to the trust individuals and civil society at large have in such systems. With RFID poised to permeate all aspects of life of the individual, a concerted and consistent effort will be necessary to balance on the one hand the economic and security benefits and on the other hand the social benefits in order to generate such trust. One option is privacy by design, i.e. building the protection of privacy and other fundamental rights in technology and systems. The consumer and public perception of "Radio Frequency" raises issues of observation round corners and through materials (walls, clothes, etc.). In addition consumers associate "identification" in this technical area with themselves and their possessions being identified without their knowledge. Whilst the present document addresses one particular family of radio identification technology many of the issues and concerns identified in this report also apply to a wide range of technologies that include mobile phones (e.g. GSM, UMTS), Bluetooth, and WiFi (IEEE 802.11.x). In most consumer selected radio technologies with the exception of RFID the consumer can turn the radio function off.

With increasing convergence of technologies anticipated over the next 5 to 10 years it is fully expected that there will be hybridisation of RFID and other radio systems including WiFi and 3G. The capabilities currently understood to belong to RFID will increasingly apply to the other radio technologies and as such need to be addressed from both a functional and a technological viewpoint in order to secure consumer and public confidence and trust.

Radio Frequency Identification (RFID) is a technology that allows objects to be "tagged" with an identifier that can be read remotely using either inductive electromagnetism or emitted radio waves. The item to be read is referred to as the tag, and the item doing the reading is referred to as the interrogator. The association of tag to object is not strictly part of the RFID system but is considered as a component of the RFID ecosystem. The interrogator is itself connected to some form of back end processing, such as a logistics goods tracking application, that is also considered as a component of the RFID ecosystem, as is the connecting network. Tags may be passive (i.e. need to be powered by the interrogator) readable typically from 2 cm to 60 cm in normal operation, or active (i.e. self powered) readable from a few metres, and may include the beacon technologies used in Real Time Location Systems (RTLS) that allow items to be tracked from tens or hundreds of kilometres (including by satellite).

NOTE 1: Whilst public perception and industry announcements place the beacon technologies in RTLS as an RFID technology the scope of RFID considered in the remainder of this report does not consider RTLS and RFID as equivalent.

NOTE 2: There is a close relationship between the capabilities of RFID tags and generic transponder technologies and thus where the term tag is used it may also be read to refer to transponder.

NOTE 3: It is the tag that is read and not the object it is attached to. 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.

Typically the operation of the RF part of RFID can be summarised rather crudely by the following sequence of events for passive tags:

- Preamble that selects the tag
- Interrogator **requests** specific data from a tag

NOTE: In practical implementations of tags the read command requests data at a very low level from storage locations in the tag and the data elements understood at the application may traverse many storage locations of the tag.

- The tag responds to the read request with the specific data sent back to the interrogator

NOTE: Active and battery assisted tags modify the middle and last phase of this sequence.

The simplest overview of the ecosystem is shown in the core of the document as Figure 1, which can become increasingly complicated when details of the tagged item to tag connection are considered, and of the interconnection of interrogators to the back end system. It is expected in the future that the back end system will itself be composed of many interconnected elements (in like manner to the evolution of computing and communications).

Implementation of the RFID ecosystem itself may take many forms. The simplest form, for the purposes of the present document, is one in which all key elements (tagged items, tags, interrogator, network connections and back end systems) are under the management of a single entity. This may then be extended in any number of ways that make all key elements of the ecosystem subject to independent management with the interconnections being via public networks. It is in progress to the latter model that this document concentrates.

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 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 the need for providing a wider scope for the definition of "personal data" than exists in many current data protection interpretations; and,
- 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 document describes the results of 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).

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
 - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
 - for informative references.

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 indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- [i.1] EU 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 15963: "Information technology – Radio frequency identification for item management – Unique identification for RF tags".
- [i.5] ISO/IEC 18001: "Information technology – Radio frequency identification for item management – Application requirements profiles".
- [i.6] ISO 17363: "Supply chain applications of RFID – Freight containers".
- [i.7] ISO 17364: "Supply chain applications of RFID – Returnable transport items (RTIs)".
- [i.8] ISO 17365: "Supply chain applications of RFID – Transport units".
- [i.9] ISO 17366: "Supply chain applications of RFID – Product packaging".
- [i.10] ISO 17367: "Supply chain applications of RFID – Product tagging".
- [i.11] EPCglobal UHF Gen 2 Air interface specification
- [i.12] EPCglobal HF Gen 2 Air Interface Specification.
- [i.13] ISO/IEC 14443 "Identification cards – Contactless integrated circuit(s) cards – Proximity cards"
- [i.14] ISO/IEC 7816: "Information technology – Identification cards – Integrated circuit(s) cards with contacts"
- [i.15] ISO/IEC 15693: "Identification cards – Contactless integrated circuit(s) cards – Vicinity cards"
- [i.16] 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 management and their resolution in the NGN"
- [i.17] ETSI TS 187 016: " Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Management ..."
- [i.18] ITU-T X.200: "Information technology – Open Systems Interconnection – Basic Reference Model: The basic model"
- [i.19] ETSI TS 102 359: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Equipment Information in the Management Information Base (MIB)".
- [i.20] ETSI TS 102 209: "Telecommunications and Internet converged Services and Protocols for Advancing Networks (TISPAN); Telecommunication Equipment Identification".
- [i.21] ISO/IEC 18000 (all parts): "Information technology – Radio frequency identification for item management".
- [i.22] ITU-T Recommendation M.1400 (2004): "Designations for interconnections among operators' networks".

- [i.23] ITU-T Recommendation M.3320: "Management requirements framework for the TMN X-Interface".
- [i.24] European Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (notified under document number C(2009) 3200), Official Journal L 122 , 16/05/2009 P. 0047 – 0051
- [i.25] 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
- [i.26] 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.27] Capgemini (2005) RFID and Consumers – What European Consumers Think About Radio Frequency Identification and the Implications for Business
- [i.28] EU, 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
- [i.29] ISO/IEC 19762-1: Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part 1: General terms relating to AIDC
- [i.30] ISO/IEC 19762-3: Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part 3: Radio frequency identification (RFID)
- [i.31] ETSI EN 300 220: Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 1: Technical characteristics and test methods
- [i.32] ETSI EN 300 330: Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz; Part 1: Technical characteristics and test methods
- [i.33] ETSI EN 300 440: Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Part 1: Technical characteristics and test methods
- [i.34] ETSI EN 302 208: Electromagnetic compatibility and Radio spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W;Part 1: Technical characteristics and test methods
- [i.35] 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.36] 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.37] UK Home Office; R.V.Clark; "Hot Products: understanding, anticipating and reducing demand for stolen goods", ISBN 1-84082-278-3.
- [i.38] 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.39] ITU-T Recommendation E.164 (02/2005): "The international public telecommunication numbering plan".
- [i.40] ISO/IEC 17799 2005: "Information technology – Security techniques – Code of practice for information security management".
- [i.41] 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.42] ISO/IEC 15408-1: "Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model".
- [i.43] ISO/IEC 15408-2: "Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements".
- [i.44] AS/NZS 4360: "Risk Management".
- [i.45] 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).
- [i.46] 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).
- [i.47] 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.48] 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.49] ETSI EG 202 387
- [i.50] ETSI TR 187 011
- [i.51] European Commission communication (2010) "A Digital Agenda for Europe",
- [i.52] ISO/IEC Guide 76 Development of service standards – Recommendations for addressing consumer issues

NOTE: Available from <http://register.consilium.europa.eu/pdf/en/10/st09/st09981.en10.pdf>

- [i.51] EC, (12.5.2009) Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification SEC(2009) 585, SEC(2009) 586
- [i.532] Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (19.03.2010)
- [i.543] EC, Charter of Fundamental Rights of the European Union
- [i.54] 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)
- [i.55] The Royal Academy of Engineering . Dilemmas of Privacy and Surveillance – Challenges of Technological Change, March 2007
- [i.56] EP ITRE Draft report on the Internet of Things, Rapporteur: Maria Badia i Cutchet (24.02.2010)
- [i.55] 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

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 202 387 [i.49], ISO/IEC 17799 [i.40], ISO/IEC 13335-1 [i.41], ISO/IEC 19762-3 [], ISO/IEC 19762-1 [i.29] and the following apply:

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

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

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

identity tree: the 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: an 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

Privacy: the right of the individual to have his identity and agency 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 .

Radio interception range: the 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: the practice and science of classification

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

Threat agent: an 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 to 960 MHz.

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

NOTE 2: The UHF frequency range is defined as lying from 300MHz to 3000MHz with UHF RFID occupying a small subset of the range.

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.41], 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
AKA	Authentication and Key Agreement
BES	Back End System
CIA	Confidentiality, Integrity and Availability
CRAVED	Concealable, Removable, Available, Valuable, Enjoyable, and Disposable
CSP	Communications Service Provider
DPP	Data Privacy and Protection
IdM	Identity Management
IdP	Identity Provider
NGN	Next Generation Network
OECD	Organisation for Economic Co-operation and Development
OID	Object Identifier
PET	Privacy Enhancing Technology
PIA	Privacy and data protection Impact Assessment
RFID	Radio Frequency Identification
ToE	Target of Evaluation
TSF	TOE Security Function
TVRA	Threat Vulnerability and Risk Analysis

4 Summary of findings and recommendations

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. In addition this clause identifies the way in which the main points in the Mandate have been addressed by the study of which the present document is a report.

The main points in the document are as follows:

- Attacks on privacy in large 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 a technology such as RFID;
- 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 privacy 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;
- RFID devices may contain personal data and if so should protect that data as advised by the existing regulation (including the R&TTE directive and the current data protection directives);
- If RFID tags do not contain personal data then the remainder of the system has to give assurance that protection rules for personal data in existing regulation are complied with;

- Consent of data access 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 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 privacy is examined and the role of logos and signs 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 logos and signs documented;

NOTE 1: The present report does not contain a recommendation for the choice of logo as there is a parallel consultation on the form of the sign and logo being conducted by complimentary stakeholders and the results of the parallel consultation will be taken into account in the assessment of the results of both consultations.

NOTE 2: A similar exercise in ISO has also identified a logo which should also be taken into account, even if the associated ISO Standard is not fully applicable, as this would provide greater coherence in the use of such logos on a global scale.

- The document identifies the risks to security and privacy exposed in and by RFID systems 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.

During the consultation period some of the recommendations offered in this report may be challenged and the consultation period may lead to changes in the document. In recognising this it is noted that the document is not complete in all areas but has left areas open for the consultation process to provide insight and direction.

The EC Mandate M436 extended by the support contract under which the present document has been prepared identifies the following specific points and actions that are addressed in the present document:

1. Determine the selection of terminology by reviewing and taking into consideration M/436 and its cross referenced documents.
2. Data protection, privacy & information security SWOT analysis of RFID resulting in the highlighting a hierarchy of technology, existing standards work, and standards gaps in relation to all aspects of RFID & including the networking of tags. A documented summary of the study will contribute to the recommended standardization work programme.
3. Complete a threats and opportunity analysis of future technological evolution extending from SWOT (above) and engaging a variety of organizations at the forefront of information technology (including RFID), data protection, privacy and information security. A documented summary of the study will contribute to the recommended standardization work programme.
4. Develop an inventory of actors in the area of RFID and related RFID networks and with respect to data protection, privacy and information security. Build and align effort with that of CASAGRAS and GRIFS but extend further into areas of data protection, privacy and information security.
5. Data protection, privacy, information security & interoperability review to establish essential and important aspects of “privacy by design” with respect to Policy and the OECD RFID guidelines. Develop a review document which contributes to the recommended standardization work programme.
6. Identify policies and standards with respect to “Privacy and security by design” with particular respect to physical systems components and robust consistent interfaces which foster the trust of individuals. Develop a review document which contributes to supporting the recommended standardization work programme.
7. A review of issues related to transfer of user control, deactivation and reactivation of tags (and interrogators) with transfer of liability to the technology developer. Market survey of related technologies and standards. Development of an impact analysis and recommendation based upon a review of technology, applications, the legal environment and policy in order to identify areas of future standards development. Reference to action No. 3 above and future IoT scenarios will provide an important contribution to this work. The recommendation will contribute to the standardization work programme.
8. With reference to the Communication on PETs [Com(2007) 228] in supporting the development of good practice frameworks to support PIAs identify complementary standards. Both existing and potential future standards will be documented providing a contribution to the standardization work programme. Take due

account of established and ongoing activities related to generic PIAs and ensure the development of specific RFID PIA related processes in order to deliver a standard approach to the assessment of RFID implementations throughout Europe

9. Analyse security level requirements in relation to applications and data objects and in particular those associated with high capacity and/or functionality tags. Avoid over specification of requirements for many applications. Draw upon established and ongoing work within ESOs. Document the findings and recommendations in support of the future standardization work programme.
10. Identify and classify applications by security risk levels. Draw upon established and ongoing work within ESOs and elsewhere. The classification will contribute a hierarchy of importance to the recommendations within the future standardization work programme.
11. Analyse sectoral applications needs for standards. The analysis will look into existing established needs and anticipate the future requirements and opportunities such standards may offer e.g. when migrating from open to closed applications, etc... The prime focus will remain data protection, privacy and information security. Findings will be documented in support of the future standardization work programme.
12. An assessment of standards and procedures for object identification will be completed. Consideration of European and world implications, taking into account the broad range of identification schemes. There are multiple and unique advantages to be derived from looking at RFID in the context of a broad range of identification schemes opening improvements in data protection, privacy and information security. The assessment and recommendations based upon the findings will contribute to the proposed standardization work programme.
13. Assess, and follow-up as appropriate, the opportunity to develop standards implementing Article 3.3 of Directive 1999/5/EC, subject of a Commission Decision on additional essential requirements over R&TTE.
14. Identify the needs and the requirements for cooperation to reach global interoperable solutions. To be used as a reference for the planning of Task 3 below.
15. Define clear objectives, task assignments and timetables for the delivery of the required standards or guidelines. This activity is a core element the recommended standardization work programme delivered at the end of Phase 1.
16. Assessment of the End of Life (EoL) and recycling implications for data held upon RFID tags or within components of other RFID network devices. Reference existing regulations, standards and guidelines for the disposal and recycling of electronic components in formulating a recommendation for RFID components and in particular RFID tags. The assessment and recommendations based upon the findings will contribute to the proposed standardization work programme.
17. Take due account of established and ongoing activities related to RFID logos and signage in order to offer standards which offer clear and consistent messages to the general public throughout Europe in raising awareness as well as building confidence in RFID technology and associated applications. Standards need to be developed quickly to support the RFID Recommendation.

5 Consumer aspects including interaction

5.1 Awareness

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). The initiative on logos and signage described in the present document addresses the aim to raise consumer awareness.

5.2 Purpose

A single tag may be used for a number of discrete 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 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).).

