PAS 94:2013

Implementing privacy impact assessment (PIA) frameworks in radio frequency identification (RFID) applications – Guide

Department for Business Innovation & Skills

bsi.

Publishing and copyright information

ISBN 978 0 580 76452 3

ICS 33.060.99, 47.020.70, 33.040.40

Publication history

First published May 2013

Contents

Foreword ii

Introduction iii

1 Scope 1

2 Terms and definitions 2

3 The PIA process 3
3.1 General 3
3.2 Outline 3
3.3 Description of the application 4
3.4 Initial analysis phase 4
3.5 Full-scale PIA process 5
3.6 Small-scale PIA process 5
3.7 Risk assessment phase 5
3.8 Identification of risks 5
3.9 Deactivation of tags 5
3.10 Identification and recommendation of controls 6
3.11 Documentation of resolution and residual risks 6
3.12 PIA report 6

4 The common European RFID notification signage system 7
4.1 General 7
4.2 Definition of the common European notification signage system 7
4.3 The common RFID emblem 7
4.4 Purpose of the application 8
4.5 Contact point 8
4.6 Name of the operator of the application 8
4.7 Contact method 9
4.8 Placement of common European RFID notification signs 9
4.9 Presence of readers 9
4.10 Presence of tags 10
4.11 Signage on tagged items 11
4.12 Signage on embedded tags 11
4.13 Guidelines on additional information 11

Annexes
Annex A (informative) Overview of automatic identification and privacy 12
Annex B (informative) Description of the RFID application 15
Annex C (informative) Protecting the privacy of the individual: the EC approach to RFID 20
Annex D (informative) Case studies for the use of RFID notification signage 21

Bibliography 23

List of Figures
Figure 1 – Decision tree on whether and at what level of detail to conduct a PIA 4
Figure 2 – Generic BS ISO/IEC 29160 RFID emblem 8

List of Tables
Table B.1 – Risks that can impact on privacy objectives 17

Foreword

This PAS was commissioned by the UK Department for Business, Innovation & Skills (BIS). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came in to effect on 31 May 2013.

Acknowledgement is given to the following organizations that were involved in the development of this PAS as members of the Steering Group:

- Avery Dennison
- BSI Consumer & Public Interest Network
- Chartered Institution of Logistics and Transport
- Department for Business, Innovation & Skills
- GS1 UK
- London School of Economics
- Marks and Spencer

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a specification to be rapidly developed in order to fulfil an immediate need in industry. A PAS may be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

As a guide, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in italic type, and does not constitute a normative element.

Spelling conforms to The Shorter Oxford English Dictionary. If a word has more than one spelling, the first spelling in the dictionary is used.

Contractual and legal considerations

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

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction

0.1 Background to RFID and data/privacy protection (DPP)

Radio frequency identification RFID tags in devices such as mobile phones, computers, fridges, books and cars bring many potential advantages for businesses, public services and consumer products.

Examples include improving product reliability, energy efficiency and recycling processes, paying road tolls without having to stop at toll booths, cutting time spent waiting for luggage at the airport and lowering the environmental footprint of products and services.

Similarly, many hospitals use RFID tags to track inventory and identify patients. While this technology can improve the overall quality of healthcare, the benefits should be balanced with privacy and security concerns.

The use of RFID systems can potentially create privacy, security and data protection risks.

Personal data might be read from RFID tags without the permission of the individual concerned. Even where personal data is appropriately obtained, risk can develop through insecure storage.

An emerging challenge is that of scale. McKinsey Global Institute (MGI) (May 2011) has noted that the amount of data being captured by organizations is growing exponentially, and analysing large data sets (so called "big data") will become a key driver of competition and economic growth.

Big data typically creates value by establishing and analysing relationships between many different pieces of data. Some of this data will be personal in nature, and individual privacy could be endangered by this process of data mining, e.g. associating an individual with the real time location data from their car, mobile phone and transport card.

Whilst the scenario of pervasive data collection is a recent phenomenon, the underlying issues of protection of data and personal privacy are not.

It is important that any organization considering the installation of a RFID system appreciates that the system should be compliant with existing data and personal privacy protection legislation.

In 2008, the European Commission issued a standardization mandate 436 [1] to the European standardization organizations CEN, CENELEC and ETSI in the field of information and communication technologies applied to RFID systems. The mandate addressed data protection, privacy and information security aspects of RFID. In response to this mandate, European Standards on the privacy impact assessment (PIA) process for use in RFID applications and on the public notification signage associated with