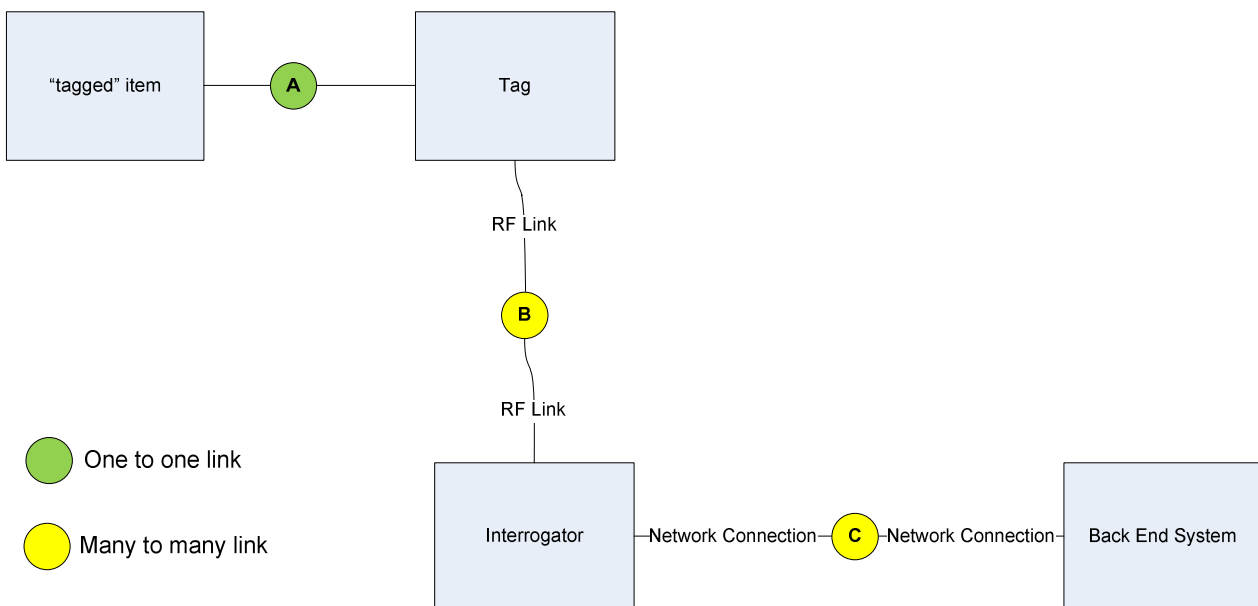
NOTE 1: Deactivation of the tag should be linked to removal or deactivation of data in the wider system.

NOTE 2: Existing and future planned regulation in Europe may not support the concerns on deactivation and purpose identified in this clause.

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. The RF link does not make the tags into elements of a radio communication system.

NOTE: The Open Systems Interconnection model defined in ITU-T X.200 [i.18] 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.29] defines the following type distinctions among RFID tags:

- active tag
 - RFID device having the ability of producing a 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 such 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: 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 allocated for RFID. The frequency selected is determined by the application.
- Size: ranges from a pinhead to a brick.
- For passive tags antenna size determines, 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 administration.

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.

The RF characteristics of the air interface between tag and interrogator are standardized in ISO/IEC 18000-n [i.21], 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 designed for GSM in the 900MHz band is typically 60dB more sensitive to radio signal detection than an RFID device in the same frequency range to achieve its design goal, this capability may be taken advantage of by a hostile attacker to identify the presence of interrogators and tags.

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 personal data 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).

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
 - 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.
- 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 for deployment of technology
- Industry and government organisations (when acting as industry) – those who operate RFID applications and services
 - In RFID different industries deploy the 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 Annex E.1, which shows that both mandatory and optional commands exist in a single standard. The same degree of optionality or feature selection freedom 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. Whilst it is recognised that proprietary technologies have a diminishing market share both the installed base and new applications being built on the proprietary platforms the ability to introduce new features to maximise privacy and security in a fragmented market offer 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 with continue to be developed. If the standardisation role in RFID is to act to assist market regulation, and freedom of access to an open market, there is need to encourage movement away from closed and proprietary systems to controlled and interoperable systems compliant to open standards.

6.6 RFID and IoT

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 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 which is a consumer concern.

6.7 Regulatory protection of Identity

The European data protection directive 95/46/EC [i.48] and the privacy directive 2002/58/EC [i.36] state the legal obligations of both users and providers to preserve a user's control of their personal data when used in electronic communication. These obligations apply to the operator of the system in which RFID is used although the directives are mostly aimed at Communications Service Providers (CSPs). It should be noted that the CRAVED analysis given in TR 187 010 [i.16] identifies identity and personal data as a target of crime that whilst illegal does require provision of measures to inhibit theft over and above the legal framework.

Where radio equipment is deployed, as in RFID, the R&TTE directive [i.47] applies and privacy of the identity has to be assured. This is explicitly cited in article 3.3 of the R&TTE directive, as follows:

- apparatus of particular types shall be so constructed that:
 - it incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected; and/or
 - it supports certain features ensuring avoidance of fraud.

For the purposes of RFID it is recommended that where explicit personal data is deployed on a tag that only those devices capable of supporting encrypted storage or transmission of data should be deployed.

At a higher level as stated in TR 187 010 protection of identity and privacy are also identified as fundamental rights that have identified a number of key principles for those gathering data illustrated in Table 1.

Table 1: Generic principles arising from OECD guidelines and EC Data Privacy directives.

Root principle	Subsidiary principle	Impact on <i>RFID</i>
Collection limitation	Limits to data collection	<p>Before collecting personal data – for example, when contracting with the data subject – an operator of the <i>RFID</i> system should obtain the prior and unambiguous consent of the data subject or inform the data subject of the collection of personal data and the indicated purposes of use according to domestic regulations.</p> <p>From the viewpoint of the operator of the <i>RFID</i> system, 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</p>
	Data collection methods	An operator of the <i>RFID</i> system 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 operator of the <i>RFID</i> system 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 operator of the <i>RFID</i> system should take suitable measures to confirm the consent of a data subject about data collection
Data quality		An operator of the <i>RFID</i> system 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, an operator of the <i>RFID</i> system should specify the purposes of use of personal data
	Limits on changing the purposes of use	An operator of the <i>RFID</i> system 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

Root principle	Subsidiary principle	Impact on <i>RFID</i>
	Change of the purposes of use required prior consent	Before an operator of the <i>RFID</i> system 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
Use limitation	Use limitation	An operator of the <i>RFID</i> system 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
	Restriction of disclosure to third parties	An operator of the <i>RFID</i> system should not provide personal data to a third party without obtaining the prior consent of the data subject
	Use without consent	The provisions of the preceding two paragraphs shall not apply to cases in which the handling of personal data is based on domestic laws. The operators of the <i>RFID</i> system 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
Individual participation		<p>An individual may have the right to:</p> <ul style="list-style-type: none"> (a) obtain from an operator of the <i>RFID</i> system, or otherwise, confirmation of whether or not the operator of the <i>RFID</i> system has data relating to him; (b) have communicated to him, data relating to him <ul style="list-style-type: none"> (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; <p>I be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and</p> <ul style="list-style-type: none"> (d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Root principle	Subsidiary principle	Impact on <i>RFID</i>
Accountability		An operator of the <i>RFID</i> system should be accountable for complying with measures which give effect to the principles stated above
Equality of regime		An operator of the <i>RFID</i> system should not transfer personal data across borders unless the destination has an equivalent privacy regime as the origin.
Anonymity		An operator of the <i>RFID</i> system should provide the means for users to transact anonymously

NOTE: The 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 Analysis

7.1 RFID system architecture

Implementation of the RFID ecosystem may take many forms as follows:

- 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:

- 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 this report to catalogue requirements for logos, and for signs, are intended to address some of the user concerns related to visibility of the RFID technology.

NOTE: In parallel to the activity reported in the present document there is parallel work being carried out on the specification and requirements for a Common European RFID logo and sign.

NOTE: The ESO's propose that the final work in defining and publishing such a logo and sign forms part of the phase 2 of the standardisation mandate, taking into account the input from the parallel activities currently in progress, together with other standards activities on a global basis.

A second privacy concern is that of the intent of the system and its 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 rather than a characteristic of the system cannot be considered as intrinsic privacy by design. 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.

Table 2: RFID Frequencies, Typical uses, and Typical Read Range

	Type	Typical application	Typical read range
125 KHz–148 KHz	Passive	Animal tracking (ISO 11784/11785), 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 to 30 cm
13.56 MHz	Passive	Library management Ticketing, (mass transportation, traffic and event management) Access control (including passports) Security Logisti-s - Item tagging Near field communication (NFC)	Up to 60 cm Typically 2 to 60 cm
433 MHz	Active	Cargo handling Container locations Real Time Location Systems Asset tracking	Up to 100 m
860-960 MHz	Passive	Logistics chain, Palettes ID etc Item tagging Integrated RFID and EAS applications Manufacturing process control & product tracking Cargo handling Airline baggage Location systems Asset tracking	Up to 4 m
2446-2454 MHz	Passive and battery assisted	Chip processing, Automotive manufacturing Toll identification Proximity sensors Location tracking Asset tracking	Up to 10 m

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. As 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 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 or associated to the tag.

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: 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: 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 (the right of the individual to have his identity and agency protected from any unwanted scrutiny and interference) regulation tends to view static data whereas it is common practice to examine behavioural data to make assertions about the behaviour of individuals or groups. The simplest expression of this as a concept relationship diagram is shown in Figure 2. In this case there is a clear link between behaviour and the person. In terms of the RFID system this means that even if the tag does not contain personal data or is not intended to be assigned to a specific person there is a risk that by examination only of behaviour a real person can be identified.

NOTE: It has to be stressed that many of this risks to privacy identified in the preceding paragraph and in the analysis that follows exist with other eco systems, including those using magnetic stripe cards, bar codes, pin & chip cards etc.

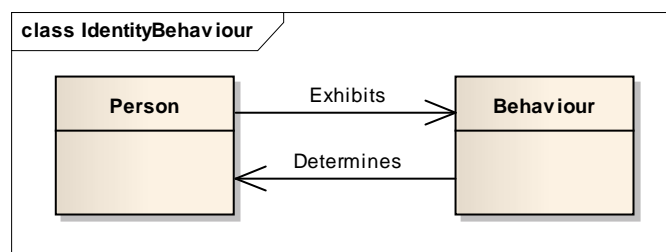


Figure 2: Very simplified concept relationship diagram of identity

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.

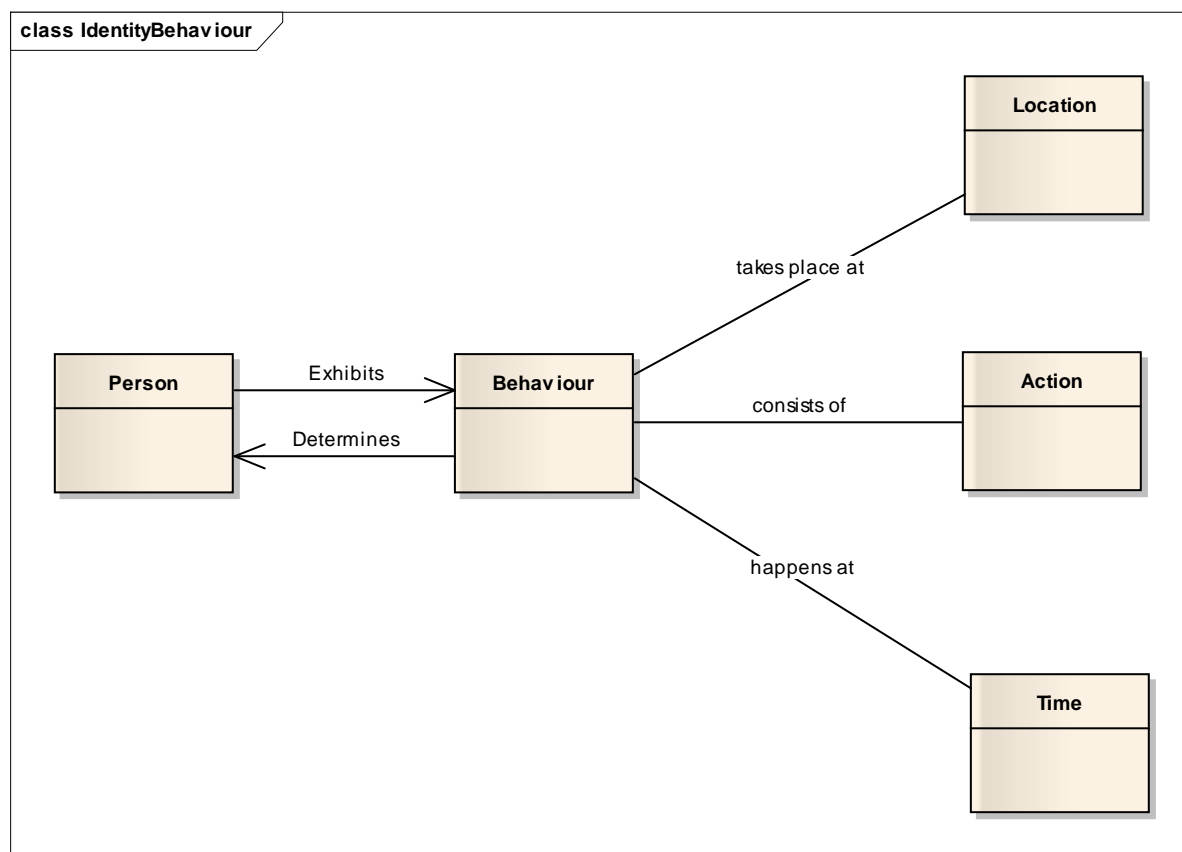


Figure 3: Expansion of simple concept relationship diagram with respect to behaviour

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.

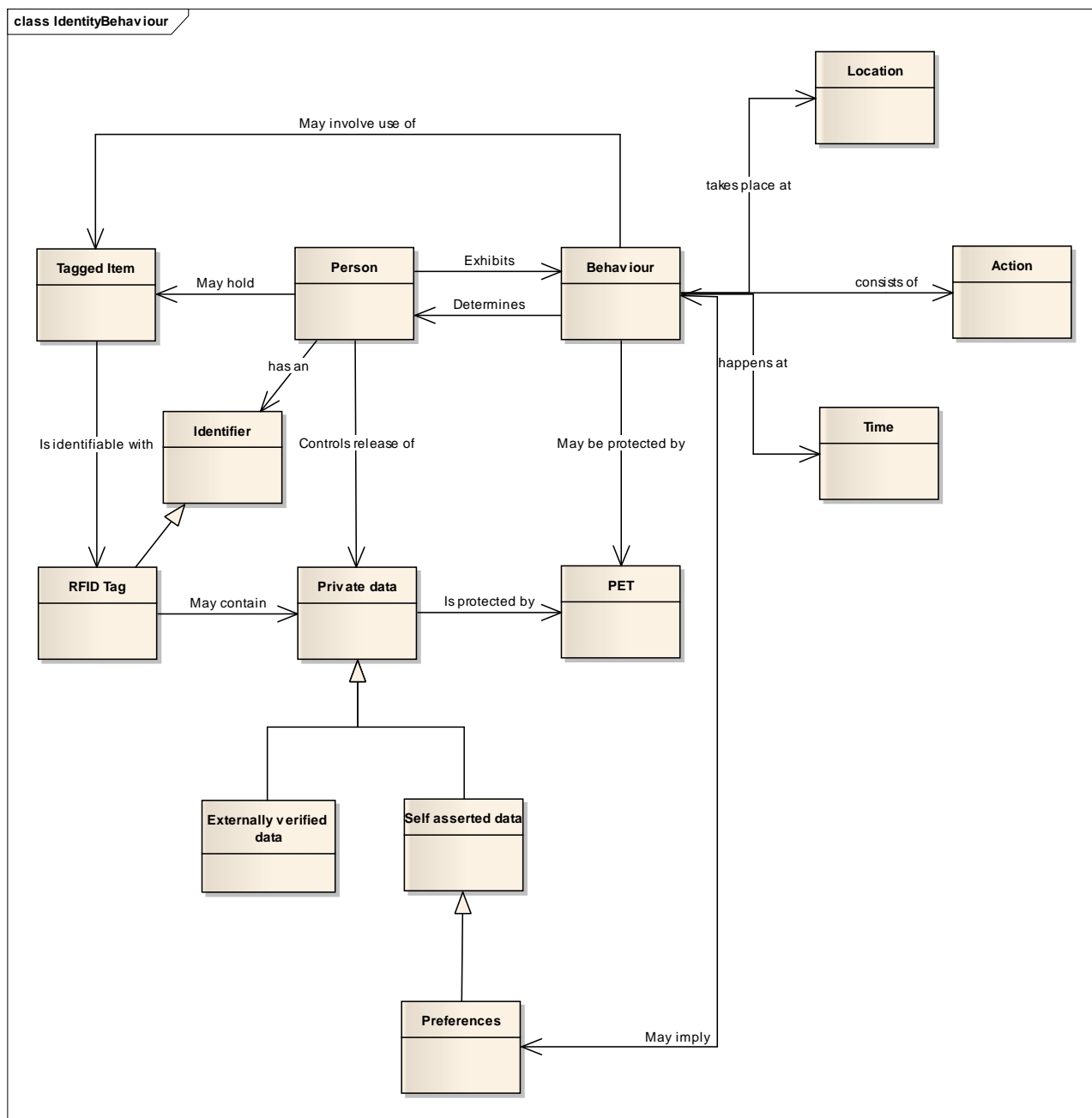


Figure 4: Concept relationship diagram for privacy in RFID

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: 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.

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 Data Protection Objectives and Requirements

As identified in TR 187 011 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.

7.3.1 Statement of objectives for Data Privacy Protection

Table 3: Summary statement of data privacy and protection objectives

Ref.	Objective	Intent
DPP0-1	Compliance with the DP Directive- Privacy by design	Privacy and security friendly technologies must be designed to ensure that applications respect the fundamental right to privacy and the data protection legislation, this may include mechanisms to control data read processes, mechanisms to provide disablement or kill functionalities and notification of the reading process.
DPPO-2	Accountability principle	An operator should be accountable for complying with measures which give effect to the DPP principles. Operators of an RFID application are 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	Information and transparency on RFID use	Operators should develop and publish a concise, accurate and easy to understand information policy for each of their application. The policy should at least include: <ul style="list-style-type: none"> i. the identity and address of the operators, ii. the purpose of the application, iii. what data are to be processed by the application, in particular if personal data will be processed, and whether the location of tags will be monitored, iv. a summary of the privacy and data protection impact assessment, v. the likely privacy risks, if any, relating to the use of tags in the application and the measures that individuals can take to mitigate these risks.

Ref.	Objective	Intent
DPPO-4	Signs	<p>Operators should take steps to inform individuals of the presence of interrogators on the basis of a common European sign to be developed (See Clause 7). The sign should include the identity of the operator and a point of contact for individuals to obtain the information policy for the application. Operators should inform individuals of the presence of tags that are placed on or embedded in products.</p> <p>RFID technology must provide the following information to data subjects:</p> <ul style="list-style-type: none"> i. identity of the controller, ii. the purposes of the processing as well as, among others, iii. information on the recipients of the data and the existence of a right of access. <p>Deployers of RFID technology are required to provide data subjects with information not only on the purposes of the processing of data, but also on the presence of RFID devices as well as to comply with the following:</p> <ul style="list-style-type: none"> i. Individuals must be informed of the presence of RFID-like or activated RFID interrogators (see section _ on sign). The provision of this type of information is essential in order to prevent t□mplementatised and surreptitious gathering of personal data through RFID technology. For example, if a store or hospital has activated interrogators, individuals should be informed about it. ii. The identification of the existence of RFIDs surrounding an individual (in clothing and objects for example) is another requirement because of the RFID's size which can make it almost invisible. Methods to carry out this requirement can adopt different forms: they can be given by standard notices but also technically. iii. Informing about the presence of RFID only will not suffice in practice, the activability or the real time activation of RFIDs is also a piece of information to be provided to individuals that derive from the data protection Directive. So, simple techniques enabling visual indications of activation or activability states are also necessary. The presence and nature of PET technology (e.g. temporal disabler, tag physical remover feature etc.) as well □mplementationnal measures in a given environment should be part of the information easily available. <p>Retailer store will have to provide data subjects at least with clear notice about the following:</p> <ul style="list-style-type: none"> i. the presence of RFID tags on products or their packaging and the presence of interrogators; ii. the consequences of such presence in terms of information gathering; in particular, data controllers should be very clear in informing individuals that the presence of such devices enables the tags to broadcast information without individual engaging in any active action; iii. the purposes for which the information is intended to be used, including <ul style="list-style-type: none"> (a) the type of data with which RFID information will be associated and (b) whether the information will be made available to third parties and, iv. the identity of ETSI controller. <p>In addition, depending on the specific use of RFID, the data controller</p>

Ref.	Objective	Intent
DPPO-5	Requirements for consent and information in personal data collection	<p>shall comply with the DP Directive. The information to be provided to data subject should be in a clear and comprehensible manner. Data subject should be in a condition to understand easily the effects of the RFID application. Therefore, the consent</p> <ul style="list-style-type: none"> i. Must be freely given, i.e., it must be given free of “deceit or coercion.” ii. Must be specific, in other words, it must relate to a particular purpose iii. Must be an indication of the individual’s effective will. iv. Must be informed. v. Finally, consent must be “unambiguous” meaning that consent that is capable of having more than one meaning would not be deemed consent. <p>Before collecting personal data – a - for example, when contracting with the data subject – a operator should obtain the prior and unambiguous consent of the data subject or inform the data subject of the collection of personal data and the indicated purposes of use according to domestic regulations;</p> <p>If the data subject is aware of the presence of an RFID interrogator and willingly submits a tag to be read consent may be implied. However if the data subject is unaware of the presence of an RFID interrogator it is unlikely that consent can be proven.</p> <p>From the viewpoint of the 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.</p> <p>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.</p> <p>Confirmation of a data subject's consent about data collection: An operator should take suitable measures to confirm the consent of a data subject about data collection.</p> <p>No change in the ownership, responsibility, content or collection of personal data pertaining to a user should occur without that user's consent or knowledge</p>
DPPO-6	Personal data pertaining to a user should be collected by the system using legitimate means only	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

Ref.	Objective	Intent
DPPO-7	Data quality principles shall be applied	<p>Data controllers collecting data in the context of RFID applications must comply with several data protection principles, including the following:</p> <ul style="list-style-type: none"> i. Use limitation principle (purpose principle): This principle partially embodied in article 6(1)(b) of the data protection Directive, among others, prohibits a further processing which is incompatible with the purpose(s) of the collection. ii. The data quality principle: This principle in the Directive requires personal data to be relevant and not excessive for the purposes for which they are collected. Thus, any irrelevant data must not be collected and if it has been collected it must be discarded (Article 6.1. c)). It also requires data to be accurate and kept up-to date. An operator should implement measures to keep personal data accurate and up to date within the scope necessary for the achievement of the purposes of use. iii. The conservation principle: This principle requires personal data to be kept for no longer than is necessary for the purpose for which the data were collected or further processed. iv. Minimising the processing of personal data using anonymous or pseudonymous data where possible. Exclusion of data capable of identifying an individual from collected data: An 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.
DPPO-8	Storage of personal data on each tag shall comply with the DP Directive	<p>It should be noted that RFID systems are very susceptible to attacks. As they work non-line-of-sight and contactless, an attacker can work remotely and passive readings will not be noticed. That would be the case of tracking without "traditional" identifiers when the use of RFID technology entails individual tracking and obtaining access to personal data</p>
DPPO-9	. Application of principle of purpose limitation	<p>Specification of the purposes of use: When handling personal data, an operator should specify the purposes of use of personal data.</p> <p>Limits on changing the purposes of use:</p> <ul style="list-style-type: none"> i. An 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; ii. Before an 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. <p>An 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.</p> <p>An operator should not provide personal data to a third party without obtaining the prior consent of the data subject.</p> <p>The provisions of the preceding two paragraphs do not apply in cases where the handling of personal data is based on domestic laws. NGN operators should grant access only to law enforcement authorities as authorized by a domestic court order or equivalent legal instrument</p>

Ref.	Objective	Intent
DPPO-10	Right of access, rectification, deletion to tag content (Art. 12 a data protection Directive)	<p>If RFID tags contain personal information as described under 3.2, individuals should be entitled to know the information contained in the tag and to make corrections using means easily accessible.</p> <p>RFID tag content access requires an interrogator working with the tag protocol and a display towards the individual. For many applications, the tag contains only an Id whose semantics can only be accessed through a complete IT application environment. RFID tags bearing semantic information (describing the object, the data controller identifier, the data collection finality etc.) poses the problem of the content access by individuals. Whatever the form they take, those semantic descriptions still pose the problem of the access by unauthorized third parties</p> <p>Tag content access: An individual may have the right to</p> <ol style="list-style-type: none"> i. obtain from an operator, or otherwise, confirmation of whether or not the operator has data relating to him; ii. have communicated to him, data relating to him <ol style="list-style-type: none"> a) within a reasonable time; b) at a charge, if any, that is not excessive; c) in a reasonable manner; and d) in a form that is readily intelligible to him; iii. be given reasons if a request made under (i) and (ii) is denied, and to be able to challenge such denial; and iv. challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended. <p>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).</p> <p>Tag content deletion (Article 12 b data protection Directive): In defining how tag disablers should work, in addition to the above, standardization bodies, manufacturers and deployers of RFID technology should take into account that individuals selecting the removal of the tag should not be penalised in any way. Also there, Working Party 29 stresses that is a continuing need for further R&D on these topics by all parties. One approach was the introduction of a “kill” command. Tag can be permanently or temporarily deactivated by sending a “kill” command.</p> <p>Tag content deletion:</p> <ol style="list-style-type: none"> i. Permanent deactivation can be done by fuse effect, memory scrambling or removing the tag. ii. Temporary deactivation could be done mechanically or by applying a software lock. A problem with this approach is that the advantage of re-using the RFID capability outside the shop is lost. So, other approaches have been proposed. iii. Overwriting the data stored on an RFID tag with zeros. <p>Note: Problem: A well-informed company can make an educated guess. Secondly, it appears that at first, RFID tags are going to be used on valuable items. For a few years, the mere presence of an RFID tag (even if it returns zeros or unintelligible data) will help thieves looking for items worth stealing in cloakrooms or parking garages.</p> iv. Physical shielding of the tag, which can be implemented by the user. For example, purses with shields can be used, so that

Ref.	Objective	Intent
DPPO-11	Tags disablers or the right to 'silence of the chips'	<p>It expresses the idea that individuals should be able to disconnect from their networked environment at any time.</p> <p>In some RFID applications, for example when the individual has a right to withdraw his/her consent or to object to the processing (ex 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.</p> <p>When under the data protection Directive consent is the only legal ground to legitimise the collection of personal data through RFID technology, individuals can always withdraw their consent to the processing of personal data (ex Article 7 a).</p> <p>If no device enabling the individual to disable the tag is available, an individual who does not wish the tag to continue providing information on him/her will be prevented from exercising this right.</p> <p>When personal data embedded on RFID tags has been provided collected on legal grounds other than consent, it is not always necessary for such tags to have disabler devices. For example, personal information contained in tags used in the work context for the purposes of monitoring access to work may not require having available tags disablers insofar as the data processing is based on the employment relationship.</p> <p>It is then necessary to elaborate the concept of user control over deactivation and re-activation of RFID tags at point of sale, to develop a standard which can transfer control to the consumer.</p> <p>NOTE: Removal of the tag from its associated object may be equivalent to deactivation.</p>

7.3.2 Statement of objectives for Security

Table 4: Security objectives and linked security functional requirements

SO No.	Security Objective	Sec. Functional Requirements
SO-1	personal data, behavioural information and data related to possessions 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	personal data, behavioural information and data related to possessions 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	personal data, behavioural information and data related to possessions 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	personal data, behavioural information and data related to possessions held within one or more components of the RFID ecosystem (tagged item, tag, interrogator, network connections, backend systems) should be protected from non-legitimate access from within the RFID ecosystem	Access control; Identification of parties; Authentication of parties
SO-5	personal data, behavioural information and data related to possessions held within one or more components of the RFID ecosystem (tagged item, tag, interrogator, network connections, backend systems) should be protected from non-legitimate access from outside of the RFID ecosystem.	Access control; Identification of parties; Authentication of parties
SO-6	personal data, behavioural information and data related to possessions held within one or more components of the RFID ecosystem (tagged item, tag, interrogator, network connections, backend systems) should be protected from unauthorised modification.	Integrity control; Access control
SO-7	personal data, behavioural information and data related to possessions held within one or more components of the RFID ecosystem (tagged item, tag, interrogator, network connections, backend systems) 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 (tagged item, tag, interrogator, network connections, backend systems) 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 (tagged item, tag, interrogator, network connections, backend systems) 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: Repudiation is not considered in the above table as repudiation requires user determination and control to invoke, and this is considered as unreasonable in the RFID systems examined in the present report.

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) the Common Criteria defined in ISO/IEC 15408-2 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 (i.e. the PIA is considered as a PET).

8 Security risk analysis of RFID systems

8.1 Security analysis and requirements derivation

NOTE: This clause 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 easily identify and track objects by means of their attached RFID tag. The primary characteristic in RFID is that many tags can be read remotely by interrogators at known locations, where the interrogator is able to provide additional information including the location and time of the read, and 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).

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 [ref], which include the following categories:

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

The following sub-clauses describe the threat 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: 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.

8.2 Weaknesses and threats in RFID systems

The identification of the following threats are considered in the RFID system (a more detail analysis of these threats and scenarios in which they may exist in RFID systems is given later in this clause).

- T1-Denial of service attack / flood / buffer overflow;
- T2-Blocking;

- T3-Collision attack;
- T4-Blocking;
- T5-De-synchronization;
- T6-Replay
- T7-Man-in-the-middle attack;
- T8-Theft
- T9-Unauthorised access to / deletion / modification of devices / data etc;
- T9-Unauthorised access to / deletion / modification of devices / data etc;
- T10-Use erroneous and/or unreliable data
- T-11 Procedures / instructions not followed leading to tags being used passed end of purpose;
- T12-Cloning of credentials and tags (RFID related);
- T13-Illicit access to data
- T14-Physical RFID tag destruction
- T15-Malfunctioning/breakdown of systems /devices / equipment
- T16-Worms, viruses & malicious code;
- T-17 Low acceptance of devices / equipment / procedures;
- T18-Spoofing of credentials / bypass authentication;
- T19-Large-scale and/or inappropriate data mining and/or surveillance;
- T20-Masquerade;
- T-21 Social engineering attack;
- T-21 Traffic analysis / scan / probe;
- T-22 Identity theft;
- T-24 Non-compliance with data protection legislation;
- T-25 Function creep (data used for other purposes than the ones for which they were originally collected)
- T-26 Side channel attack;
- T27-Fake / rogue RFID readers / scanning of RFID reader and /or tag
- T-28 Data linkability;
- T29-Profiling;
- T-30 Exclusion of the data subject from the data processing process due to disabling of RFID tag
- T32-RF eavesdropping;
- T32-Trivialization of unique identifiers
- T33-Tracking

8.3 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.

Table 5: List of vulnerabilities to an RFID ecosystem

Vuln. No.	Weakness	Threat
V1	Lack of respect of the data minimization and proportionality principles	T18-Spoofing of credentials / bypass authentication; T19-Large-scale and/or inappropriate data mining and/or surveillance; T20-Masquerade; T33-Tracking
V2	Lack of respect of the purpose limitation (finality principle)	T-11 Procedures / instructions not followed leading to tags being used passed end of purpose
V3	Lack of respect of the transparency principle	T-24 Non-compliance with data protection legislation; T-30 Exclusion of the data subject from the data processing process due to disabling of RFID tag
V4	Inappropriate / inadequate identity management	T18-Spoofing of credentials / bypass authentication; T20-Masquerade; T-21 Social engineering attack; T-22 Identity theft; T32-Trivialization of unique identifiers
V5	Inherent features (size, material etc.): easy to lose, to be stolen and/or copied (especially for RFID tags)	T8-Theft
V6	Actual RFID range longer than standard	T-11 Procedures / instructions not followed leading to tags being used passed end of purpose; T18-Spoofing of credentials / bypass authentication; T20-Masquerade; T-21 Traffic analysis / scan / probe; T33-Tracking
V7	RFID tags do not have a turn-off option	T-21 Traffic analysis / scan / probe; T-22 Identity theft; T33-Tracking
V8	Insufficient protection against reverse engineering	T12-Cloning of credentials and tags (RFID related); T27-Fake / rogue RFID readers / scanning of RFID reader and /or tag
V9	Inadequate security measures of data storage (e.g. inadequate encryption measures)	T16-Worms, viruses & malicious code; T-17 Low acceptance of devices / equipment / procedures; T-21 Social engineering attack; T29-Profiling; T33-Tracking
V10	Over-sensitivity of devices (generating many false alarms)	T15-Malfunctioning/breakdown of systems /devices / equipment
V11	Sensitivity to magnetic fields	T14-Physical RFID tag destruction
V12	Communication of data over unprotected or publicly accessible channels	T7-Man-in-the-middle attack; T29-Profiling; T33-Tracking
V13	Data linkability	T19-Large-scale and/or inappropriate data mining and/or surveillance; T-28 Data linkability; T33 Tracking
V14	Lack of data correction mechanisms (as normally data subjects do not have access to the databases)	T9-Unauthorised access to / deletion / modification of devices / data etc; T10-Use erroneous and/or unreliable data
V15	Lack of common or harmonized legislation in EU Member States	T9-Unauthorised access to / deletion / modification of devices / data etc; T13-Illicit access to data; T19-Large-scale and/or inappropriate data mining and/or surveillance; T-30 Exclusion of the data subject from the data processing process due to disabling of RFID tag
V16	Insufficient protection of data communication (weak or no encryption etc.)	T7-Man-in-the-middle attack; T13-Illicit access to data; T-26 Side channel attack; T32-RF eavesdropping; T33-Tracking
V17	Lack of respect to the legitimacy of data processing, e.g. consent	T-24 Non-compliance with data protection legislation; T-25 Function creep (data used for other purposes than the ones for which they were originally collected)

V18	Lack of respect to the data conservation principle	T-24 Non-compliance with data protection legislation; T-28 Data linkability; T-30 Exclusion of the data subject from the data processing process due to disabling of RFID tag
V19	Lack of respect to the rights of the data subject (such as the right for rectification, blocking or deletion of data)	T7-Man-in-the-middle attack; T9-Unauthorised access to / deletion / modification of devices / data etc; T10-Use erroneous and/or unreliable data; T13-Illicit access to data
V20	Insufficient protection against DoS attacks	T1-Denial of service attack / flood / buffer overflow; T2-Blocking; T3-Collision attack; T4-Blocking; T5-De-synchronization; T6-Replay

8.4 Attacks on RFID and associated systems

8.4.1 Identity spoofing

Spoofing of identity occurs when an attacker successfully poses as an authorized user of a system (in technical environments this is most often referred to as a masquerade attack).

There are many ways in which such an attack can be achieved, ranging from competitors performing unauthorized scanning of inventory to obtain information on types and quantities of items. The tag identities can then be emulated, e.g., in a large convenience store to "trick" customers into purchasing particular products. This is made possible if a tag cannot distinguish between authorized and unauthorized interrogators. To the tag, a interrogator is a interrogator. Also, the numbering schema used for RFID tags makes up the tag identity and includes information about the manufacturer and possibly the product number. This attack can also be carried out by an attacker with a valid interrogator or equipment able to eavesdrop on the RF interface.

SCENARIO: Assuming that EPC numbering is used, it is possible for an attacker to pose as an authorized Object Name Service (ONS) user and submit queries of either gathered EPC numbers or random EPC numbers to ONS to determine the exact URL of the database containing the information of a particular EPC number. This way the attacker can successfully obtain information on the association to a particular EPC number and the product type that the tag is attached to.

8.4.2 Tampering with data

Data tampering occurs when an attacker modifies, adds, deletes, or reorders data. The impact of such attacks range from serious threats as an attacker modifying the tag in a passport to modifying the 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, economical 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 it can also be misused by an attacker as a consequence of the password distribution being difficult to secure, or 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).

8.4.3 Repudiation

Repudiation occurs when a user denies an action and no proof exist to prove that the action was performed.

SCENARIO#1: An attacker denies receiving and holding of an item (*repudiation*). If the tag remains present on the item it may be read by an investigator to repudiate the denial (*counter to repudiation*).

SCENARIO#2: An attacker denies receiving and holding an item but is aware of the presence of the tag and either removes it (without damage) or modifies the tag such that it does not properly identify the item (*system unable to determine the presence of the item*).

8.4.4 Information disclosure

Information disclosure occurs when information is exposed to an unauthorized user. It is a threat to privacy if the information disclosed is of a private or sensitive nature covered by the Data Privacy Protection Act.

SCENARIO: An attacker may track tags and some tags will carry personal data or information that can be used to derive the identity or link behaviour to person.

8.4.5 Denial of service

Denial-of-service denies service to valid users. Denial-of-service attacks are relatively easy to accomplish and difficult to guard against.

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 powerful signal generator jams the interrogator or return signal from the tags thus making the system unavailable to authorized users

8.4.6 Elevation of privilege

Elevation of privilege occurs when an unprivileged user or attacker gains higher privileges in the system than what they are authorized.

SCENARIO: A user logging on to the database to determine product information can become an attacker by raising his/her status in the information system from a user to a root server administrator and write or add malicious data into the system.

8.4.7 Other RFID security threats

In addition to the threats that can directly be associated with the STRIDE model there are also some RF specific security threats of relevance, as well as some general security threats. The RF specific security threats of relevance are:

- RF eavesdropping
- Collision attack
- Tracking
- De-synchronization

The general security threats of relevance are:

- Replay
- Virus

8.4.7.1 RF eavesdropping

Since an RFID tag is a wireless device, there exists a risk that the RF signal between tags and interrogators can be eavesdropped.

NOTE: Such tests have been performed at the German Ministry of Interior yielding a Read range of 2.7m with an ISO 14443 card but need to be formally validated.

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.

8.4.7.2 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 a 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 among 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 the query from the interrogator at the same time hence collision happens. Collision attack is a variant of DoS attacks.

8.4.7.3 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 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.

8.4.7.4 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 the identity of 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.

8.4.7.5 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.

8.4.7.6 Virus

Software infections, commonly referred to as a virus, can be used to manipulate, disclose or maliciously prevent communication between the tag and the interrogator or the network. Whilst it is reasonable to claim that the payload of an RFID tag is insufficient to carry a virus it is sufficient to carry a trigger or link to a virus. This may be of particular relevance in object hyper-linking scenarios.

NOTE: The virus problem is not specific to RFID and therefore should be addressed outside the RFID sector with due care given to adequately consider the use of RFID elements as vectors to trigger or manage previously installed viruses.

Table 6: Application of identified standardisation gaps across technologies of RFID

	Standardisation gap	Technology						
		Tag	Tag to Reader Interface	Reader	Reader to Back End System Interface	Application and multi application	RFID Open System Data Design	RFID Open System Operations
A	Tag access and security	X	X					
B	Control of data read by application			X				
C	Tag kill	X	X	X				
D	Authentication		X					
E	Access control			X				
F	Informed consent procedural standard							X
G	System operational standards						X	X
H	Reader authorisation by application			X	X			
I	RFID system Privacy by design standard	X	X	X	X	X	X	X
J	Operational audit standards							X
K	System data access by design standard	X	X	X	X	X	X	X
L	Addition of tag facilities	X						
M	Deletion and modification in multi app environment					X		
N	Open system interoperability design standards						X	
O	System interoperability service/procedures standards							X
P	System penetration testing standards (e.g. for different categories of application privacy risk)	X	X	X	X	X	X	X

9 Privacy Impact and Data Protection Assessment (PIA) outline

The European Commission Recommendation of 12 May 2009 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 was to undertake the task in collaboration with relevant civil society stakeholders. At the time this draft document was issued, the framework has been submitted for review to the Article 29 Data Protection Working Party and the results of the review are expected in October 2010.

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 consequently been amended. With regard to the privacy impact and data protection assessment (henceforth PIA), the work of the specially appointed Specialist Task Force (henceforth STF) has consisted of defining the general requirements for a PIA. On the basis of the requirements thus defined, the STF has performed a gap analysis aiming to identify related standardization needs not yet addressed.

Synergy with the industry PIA will take place upon availability of the definitive version.

9.1 Role of PIA

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.

NOTE: 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 (Quality) and ISO 27000 (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.

RFID systems not processing information that can be used to identify individuals directly or indirectly will not require a PIA. Whether a system requires a PIA or not will be determined by means of a prior assessment – sometimes called a threshold assessment.

NOTE: For example, pure inventory control applications will not require a PIA.

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.

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 activities of 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, in assessing all technological, organizational and regulatory risks relevant to a (proposed) RFID system. And 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,
- 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.

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.

9.2 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: Disruptive technologies do not have negative connotations.

- 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: The 2005 pan-European survey on RFID and Consume–s - What European Consumers Think About Radio Frequency Identification and the Implications for Business [i.27] 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.

- the RFID technology and related applications enjoy various levels of maturity, resulting in fragmented understanding of related risks;
- RFID tags include unique identifiers which makes it possible to reference them back (directly or indirectly) to their owners (tracking);
- RFID can enable real-time tracking;
- the stealth nature of RFID (i.e. the ability to continue to function in the background unobservably to the individual);
- 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 their ubiquitousness;

- RFID tag lifetime usually exceeds its useful purpose or data protection legal prescriptions;
- 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.).

9.3 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 consumer concerns.

9.4 PIA Methodology Requirements

As mentioned above, certain current features of RFID technology and RFID-enabled applications 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.

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 this 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 an 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 and impact on privacy, or the context of domain in which RFID systems are employed).

9.4.1 Assets and the RFID PIA

Assets refer to the object of protection 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 let alone (e.g. via direct marketing, etc.), trust in organizations deploying RFID, financial assets, etc.

9.4.2 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, threats 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.

Standardization gaps identified thusfar include:

- Standard RFID-specific PIA methodologies.
- Domain and sector-specific PIA templates & guidance.

9.4.3 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 appoint 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. That 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 possible quantifying privacy risks and defining means to mitigate them;
- 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 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).

9.4.4 Data Protection and Privacy requirements of the RFID PIA

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

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

9.4.4.1 Data protection requirements

This section addresses primarily general issues of data/information privacy; issues of compliance with European, national, regional, local, sector-specific legislation. The detailed analysis of RFID-specific data/information privacy is presented in table 4 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 ☐ mplementainga 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 is kept which should not exceed the period of time necessary to fulfil the purpose for which it was collected;
3. Data quality;
4. Transparency and openness – referring to the individual's 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;
5. Accountability – referring to assigning responsibility for compliance with overall privacy and data protection requirements; measurement and monitoring of fulfilling these responsibilities and potential compliance; and defining redress measures;
6. Rights of data subjec–s - right to information, correction, removal; availability of contact information. Additional attention should be paid to issues of:
 - a. Citizen/consumer awarene–s - 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 behavio–r - 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 – currently not specifically addressed by the data protection legislation
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 of 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.

9.4.4.2 Privacy requirements

This section addresses broader privacy requirements which 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 beside data privacy, namely: spatial, temporal, bodily and behavioural privacy.

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

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. Bodily privacy - referring to the integrity of the individual's body [i62]
3. Behavioural privacy - referring to the individual's activity and preference patterns, both explicit and implicit
4. 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, 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

9.4.4.3 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 of minors;
- workplace privacy – in relation to using RFID to track and/or trace activities of employees;
- tracking by proxy – referring to inferring the identity of an individual through an RFID tagged belonging;
- 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, etc. advantage.

The tables that follow summarise as a first pass the analysis of each of the three areas described above.

Table 7: Data protection requirements

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure	Standardization gaps
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. See annex A.4.2 for details.	all	PETs, authentication and authorization, Training of personnel	details are in clause 12

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 Further details in annex A.2 and clause 5.	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.	details are in clause 12
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 annex A.2 and clause 5.	Backend system	Automatic deletion or disabling of information according to fulfilment of some parameter (time, period, action, event).	details are in clause 12
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 semantical validations	details are in clause 12
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; logos and signage etc.	details are in clause 12

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure	Standardization gaps
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	details are in clause 12

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 A.2	all	encryption of data on tag, encryption of data transfer, shielding, authentication and authorization, anonymization, use of pseudonyms etc.	details are in clause 12
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 clause 5 and annex A.2	backend system (databases)	regulation	For Further Study
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	For Further Study

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure	Standardization gaps
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	For Further Study

The privacy requirements captured in table 4, 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 8: Privacy requirements

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure	Standardization gaps
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	For Further Study

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 A.2 and clause 5.	all	regulation, use of pseudonyms, encryption, use of session id rather than tag identity etc.	see clauses 5 and 12
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.	see clauses 5 and 12
bodily dimension of privacy	refers to the integrity of the individual's body [i62]	tags on body & implants monitoring bodily functions etc.	tag, interrogator	regulation, shielding, controlled readings, encryption, use session id rather than tag identity etc.	see clauses 5 and 12
behavioural privacy	refers to individual's activity and preference patterns, both explicit and implicit	profiling	all	regulation, implementation, pseudonyms, use of session id rather than tag identity etc.	see clauses 5 and 12
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	tag, interrogator, backend database	regulation, encryption, pseudonyms, anonymization, etc.	For Further Study

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure	Standardization gaps
		A.2)			
	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.	see clauses 5 and 12
	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.	see clauses 5 and 12

Table 5 below 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 A.2.

Table 9: Emerging issues

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure	Standardization gaps
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" [i.62]	details are given in annex A.2	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.	see clauses 5 and 12
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 A.2	all	randomisation of data, shielding, minimizing of data, control of purpose, consumer awareness, logos and signage, etc.	see clauses 5 and 12

Category/issues	Explanation/comments	Threats and Risks	Ecosystem component involved: tag, interrogator, database, architecture, other	Control/measure	Standardization gaps
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 private information	all	consumer awareness, encryption, authentication and authorization, pseudonyms, etc.	see clauses 5 and 12

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.	For Further Study
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 & home workers	blurring of the boundaries between the private and public spheres tracking and tracing disclosure of private information, profiling, etc.	all	Consumer/citizen awareness, regulations, signs and logos, use of pseudonyms, etc.	For Further Study
tracking by complementing the identity of an individual via a proxy (e.g. pets chip implants as pointers for their owner's identity and / or contact information)	Tracking, tracing, profiling, disclosure of personal information, etc.	tag, interrogator, backend database	encryption, data minimization, unlinkability etc.	see clauses 5 and 12	
corporate espionage	unauthorized access to customer performance	unauthorized access to customer performance etc.	all	security safeguards, architecture solutions (privacy by design) etc.	For Further Study

10 Common European RFID Emblem/Logo/Sign

The common RFID sign initiative results from a number of similar initiatives undertaken by organizations within the European Member States and internationally. The European Commission supports a common RFID sign through Mandate M436, RFID Recommendation and through support of Work Package 5 within RACE networkRFID.

There can be many reasons for applying an RFID sign. The purpose of this document is to aid the process of clarifying these goals, providing a solid foundation to a recommendation and assisting in driving towards a consensus amongst the key stakeholders.

NOTE: Stakeholders identified by the European Commission includes members of the RFID Recommendation Informal Working Group, RACE networkRFID and the Coordination Group of the ESOs under Mandate 436.

There are many approaches to a common RFID sign. Many initiatives have focused upon logos or emblems and some on informative signs. Recognizing the contribution of the EC sponsored RACE networkRFID project to a common RFID sign the purpose outlined is to notify and inform the public about two aspects of RFID in order to foster greater public confidence in public facing RFID applications. These aspects relate to the presence of RFID tags and interrogators and, information about the RFID related application.

NOTE: Recognizing that there could be more than one RFID application at any location. Also that RFID relates to a wide variety of devices offering different levels of performance and functionality and, used in broad spectrum of applications. This is unlike most other technologies which have a common sign for public notification.

There is an understanding that there are both many types of RFID and many types of RFID related applications. Also that the purpose of the common RFID sign is neither to make the public experts in RFID nor in a broad range of RFID applications, nor to imply any such responsibility should be shouldered by the general public.

The common RFID sign best meets the goals of public notification if it is easy and quick to recognize. Additionally the

“common” in common RFID sign is understood to underline the need for consistent application and, through consistent application the RFID sign it then serves the public travelling throughout Europe.

Notification is not the same as informing the public. To this end it is necessary to consider a sign which provide the opportunity to describe the RFID related application and other associated information. This creates a challenge as such information signs take deliberate actions and time to digest their message. The consequence is that the recommended approach is to define a specification for a common RFID emblem/logo for the purpose of notification and linked to a common RFID (information) sign.

NOTE: While it is technically feasible to define RFID precisely the ‘real world’ marketing of RFID devices and services and, its common use in the public domain (anything wireless where the principle purpose is identification) results in possible confusion for either or both private individuals and, RFID operators and suppliers of tagged items. As emblems, logos and signs are for a public purpose the RFID definition adopted here is therefore “anything wireless where the principle purpose is identification.”

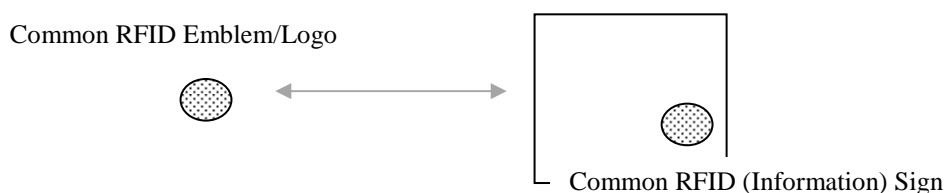


Figure 3: Simple view of RFID Emblem/logo and RFID Information Sign

10.1 Approach

The approach is to gather and structure the requirements, describe the stakeholders, compare the requirements with established signs identified by RACE networkRFID and based upon the comparison make a recommendation to the stakeholders. Depending upon the stakeholder response to the analysis and recommendation there may be a development phase after which the new proposal(s) will be analysed against the requirements and a new recommendation provided to the stakeholders.

The general notion is that due to RFIDs multiple uses in the public domain and associated with a wide range of differently performing RFID technologies there is a need for a logo/emblem to indicate RFIDs possible presence and an informative sign which can describe the RFID application and include all important information which cannot be

present on a emblem or logo. Of importance is that the common RFID sign whether emblem/logo or sign is recognizable by the general public across Europe whether they are in their home country or in another European country. Consistency in the presentation and in the location of the common European RFID sign are important success factors to achieving public notification and to minimize confusion or conflict with other emblems/logos/signs already found in the public domain. Therefore importantly the specification of the position is also taking into consideration other signs in order to encourage deployment.

10.2 Summary of RACE network RFID Report

RACE networkRFID document (ref.: WP5 Deliverable 5.1.2_final draft.pdf) identified the following requirements related to the common European RFID sign:

1. Signs need to be visible, easy to understand and provide distinctive information on RFID use
2. Signs should include or be accompanied by the name of the operator and contact information
3. Signs should be able to coexist with established signs that fulfil at least the same objectives and provide relevant information to the consumer
4. Signs should be part of a broader awareness and consumer information strategy
5. Signs should be comprehensive, unambiguous, uniform and standard compliant
6. Operators should be granted sufficient flexibility with respect to the exact placement of such signs
7. Signs should take into account and not discriminate against the global scope of certain RFID Applications
8. The signs should be neutral in regard to value judgments
9. The signs should offer sufficient flexibility to be combined with different technologies offering additional information and to use different communication technologies for public notification

These are general points which clarify many of the objectives but do not provide sufficient detail in order to define a specification or related standards.

10.3 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 information giving RFID sign has been structured into the initial requirements specification.

The following requirements have been collected from preliminary input from CEN TC225 and from the discussion within RACE networkRFID Work Package 5. The requirements do not replace a specification or standard. They are established as a basis to judge the suitability of established RFID signs and if necessary as a guide to the development of future candidate RFID signs and standards.

A key assumption is that the common European RFID sign will be introduced on a voluntary basis at least initially. Furthermore the common European RFID sign may be made mandatory in certain application areas identified by the RFID Recommendation but, that it may be adopted and used by any application without geographic boundary. For these reasons the following requirements do not imply that all the requirements are essential to every application. Nevertheless the structure of the tables is designed to identify and differentiate those stakeholder requirements which are important to ensure commonality and those which are optional for some applications.

10.4 RFID Emblem/Logo classified requirements

10.4.1 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?	<p>1) Public confidence in RFID applications through notification/awareness 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)</p> <p>2) Link to signs which explain the RFID application (see RFID sign specification)</p>	<p>Contributing to:</p> <p>1) Wider, faster paths to RFID adoption in Europe.</p> <p>2) Broader industrial applications through visibility increasing the confidence of all stakeholders and; thereby in reinforcing consistent and uniform European application of privacy & security requirements.</p> <p>3) Providing access to a broader range of trusted RFID applications serving or interacting with the public.</p> <p>4) Reinforcing European competitiveness through innovation and efficiency in broader areas of society.</p> <p>5) Increased security and safety for private individuals and organizations.</p>		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.
E.2	What is the purpose?	<p>1) Public awareness /notification of possible presence of RFID interrogators or tags</p> <p>2) Building trust through providing visibility to something which is invisible (devices small, difficult to identify, located inconsistently, often hidden, etc)</p> <p>3) Consistent presentation across EU Member states</p>	<p>1) Removing the “hidden” and “silent” aspect of RFID which generates fears of vulnerability through a loss of control to unknown 3rd parties.</p> <p>2) As a deterrent to property theft.</p>	<p>Building trust in:</p> <p>1) The application(s).</p> <p>2) The owner/operator.</p> <p>3) The technology.</p>	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?	<p>1) Suitable for all</p> <p>2) Optimized for the following:</p> <p>i) Retail environments:</p>	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
------	--	---------	-----------	---------------------	---------------------

		<p>a) On product where RFID tag or RFID interrogator embedded or associated with the product.</p> <p>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.</p> <p>c) On displays or promotional stands.</p> <p>d) On shelves.</p> <p>e) At POS.</p> <p>f) At access doorways, etc.</p> <p>g) On product advertising or promotional material where this is associated with RFID associated products or packaging.</p> <p>ii) Pharmaceutical:</p> <p>a) Product packaging.</p> <p>b) POS/dispense.</p> <p>c) Product instructions.</p> <p>d) Notifications /instructions + as retail above.</p> <p>iii) Libraries:</p> <p>a) All forms of tagged media. + as retail above.</p> <p>iv) Passports/ID document systems/Loyalty Cards.</p> <p>v) Contactless payment systems.</p>			
--	--	--	--	--	--

Ref.		Primary	Secondary	Further Information	Additional Comments
		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 bei□mplemen tatted 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 & 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 applications			Not necessarily for RFID tag manufacturers unless they are delivering RFID tags (converted or otherwise) which are or could be public facing.
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)	1) Text and/or symbols can be present but should then: i) Mention the letters “RFID”. ii) Optionally indicate the relationship with the common	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

Ref.		Primary	Secondary	Further Information	Additional Comments
		<p>presence of RFID tags or RFID interrogators and linking with the common European RFID sign.</p> <p>2) Must be visibly clearly recognizable from a minimum distance of 6 metres.</p> <p>3) Must not detract or divert attention from safety or safety related emblems/logos/signs.</p>	<p>European RFID application sign through the economic/minimal use of text, symbols or other elements.</p> <p>iii) Not confuse or detract from the application sign.</p> <p>iv) Not confuse or detract from the purpose of the emblem/logo i.e. not include a warning word or message.</p>		<p>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.</p> <p>Provisions for emblem/logo use for the purpose of public notification for technologies similar to RFID but not RFID.</p>

E.8	What information?	<p>No information provided on the logo/emblem should be <u>essential</u> to the logo/emblem meeting the requirements for public notification.</p>	<p>1) Mention of "RFID" is the only possible exception and if necessary.</p> <p>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.</p>	<p>Presence of information makes it an RFID sign (See RFID Sign below)</p>	<p>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 must only 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. 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.</p>
E.9	What communication medium?	<p>Visual:</p> <p>1) Printed (all forms of printing).</p> <p>2) Electronic display.</p> <p>i) Fixed at the location.</p> <p>a) Moderate or high resolution.</p> <p>b) Low resolution.</p> <p>ii) Mobile wireless device.</p>	<p>Touch:</p> <p>1) Embossed.</p> <p>2) Braille.</p> <p>Not audible signal.</p>	<p>Need for "Touch" optional as:</p> <p>1) There is no suitable supporting existing comparable reference. And RFID systems themselves pose no known risk to health.</p> <p>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</p>	<p>Mobile wireless devices may display an RFID emblem/logo on their electronic screen when an RFID application 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).</p>

Ref.		Primary	Secondary	Further Information	Additional Comments
				audible RFID sign information about tagged item or tagged shelf "Size S, red T-shirt", etc..	
E.10	Linking to?	RFID Signs (see below)	<p>Avoiding confusion with existing popular logos/emblems/signs:</p> <ol style="list-style-type: none"> 1) European Privacy Seal. 2) EPCglobal emblem. 3) ISO RFID Emblem. 4) RFID Passport Logo. 5) NFC Logo. 6) WiFi Logo. <p>Etc.?</p>	<p>It is important that the emblem/logo is:</p> <ol style="list-style-type: none"> 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. 	

E.11	Accessibility of technical specification/ guidance notes?	<ol style="list-style-type: none"> 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.

10.4.2 Location & Placement

Ref.		Primary	Secondary	Further Information	Additional Comments
EL.1	When?	Must 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.		<p>A sign or signs are <u>not necessary</u> 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 <u>not permitted</u> when there is an association or exchange of information between:</p> <ol style="list-style-type: none"> 1) The owner/operator of any RFID system or application which 	The exception described in further information is there to avoid an obligation on the operator to place 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
				projects an RFID electromagnetic field into the area and, 2) The area owner or lessee of the area.	

EL.2	Where?	<p>Europe: The RFID emblem/logo must be suited to placement at the following locations:</p> <ol style="list-style-type: none"> 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 	<p>Worldwide: Suitable to encourage:</p> <ol style="list-style-type: none"> 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. 	<ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 1) The RFID emblem/logo must be positioned above or to the left of any other emblem/logo associated with RFID. 2) Must be below or to the right of any: Privacy seal, National or Royal flag or emblem, etc.. 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 <u>not mandatory</u>, 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.
------	--------	---	---	---	--

Ref.		Primary	Secondary	Further Information	Additional Comments
		(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.		packaging. iii) The product is marked with the RFID emblem/logo.	
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..

10.4.3 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 must not 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	

10.5 RFID Sign classified requirements

10.5.1 General Requirements Specification

Ref.		Primary	Secondary	Further Information	Additional Comments
------	--	---------	-----------	---------------------	---------------------

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.

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. (ref. Rec. 8, page 7) 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. (ref. Rec. 9, page 7) 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 communication medium?	<p>Either or any combination of the following:</p> <ul style="list-style-type: none"> 1) Printed. <ul style="list-style-type: none"> i) Fixed sign/poster. ii) Flyer. (Must have permanent back-up). 2) Electronic display. <ul style="list-style-type: none"> i) Fixed at the location. <ul style="list-style-type: none"> a) Moderate or high resolution. b) Low resolution. ii) Mobile wireless device. 3) Projection. 4) Sound. 	<p>Optionally:</p> <ul style="list-style-type: none"> 1) Braille. 2) Acoustically delivered verbal message. 	<p>Avoiding confusion with existing popular logos/emblems/signs.</p> <p>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.</p>	Multiple media formats will be necessary and must support intention to inform all.

S.6	What form?	<p>Either or any combination of the following:</p> <ul style="list-style-type: none"> 1) Text. 2) Diagrams. 3) Video. 4) Acoustically delivered verbal message. 	<p>Optionally:</p> <ul style="list-style-type: none"> 1) Braille. 2) Acoustically delivered verbal message. 	Signs should be comprehensive, unambiguous, uniform and standard compliant.	
S.7	What information source?	<p>Either or any combination of the following:</p> <ul style="list-style-type: none"> 1) Printed sign. 2) Web page. 3) 2D bar code. 3) Electronic memory: <ul style="list-style-type: none"> i) Contact memory (e.g. USB stick). ii) Contactless electronic memory device (e.g. RFID). 	<p>Optionally:</p> <ul style="list-style-type: none"> 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?	<ul style="list-style-type: none"> 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	

Ref.		Primary	Secondary	Further Information	Additional Comments
				standard(s).	

10.5.2 Location & 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?	<p>Europe: The RFID sign must be suited to placement at the following locations:</p> <ol style="list-style-type: none"> 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. 	<p>Worldwide: Suitable to encourage:</p> <ol style="list-style-type: none"> 1) Use of the RFID sign in a way consistent with Europe. 	<ol style="list-style-type: none"> 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. 	
SL.3	How often should the emblem/logo	<ol style="list-style-type: none"> 1) Minimum once: <ol style="list-style-type: none"> i) In the vicinity of RFID emblems/logos at locations 		Where there are multiple RFID applications in the area it is considered preferable that the RFID	

Ref.		Primary	Secondary	Further Information	Additional Comments
	be repeated?	accessible to the public.		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 manor.	

10.5.3 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	

11 Environmental aspects of RFID tags and components

11.1 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). 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, 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. 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. EN50357:2001 provided the methods of assessment and EN50364:2001 was the harmonised standard which linked the methods of assessment to limits from the EC Recommendation 1999/519/EC. The reason for producing two standards was so that the EN50357:2001 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 IEC62369-1, produced by IEC106. This standard was derived from the EN50357, updated to include the latest state of the art. This was then also published in Europe as EN62369-1. The updated EN50364:2010 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. 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. EN50499:2008 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 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 (this should cover safety in the presence of both continuous emission and pulsed emissions).

11.2 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 structures to manage these aspects and any existing sector specific regulations (e.g. Waste Electrical and Electronic Equipment (WEEE) directive []).

11.3 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).

12 Standardization Gaps Analysis and Summary

12.1 Context for the Standards Gap analysis

12.1.1 Technology

The present report considers RFID technology as part of 21st century information and communication technology (ICT) where current standards are for radio frequency identifiers which are always readable, where identification is possible at multiple points, where passive unseen collection of data can take place without a person being involved in providing the data and with RFID tag data being used for multiple purposes.

Data collection can occur on an ongoing basis unlike the single data entry event inherent in ICT when data protection was originally conceived. The huge amounts of data that may be collected can now be processed so that personal behaviour and data can be deduced from what appears to be non personal data.

All these factors apply particularly to RFID and to varying extents to other 21st century technologies too.

At the periphery of any application, RFID can range from very simple un-powered tags to devices which are more complex and sometimes powered (smart cards, mobile phones etc.).

12.1.2 Market growth

To date RFID has achieved sales of billions of tags and up to a million interrogators globally with technology which was established in some cases up to 15 years ago. This represents a considerable installed base which is likely to perpetuate for some time yet. Production and hence RFID tagging of items occurs outside as well as inside Europe for supply globally both inside and outside the EU. In some key areas this means that Europe cannot formulate its own standards to fill gaps, but that progress and commitment would have to be achieved internationally.

For this type of research, the most optimistic industry forecasts for growth need to be taken into account. The most optimistic forecasts over the next 10 years indicate volumes of tags rising to hundreds of billions globally and an installed base that means today's base is 0.02% of that of 2020, i.e. 500 times greater than today. The services and facilities offered by RFID applications can be expected to increase dramatically over this period.

RFID is facing and will continue to face privacy and security challenges. Its use in some transportation systems in Europe has been compromised and security for these is being enhanced to compensate for the original security weakness. RFID growth of the scale forecast cannot be expected to be free of continuing hostile attack and exploitation which will require the revisiting of base standards with perhaps a move to newer technology than the 15 year old base.

The current technology cannot be ignored, and gaps should be filled to meet consumer and public concerns thereby supporting the industry development of the wider beneficial use of RFID in as safe and as protective a manner as possible.

12.2 Gaps in current standards

12.2.1 Overview

The standards gaps analysis have uncovered critical gaps and there is an urgent need for standardisation activities in a number of fields. 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, which is necessary to build consumer confidence and which

should be founded on the privacy by design principles and RFID privacy impact assessment. Beyond the immediate need there is the possibility of security enhancement of tags and interrogators standards to provide increased services and facilities supported by RFID tags and interrogators with potentially newer designs and technology.

12.2.2 Summary of main gaps

Table 10: RFID standards gaps summary

Technical issues	Gaps to be filled
1. Personal information inferred from 'non personal' data	<p>1.1 EU Data Protection needs to improve the interpretation of personal data to ensure inference from "non personal" data is covered by the guidance and standards applicable to Data Protection.</p> <p>1.2 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.</p>
<p>2. Tags always readable with associated fears of unauthorized reading.</p> <p>Technically this impacts upon the data to be held on the tag, read distances and the security measures on the tag.</p>	<p>Commentary – affected by this issue are requirements to support Tag "kill" functions (which could invalidate multipurpose use of tags, see point 3)</p> <p>Consumer's ability to change their minds about agreeing to data collection</p> <p>2.1 Short term: Privacy by design standards for tag data through to security throughout the rest of the system. Readers, back end systems and applications all need to be addressed to minimize privacy and security risks.</p> <p>2.2 Short term: determine maximum out of spec read distances (see discussion on RFID penetration testing standardization in annex C).</p> <p>2.3 Medium term: Enhanced on-tag control of readability with possible solutions including ability to change read distances and tag readability switching facilities.</p> <p>2.4 Longer term: smarter tags with greater access control and security.</p>
<p>3. Multipurpose tags</p> <p>Example production, sales, service and end of life</p>	<p>3.1 Medium term: Data Protection guidance and standards which ensure that for multiple purpose tags each purpose is correctly addressed.</p> <p>3.2 Medium term: Tags and interrogator standards ensuring suitable authentication and access control by each application/purpose.</p> <p>3.3 Medium term: Consumer notification and informed consent process standards especially when one purpose ends and the next starts.</p> <p>3.4 Medium term: Consumer information standards for items intended for multiple purposes.</p> <p>3.5 Longer term: possible interoperability standards for applications which make use of interrogators provided by a number of operators for multiple purposes.</p>
4. Lack of interaction capability	<p>Commentary – affected by this issue are requirements to support various Data Protection requirements</p> <p>Consumer notification of and consent given to data collection</p> <p>Minimizing data collection and purpose limitation</p> <p>4.1 Application management and operational standards.</p>

5. RFID characteristics in total	5.1 Application management and operation standards accommodating the full range of technology issues 1 to 4 above.
----------------------------------	--

12.3 RFID systems structure

Figure 5 shows 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. A detailed description of the technology and the relevant standards is provided in [annexes A and D](#).

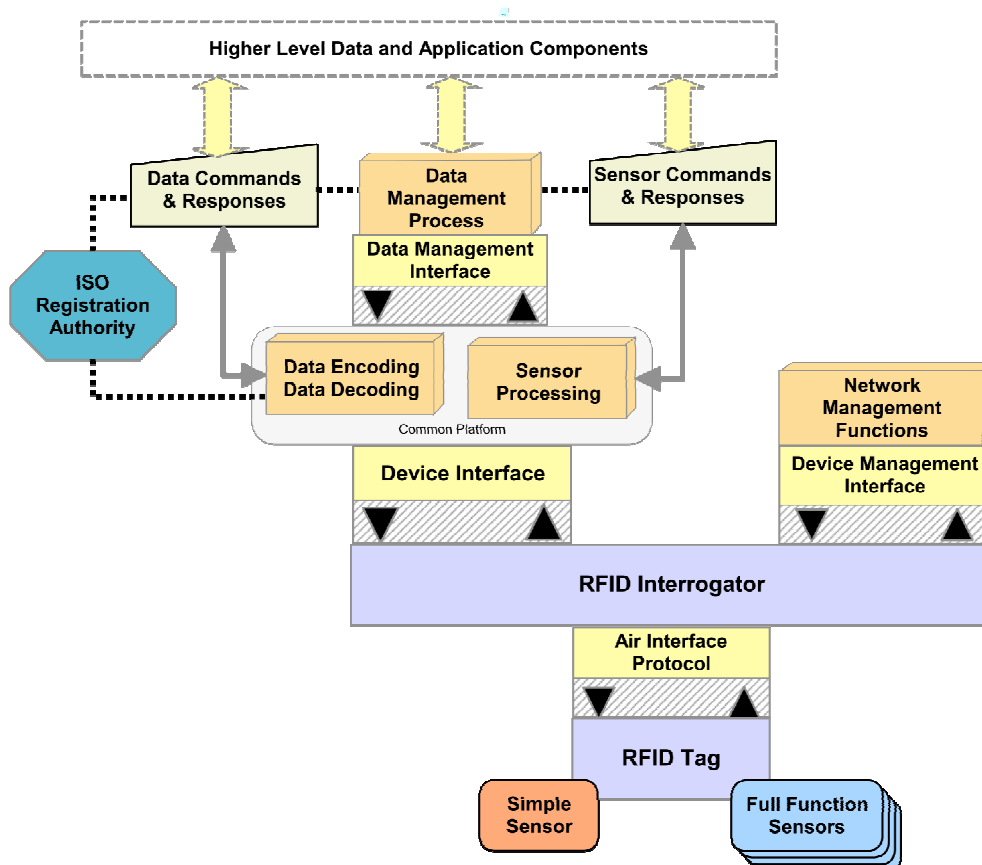


Figure 5: Schematic diagram outlining the main components in an RFID application

12.3.1 Notes on standards gaps associated with this structure

Tags

The tag types with embedded chip identities have this as a fundamental feature, often an integral part of the chip and require for any communication with the tag. Some of these tags are today also used in smart card applications. This challenges the privacy and security standardization of RFID, as it is very costly to replace large quantum of already existing and in-use tags. An option is to rather than extend these tags with privacy and security controls, for these to be address otherwise in the system.

Sensors

There are two considerations that should be addressed carefully in the future and these are:

- As disposable sensor tags are developed, killing them might reduce their useful functionality
- Sensor data, in any application, needs to be protected from tampering; so there might need to be requirements for added security

Air Interface Protocol

Many tag types require a permanent chip id for the anti-collision algorithm. As this dependency cannot easily be changed, it is important to restrict the use of the chip id to its prime purpose for use in anti-collision for basic communications, and avoid using it in back-end system.

The kill function is only supported by the 18000-6C standards and therefore only tags complying to this standard has this feature deployed. The kill function is implemented as a password string comparison, where the kill command is only invoked in cases of string matching of tag kill password and kill password received together with the kill

command. There are some challenges with the kill function as currently deployed and these are:

The 32-bit password is best encoded at the point of manufacture, but this require that the password is securely distributed, which is difficult in open systems for branded consumer goods.

Alternatively the retailer has to write a common password, for this to be invoked at the point of sale, requiring very robust stock transfer systems from back stockroom to the sales floor – quite a challenge if current processes are taken into account.

- The kill function is unlikely to be acceptable to retailers with high return rates
- The kill function might restrict the implementation of maintenance and end of life applications
- Alternative schemes like truncating part of the serial number still require a write command to be invoked for each sales transaction
- A multiple use tag (transport ticket, library RFID tag) cannot have a kill function applied without rendering the application useless

An alternative to the kill feature is to significantly reduce the read range, but such solutions are currently only proprietary.

The Interrogator

The interrogator controls access to the back-end system. Given the different technologies and proprietary interfaces, it is essential that systems that are used in applications involving the public have a means to only communication to and from authorised interrogators.

Device Interface

The only existing standards are the EPCglobal Reader Protocol and the more recent and more comprehensive (despite the name) Low Level Reader Protocol. The basic EPCglobal standard has been extended by ISO in the ISO/IEC 24791-5 standard, scheduled for publication in 2010.

ISO/IEC 24791-5 needs to be reviewed to establish whether the command set can support or be extended to support device authentication. For tag technologies where the device interface is proprietary, it might be necessary to develop specific interface APIs for authentication.

Device Management Interface

Because ISO/IEC 18000-6C RFID systems have an EPCglobal and OASIS framework for the device management interface, each needs to be examined in detail to assess whether it meets the basic requirements for privacy and security. As there are no standards for RFID systems based on other air interface protocols, new standards or guidelines are required.

Network Management Functions

As the network management functions very likely will deal with private information there is a clear need for standardising the behaviour and capabilities of these functions.

Data Encoding and Decoding

Data encoding and decoding rules are in place to ensure that only compliant data gains access to the application. These rules and application context information are used to check data and will also protect against malicious data that does not confirm to the encoding rules. However, as these rules are public they do not protect against unauthorised access to private data held on the tag. Therefore the need to include explicit personal data needs to be justified through the rigors of the PIA process.

Sensor Processing

Sensor processing are often deployed in a proprietary manner. In cases where private information are involved, the sensor processing should be standardised.

ISO Registration Authority

The detailed data dictionaries and application-specific processes are a target for identifying gaps in what are probably well-defined systems from an operation perspective, but not necessarily covering all relevant DPP and security aspects. This should be studied.

Data Management Interface

It should be investigated whether existing standards sufficiently addresses the relevant DPP and security aspects as identified by the DPP and security objectives.

Data Management Process

Need to investigate where current standards and practices for applications need enhancing to provide privacy by design when RFID is utilised along with conforming to other data protection regulations.

Data Commands and Responses

The only standard that covers this area is ISO/IEC 15961-1, which defines functional commands and responses. These are used as references for the “application side” of data encoders and decoders.

It should be investigated whether existing standards sufficiently addresses the relevant DPP and security aspects as identified by the DPP and security objectives

Sensor Commands and Responses

This is out of scope of the M436 Mandate.

A complete overview of the standards gaps are given in Annex D.

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 their status for each component is discussed in the following.

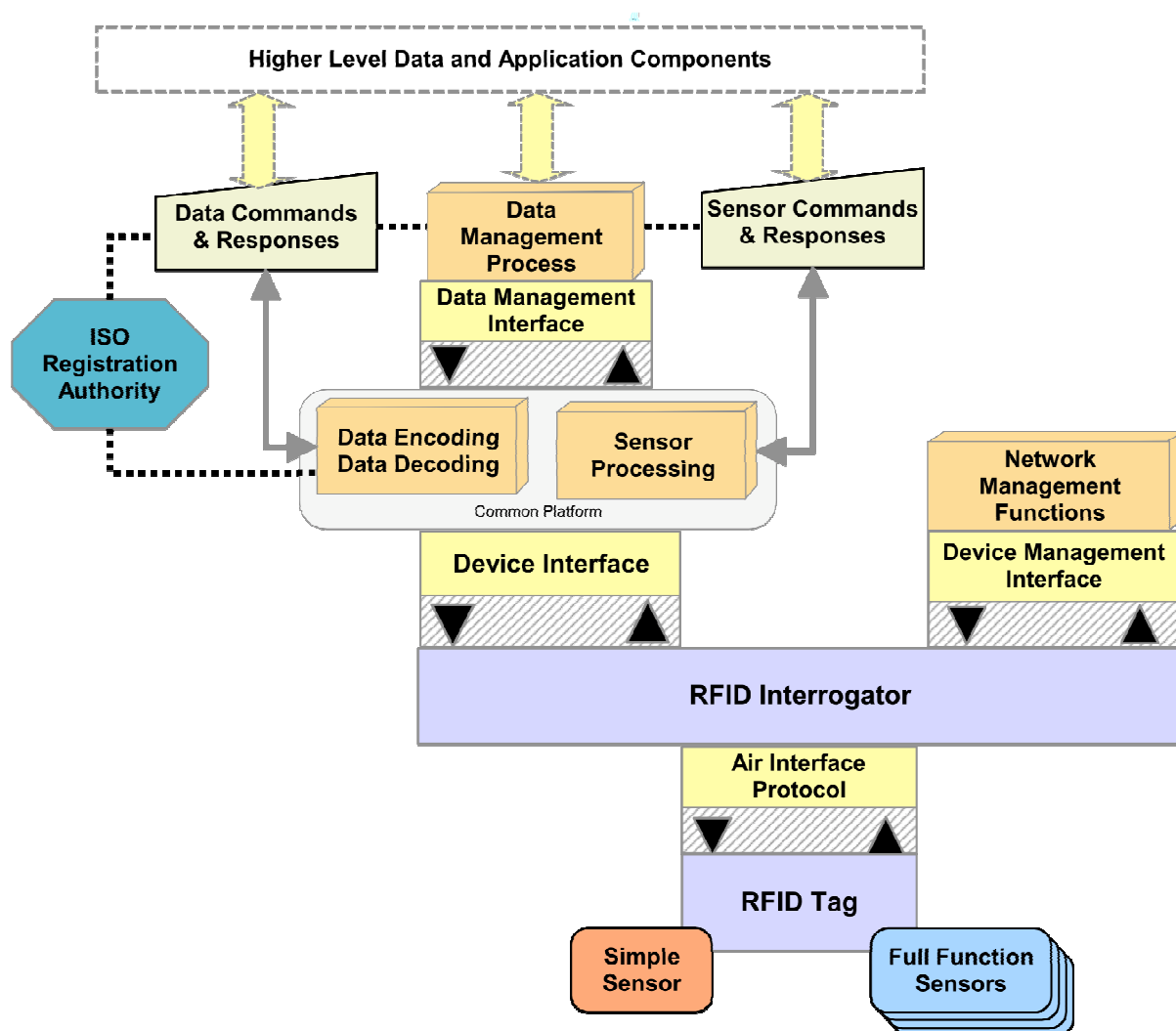


Figure A.1: Schematic diagram outlining the main components in an RFID application

RFID Tag

There are no standards that specify the requirements for the tag. What is standardised, although not necessary covering the privacy and security aspects, is the air interface. Air interface protocol standards specify how tags shall deal with commands from the interrogator. Some of these standards also specify the basic memory architecture on behalf of the tag. Tags from different vendors that conform to the same air interface protocol need to be interoperable, but may support none or a selection of the optional features described in the relevant standard.

The tag identity varies depending on the requirements specified for the particular RFID technology. Some technologies require the use of a unique chip Id for communication purposes while others use a more dynamic "session" id. All applications using a particular tag type therefore use the same tag identifier scheme.

Sensors

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. Relevant standards are close to publication for sensors to be added to ISO/IEC 18000-6 Type C and D tags. All other solutions are proprietary. Sensors are not yet supported by EPCglobal although the ISO standards apply to the type of tag that the system uses.

Air Interface Protocol

Air interface protocol standards of relevance are those in the ISO/IEC 18000 series. Each part of the standard is

currently focused on the communication frequency and therefore can specify more than one RFID technology. In addition, the 18000 series specifications specify mandatory and optional features for tags and interrogators. Manufacturers have a great flexibility resulting in numerous and rather different product variants, all compliant with the standard. The only way to properly address privacy and security is to consider each air interface protocol and its mandatory and optional features. A single technical solution cannot be applied retrospectively.

The Interrogator

There are no standards other than those related to the process behaviour with the air interface. This means that manufacturers of interrogators are given a great deal of freedom in the design and deployment of interrogators, provided that they comply with the relevant air interface standard.

Device Interface

The device interface is the communication point between the interrogator and the application. This interface is used for sending and receiving commands from the application and for remote configuration of the interrogator. Little standardisation work has been undertaken for the device interface and therefore the existing deployments are proprietary. The only existing standards are the EPCglobal Reader Protocol and the more recent and more comprehensive (despite the name) Low Level Reader Protocol. The basic EPCglobal standard has been extended by ISO in the ISO/IEC 24791-5 standard, scheduled for publication in 2010. The ISO additions also cover the encoding of data required for applications other than that of EPCglobal.

Device Management Interface

Currently, the standards being developed in this area only apply to 18000-6 Type C tags.

EPCglobal's Discovery, Configuration and Initialisation (DCI) standard was published in June 2009. The development of the ISO/IEC 24791-3 device interface standard incorporates both of EPCglobal's DCI standards and an alternative based on the device profile for web services standard (published by OASIS).

The fundamental purpose of these standards is to specify mechanisms for:

- discovery of the RFID devices and services on a local or remote subnet,
- a firmware upgrade service,
- a management service that implements configuration related functions,
- a monitoring service for reporting alerts, diagnostics, and performance information.

Network Management Functions

There are no standardisation activities for the network management functions.

Data Encoding and Decoding

The encoding process is concerned with creating the bytes that are encoded on the RFID tag. There are two groups of relevant standards:

- The EPCglobal Tag Data Standard that converts the EPC Manager, Product and Serial Number into the bit string encoded on the RFID tag.
- ISO/IEC 15962 supported by (ISO/IEC 15961, the application command standard used for encoding data

The decode process is effectively the inverse of the encoding process.

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

The rules for the ISO Registration Authority are defined in ISO/IEC 15961-2. The general idea is to have an authority to which organisations responsible for particular RFID applications (e.g. IATA) can apply for various features to be assigned and registered to enable the application to operate harmoniously with other registered applications. The data dictionaries remain under the control of the requestor (e.g. IATA) and can be used in a PIA process to identify whether private information is involved.

Data Management Interface

The standards that apply to the data management interface have a broader scope than those for the device interface. EPCglobal's Application Level Events standard addresses only the EPC UHF tag. The latest version (1.1) addresses both reading and writing of data. The development of the ISO/IEC 24791-2 data management interface standard provides support for two additional tag types, but it is important to recognise that established systems use their own mechanisms to achieve the same basic functionality.

Data Management Process

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

The only standard that covers this area is ISO/IEC 15961-1, which defines functional commands and responses. These are used as references for the “application side” of data encoders and decoders.

Sensor Commands and Responses

This is out of scope of the M436 Mandate.

Annex B: Summary of tag capabilities

B.1 Command set

The following example is taken from the ISO 18000-6 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 shall contain 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 18000-6type 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 11784/85	<135 kHz			No	No	Integrity: CRC
ISO 14223	<135 kHz			No	No	Integrity: CRC
ISO/IEC 14443	13.56 MHz	Yes	Yes	No	ISO/IEC 14443-4	Confidentiality: by passwords or keys, various solutions exist on top of the basic air interface standards ISO/IEC 14443-1, -2 and -3 Integrity: CRC and additional means Authentication: Mutual authentication Authorization: multiple keys
ISO/IEC 15693	13.56 MHz			No	No	Confidentiality: only as proprietary solutions
ISO/IEC 18000-2	<135kHz			No	No	Integrity: CRC
ISO/IEC 18000-3 Mode 1	13.56 MHz	permanently lock any block	No	No	No	Confidentiality: only as proprietary solutions Integrity: CRC
ISO/IEC 18000-3 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 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 and #ISO/IEC 29167-3 under development	Confidentiality: Access password Integrity: CRC and additional means in ISO/IEC 29167-3 Authentication: Mutual authentication Authorization: multiple keys
ISO/IEC 18000-4 Mode 1	2.45 GHz	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 18000-4 Mode 2	2.45 GHz	No	No	No	Np	Integrity: CRC
ISO/IEC 18000-6 Type A	8–0 - 960 MHz	Selectively by block	No	No	No	Integrity: CRC
ISO/IEC 18000-6 Type B	8–0 - 960 MHz	Selectively by individual 8-bit block	No	No	No	Integrity: CRC
ISO/IEC 18000-6 Type C	8–0 - 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 and ISO/IEC 29167-6 under development	Confidentiality: Access password Integrity: CRC and additional means in ISO/IEC 29167-6 Authentication: Mutual authentication Authorization: multiple keys

ISO/IEC 18000-6 Type D	8–0 - 960 MHz	Selectively in 16-bit, or 32-bit, or 64bit sequences depending on the IC manufacture	No	No	No	
ISO/IEC 18000-7	433 MHz	Yes	Yes	No	ISO/IEC 29167-6 planned	Confidentiality: Access password
ISO/IEC 18092	13.56 MHz				Various additional standards related to ISO/IEC 18092	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: RFID Penetration Testing Standardization

C.1 Short Introduction to PEN testing

Risk assessment (analysis) is an essential part of penetration (PEN) testing and should be carried out prior to or as the first activity of a PEN test. 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 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.

NOTE 1: Countermeasures may be security mechanisms, security protocols, security procedures, or detailed security requirements.

NOTE 2: In cases where the countermeasure framework consist 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 or their realization in an RFID application deployment, if such exist.

The goal of a PEN test is to check whether the countermeasure framework is complete, consistent and indeed protects the RFID system and should be carried out on the actual implementation of the system with the countermeasure framework deployed, if possible. The purpose of a PEN test is to identify and fix security weaknesses before they get exposed. Off-line or paper PEN testing can be executed on design specifications such as standards, but in such cases an additional on-site PEN test should also be carried out to analyse the security of the particular application of the standard or specification (does it actually implement the standard accordingly).

A PEN test analyses the identified vulnerabilities and other vulnerabilities discovered as part of the analysis 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 privacy sensitive information.

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 are provided up-front. The goal of the 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 stockholders 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 specific system knowledge. This means that the attack may have general knowledge about RFID, but not about the specific RFID application being analysed. The tester will use all of the tricks and methodologies at their disposal in an effort to emulate the persistence, knowledge and expertise level of potential attackers. The tester may also use specialized equipment that are normally only available to producers or operators of the RFID application to emulate the power and abilities of professional attackers or attacker networks. A black box PEN testing is usually more expensive than white box PEN testing.

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 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.

C.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. 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) 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

C.3 RFID PEN testing standardization issues and roadmap

The scope of RFID goes beyond that of RFID technology and includes the application or the way in which RFID is used. It covers not only the tag, the interrogator and the RF link, but also the tagged item, back end system and any network connection between the interrogator and the back end system as shown in figure C.1. This means that the responsibility of preserving privacy and protecting an RFID system from being exploited not only lies in the hand of those producing or integrating RFID technology (system integrators), but also those providing the back end system. This also means that security measures or the placement of privacy relevant information can be distributed among the components in the RFID ecosystem accordingly. For example, if the tag cannot tackle the necessary cryptography requirements for the information that it is intended to record or hold, 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.

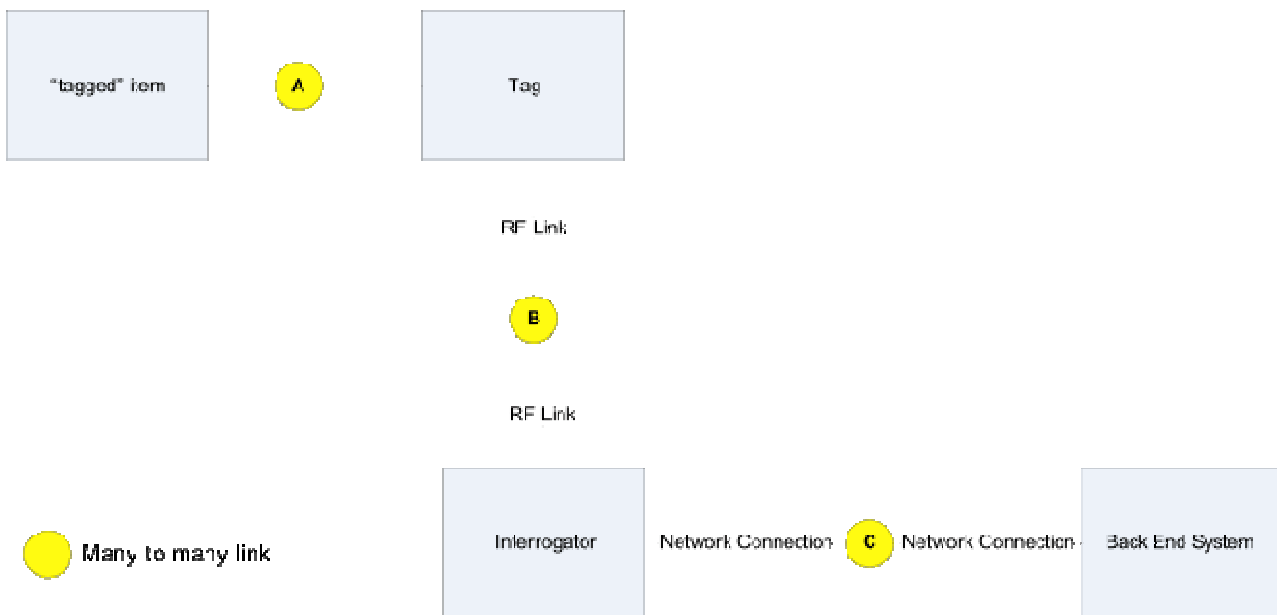


Figure C.1: Simple view of RFID ecosystem

As a consequence, RFID PEN test guidelines must be developed for all components of the RFID ecosystem (for some of the components it will be possible to reuse existing PEN testing methodology) and to analyse the specific RFID application deployment (system integration PEN testing). We envision specific PEN testing guidelines for the RFID technology (tag and interrogator) and the reuse of existing PEN testing methodology and analysis for the RF link, the network connection to the back end system and the back end system. We also envision the need for a specific RFID system integration PEN test guidance and standards.

There will be multiple RFID sectors and RFID applications or ecosystems within each sector that may have varying level of privacy and security needs. We therefore need to identify and describe these RFID sectors and analyse their privacy and security needs. The privacy and security objectives for RFID in general are outlined in the main body of this document and these together specify the privacy and security needs of a general RFID ecosystem. More specifically, the privacy and security objectives together define the parameters that the RFID ecosystem needs to preserve or ensure. The identified vulnerabilities all relate to one or more of the objectives and the threats describe ways to exploit the RFID system such that one or more of its privacy or security objectives are not fulfilled or provided to an appropriate level. What the appropriate level is are specific to an RFID sector and the RFID applications belonging to this sector and must be defined for each RFID application category. This level is what we should use to select the scope of the PEN test on a case-by-case basis. An example of existing RFID application levelling is given in the PIA draft "RFID Application; Privacy and Data Protection Impact Assessment Framework". We could decide to reuse or adopt these. However, it is recommended to rather define the levelling based on the privacy and security objectives.

Below is an outline of a roadmap for RFID PEN testing standardization. The goal is to produce standards that are feasible and easy to employ and follow in practice:

1. Identify RFID sectors and their associated RFID application/ecosystem categories
2. Analyse each RFID application category to identify the relevant privacy and security objectives (from the list of privacy and security objectives given in clause 7.3)
3. Define RFID application category levels based on the result of (1) and (2)
4. Identify the vulnerabilities of relevance for each RFID application category by examining the relevance or presence of the associated weakness (see table C.1)
5. Describe PEN tests based on the threats scenarios of relevance to the vulnerability set identified in (4) (the threats listed in the Threat column in table C.1). Note that there should be one or more tests (attack scenarios) per threat and that these tests or attack scenarios is what the PEN tester will perform during the PEN test.
6. Identify existing PEN testing methodology of relevance

7. Develop any missing PEN testing methodology
8. Write PEN testing standard for each component of the RFID ecosystem and one or more standards for RFID ecosystem integration PEN testing (system-wide deployment PEN test)

Note that the list of vulnerabilities given in table C.1 is just a draft list based on the knowledge available at the time and that it must be continuously updated and revised. Also note that there is a need to associate the vulnerabilities listed in table C.1 to the components in the RFID ecosystem (figure C.1) for each RFID ecosystem. This should be structured according to the RFID ecosystem categories or sectors. What will be done in the PEN test is to try to exploit each of the vulnerability in the relevant vulnerability set within the scope of a particular RFID PEN test. The most effective way of doing this is to examine the list of weaknesses and evaluate whether it is relevant for the specific RFID application. If not, the associated vulnerability is not within scope. This is how one limits the scope of the PEN test. If the countermeasures employed are sufficient, it should not be possible or be very hard to exploit the relevant vulnerabilities.

Table C.1: List of vulnerabilities to an RFID ecosystem

Vuln. No.	Weakness	Threat
V1	Lack of respect of the data minimization and proportionality principles	T18-Spoofing of credentials / bypass authentication; T19-Large-scale and/or inappropriate data mining and/or surveillance; T20-Masquerade; T33-Tracking
V2	Lack of respect of the purpose limitation (finality principle)	T-11 Procedures / instructions not followed leading to tags being used passed end of purpose
V3	Lack of respect of the transparency principle	T-24 Non-compliance with data protection legislation; T-30 Exclusion of the data subject from the data processing process due to disabling of RFID tag
V4	Inappropriate / inadequate identity management	T18-Spoofing of credentials / bypass authentication; T20-Masquerade; T-21 Social engineering attack; T-22 Identity theft; T32-Trivialization of unique identifiers
V5	Inherent features (size, material etc.): easy to lose, to be stolen and/or copied (especially for RFID tags)	T8-Theft
V6	Actual RFID range longer than standard	T-11 Procedures / instructions not followed leading to tags being used passed end of purpose; T18-Spoofing of credentials / bypass authentication; T20-Masquerade; T-21 Traffic analysis / scan / probe; T33-Tracking
V7	RFID tags do not have a turn-off option	T-21 Traffic analysis / scan / probe; T-22 Identity theft; T33-Tracking
V8	Insufficient protection against reverse engineering	T12-Cloning of credentials and tags (RFID related); T27-Fake / rogue RFID readers / scanning of RFID reader and /or tag
V9	Inadequate security measures of data storage (e.g. inadequate encryption measures)	T16-Worms, viruses & malicious code; T-17 Low acceptance of devices / equipment / procedures; T-21 Social engineering attack; T29-Profiling; T33-Tracking
V10	Over-sensitivity of devices (generating many false alarms)	T15-Malfunctioning/breakdown of systems /devices / equipment
V11	Sensitivity to magnetic fields	T14-Physical RFID tag destruction
V12	Communication of data over unprotected or publicly accessible channels	T7-Man-in-the-middle attack; T29-Profiling; T33-Tracking
V13	Data linkability	T19-Large-scale and/or inappropriate data mining and/or surveillance; T-28 Data linkability; T33 Tracking

V14	Lack of data correction mechanisms (as normally data subjects do not have access to the databases)	T9-Unauthorised access to / deletion / modification of devices / data etc; T10-Use erroneous and/or unreliable data
V15	Lack of common or harmonized legislation in EU Member States	T9-Unauthorised access to / deletion / modification of devices / data etc; T13-Illicit access to data; T19-Large-scale and/or inappropriate data mining and/or surveillance; T-30 Exclusion of the data subject from the data processing process due to disabling of RFID tag
V16	Insufficient protection of data communication (weak or no encryption etc.)	T7-Man-in-the-middle attack; T13-Illicit access to data; T-26 Side channel attack; T32-RF eavesdropping; T33-Tracking
V17	Lack of respect to the legitimacy of data processing, e.g. consent	T-24 Non-compliance with data protection legislation; T-25 Function creep (data used for other purposes than the ones for which they were originally collected)
V18	Lack of respect to the data conservation principle	T-24 Non-compliance with data protection legislation; T-28 Data linkability; T-30 Exclusion of the data subject from the data processing process due to disabling of RFID tag
V19	Lack of respect to the rights of the data subject (such as the right for rectification, blocking or deletion of data)	T7-Man-in-the-middle attack; T9-Unauthorised access to / deletion / modification of devices / data etc; T10-Use erroneous and/or unreliable data; T13-Illicit access to data
V20	Insufficient protection against DoS attacks	T1-Denial of service attack / flood / buffer overflow; T2-Blocking; T3-Collision attack; T4-Blocking; T5-De-synchronization; T6-Replay

In addition, it is useful at this point to be aware of some of the key factors that make a good PEN test and which should be addressed in RFID PEN testing standards and guidelines.

- **Establish the parameter:** Defining the scope of work is the first and most important step to performing a successful penetration test. This will define the boundaries, objectives and the validation of procedures (the success criteria).
- **PEN tester skills and ethical responsibilities:** A successful and effective PEN test relies on skilled and experienced consultants to perform the test. It is important to advice clients in need of PEN tests to ensure that the PEN tester are:
 - Legally capable
 - Experienced
 - Ethical responsible
- **Choose adequate set of tests:** Manual and automated tests will normally yield the best balance of costs and benefits for PEN tests. This means that an RFID PEN testing standard should provide general advice on how to employ and combine black, white and grey box PEN testing.
- **Follow a methodology:** PEN testing is by no mean a guessing game. Everything needs to be planned, documented and followed, requiring structured PEN testing methodologies.
- **Resulting value:** The results should be documented carefully and efforts should be made to make them understandable to the client. Whether it's a technical report or an executive summary, there is always a need to explain. The security consultant/tester should be available to answer queries or explain results.
- **Findings and recommendations:** This is a very important part of a PEN test. The final report must clearly state the findings and must map the findings to the potential risks. This should be accompanied by a balanced remediation roadmap based on RFID security best practices which should be developed as part of the RFID PEN testing standardization efforts.

C.4 Conclusion and Recommendations

RFID PEN test standards and guidelines should cover all of the components in the RFID ecosystem as shown in Figure C.1 and provide test guidelines for each component separately. The standard should also include guidelines for a deployment or system integration PEN testing, to ensure that not only each component are security robust, but also their integration into a specific RFID ecosystem.

The RFID PEN test standards should also provide RFID sector specific guidelines and account for the variety of privacy and security requirements to applications within one RFID sector resulting in PEN tests of various cost and resource demands.

Annex D:

Gap analysis in standardisation

The table that follows identifies where gaps have been identified in existing standardisation and the nature of the standard that is required to fill the gap is indicated.

Ref	Requirement Description	Tag	Tag to Reader Interface	Reader	Reader to Back End System Interface	Application and multi application	RFID Open System Data Design	RFID Open System Operations	Carry over to other standards areas
DPPO-1	Privacy and security by design	A Tag access and security	A Tag access and security						1 Notification of reading process
				B Control of data read by application					
		C Tag kill	C Tag kill	C Tag kill					
DPPO-2	CSP privacy and security measures							F Included in 2	2 Informed consent procedural standard
DPPO-3	Gathering of personal data		D Authentication	E Access control					
DPPO-4	Per app information policy						G System operational standards	G System operational standards	3 RFID App management standards inc PIA and mitigation
DPPO-5	Consumer information inc signs and signage								4 Consumer information standards both for signs and for apps
DPPO-6	Informed consent								2 and 4
DPPO-7	Legitimate means of collection			H Reader authorisation by application	H Reader authorisation by application				

DPPO-8	Data quality			H Reader authorisation by application	H Reader authorisation by application				part of 3
DPPO-9	Personal data minimisation	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard		
DPPO-10	Personal data on tag storage	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard		
DPPO-11	Tracking without traditional identifiers	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard	I RFID system Privacy by design standard		I ++ new standards of tag technology
DPPO-12 (relates to DPPO-8)	Purpose limitation								part of 3
DPPO-13 (relates to DPPO-8)	Use limitation							J Operational audit standards	part of 3
DPPO-14	Access to own personal info on tag	K System data access by design standard	K System data access by design standard	K System data access by design standard	K System data access by design standard	K System data access by design standard	K System data access by design standard	part of G	part of 3
DPPO-15	Access to own personal info in system	K System data access by design standard	K System data access by design standard	K System data access by design standard	K System data access by design standard	K System data access by design standard	K System data access by design standard	part of G	part of 3

DPPO-16	Risht to recify incorrect data	part of K	part of K	part of K	part of K	part of K	part of K	part of G	part of 3
DPPO-17	Tag deletion	L addition of tag facilites				M deletion and modification in multi app environemnt	part of I	Part of G	part of 3
DPPO-18	Rendering Tag non readable (reversable)	part of L				part of M			
DPPO-19	Tag user selected non readability (reversable)	part of L				part of M			
DPPO-20	Hamonised interoperable privacy based RFID systems	Part of I	Part of I	Part of I	Part of I	Part of I	N Open system interoperability design standards	O System interoperability service/procedures standards	5 RFID Interop maangement - agreemments, service levels etc standards
DPPO-21	Remove privacy and DPP uncertainty as to aplicability								part of 3 - clear classification of apps - do they involve people being in possession of tagged items ?
DPPO-22	Innovation and more apps for RFID								6 Dissemination of standrads role in reducing privacy etc risks with publically credible compliance regime

DPPO-23	Mitigating privacy etc risks in Public service and B2C markets	P System penetration testing standards (for different categories of app privacy etc risk)	P System penetration testing standards (for different categories of app privacy etc risk)	P System penetration testing standards (for different categories of app privacy etc risk)	P System penetration testing standards (for different categories of app privacy etc risk)	P System penetration testing standards (for different categories of app privacy etc risk)	P System penetration testing standards (for different categories of app privacy etc risk)	P System penetration testing standards (for different categories of app privacy etc risk)	7 EU Penetration tests followed by acceptable penetration resistance standard with respect to those tests
DPPO-24	PIA responsible people								part of 3
DPPO-25	PIA availability of assessments								part of 3
DPPO-26	PIA implementation of provisions	part of I	part of I	part of I	part of I	part of I	part of I	part of I	part of 3

SO-1	Revelation: personal information, behavioural information and data related to possessions on tag to authorised parties only	part of K and I	part of K and I	part of K and I	part of K and I	part of K and I	part of K and I	part of K and I	
------	---	-----------------	-----------------	-----------------	-----------------	-----------------	-----------------	-----------------	--

	Revelation: personal information, behavioural information and data related to possessions on tags by legitimate means only								
SO-2		part of K	part of K	part of K	part of K	part of K	part of K	part of K	
SO-3	access to personal information, behavioural information and data related to possessions in system by authorised parties only	part of K	part of K	part of K	part of K	part of K	part of K	part of K	
SO-4	No non legitimate access to any part of ecosystem within system	part of K	part of K	part of K	part of K	part of K	part of K	part of K	
SO-5	Access to ecosystem 'outside' legitimate system	Q System design for security standard	Q System design for security standard	Q System design for security standard	Q System design for security standard	Q System design for security standard	Q System design for security standard	Q System design for security standard	part of 3
SO-6	Modification of data in ecosystem by others outside legitimate system	part of Q	part of Q	part of Q	part of Q	part of Q	part of Q	part of Q	part of 3

SO-7	Deletion . Removal of data in ecosystem by others outside legitimate system	part of Q	part of Q	part of Q	part of Q	part of Q	part of Q	part of Q	part of 3
SO-8	Legitimate access blocking by illegitimate means within ecosystem	part of Q	part of Q	part of Q	part of Q	part of Q	part of Q	part of Q	part of 3
SO-9	Legitimate access blocking by illegitimate means outside ecosystem	part of Q	part of Q	part of Q	part of Q	part of Q	part of Q	part of Q	part of 3
SO-10	Identity should not be comprised by any action of the system	Combination of I, K and Q - validation of system operation requirement ?	Combination of I, K and Q - validation of system operation requirement ?	Combination of I, K and Q - validation of system operation requirement ?	Combination of I, K and Q - validation of system operation requirement ?	Combination of I, K and Q - validation of system operation requirement ?	Combination of I, K and Q - validation of system operation requirement ?	Combination of I, K and Q - validation of system operation requirement ?	part of 3
SO-11	Users should not become targets	part of I	part of I	part of I	part of I	part of I	part of I	part of I	part of 3

Reader Device Interface	Reader Device management interface	Data encoding	Data management interface	Data commands and resonses	ISO Sector standards
-------------------------------	---	------------------	---------------------------------	----------------------------------	-------------------------

Annex E: Bibliography

E.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

E.2 GRIFS database extract

<<To be included in final report – refer to GRIFS via the Internet>>

E.3 Sign Related Standards

E.3.1 In development

Reference	Title	Scope or sector for use	Notes
ISO 20712-1	Water safety signs and beach safety flags Part 1: Specifications for water safety signs used in workplaces and public areas	Environmental, water hazards	
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-related 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.		
EN ISO 24502	Ergonomics - Accessible design - Specification of age-related relative luminance in visual signs and displays	Ergonomic guidance	
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 pictoria-s - General principles		
--	---	--	--

E.3.2 Published

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 3864-1:2002 is applicable to 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, generally speaking, to those sectors subject to a regulation which may differ.

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 17398:2004 does not cover electrical power supplies, their components or electrically powered elements. It also does not cover properties of illuminating components, but the photometric properties for the particular types of safety signs are covered.

ISO 7010:2003 prescribes safety signs for the purposes of accident prevention, fire protection, health hazard information and emergency evacuation.

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 7010:2003 specifies the safety sign originals that may be scaled for reproduction and application purposes.

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 23601:2009 is not intended to cover the plans to be used by external safety services nor detailed professional technical drawings for use by specialists.

ISO 20712-1:2008 prescribes water safety signs intended for use in connection with the aquatic environment. It is intended for use by owners and operators of aquatic environments and by manufacturers of signs and equipment. However, it is not applicable to signalling used for maritime traffic.

ISO 20712-1:2008 specifies the water safety sign originals that may be scaled for reproduction and application purposes.

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/IEC Guide 74:2004 gives procedures for the development of graphical symbols for public information, use in safety signs and product safety labels, and use on equipment and products.

ISO/IEC Guide 74:2004 does not cover road traffic signs and graphical symbols for use in technical documentation.

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 22727:2007 specifies requirements for the creation and design of public information symbols. It specifies requirements for the design of public information symbols for submission for registration as approved public information symbols, including line width, the use of graphical symbol elements and how to indicate negation. It also specifies templates to be used in the design of public information symbols.

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/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).

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 hazard pictorial -- General principles

ISO 16069:2004 describes the principles governing the design and application of visual components used to create a safety way guidance system (SWGS).

ISO 16069:2004 contains general principles valid both for electrically powered and for phosphorescent components. Special information which is related to the type of component is given to assist in defining the environment of use, choice of material, layout, installation and maintenance of SWGS.

ISO 16069:2004 does not cover risk assessment. Applications with different risks to the occupants typically require different layouts and types of SWGS. The specific application and exact final design of SWGS is entrusted to those persons responsible for this task.

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 16069:2004 is intended, by collaboration and coordination, to be used by all other Technical Committees within ISO and IEC charged with developing SWGS for their specific requirements. ISO 16069:2004 is not to be used for ships falling under regulations of the International Maritime Organization (IMO).

ISO 16069:2004 describes the principles governing the design and application of visual components used to create a safety way guidance system (SWGS).

ISO 16069:2004 contains general principles valid both for electrically powered and for phosphorescent components. Special information which is related to the type of component is given to assist in defining the environment of use, choice of material, layout, installation and maintenance of SWGS.

ISO 16069:2004 does not cover risk assessment. Applications with different risks to the occupants typically require different layouts and types of SWGS. The specific application and exact final design of SWGS is entrusted to those persons responsible for this task.

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 16069:2004 is intended, by collaboration and coordination, to be used by all other Technical Committees within ISO and IEC charged with developing SWGS for their specific requirements. ISO 16069:2004 is not to be used for ships falling under regulations of the International Maritime Organization (IMO).

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 3864-2:2004 is applicable to all products in all industries where safety-related questions can be posed. However, it is not applicable to safety labels used for chemicals, for the transport of dangerous substances and preparations, and in those sectors subject to legal regulations which differ from certain provisions of this document.

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.

IEC 80416-1:2008 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)..

History

Document history		
V0.0.0	February 2010	First outline of ToC for STF396 review
V0.0.1	April 2010	Approved output of TISPAN#24W
V0.0.2	April 2010	Input to ERM TG34 for review/discussion
V0.0.3	May 2010	Development within the STF for finalisation
V0.0.4	July 2010	Preparation for submission to public consultation
V0.0.5	July 2010	Public consultation review version
V0.0.6	July 2010	Submission to public consultation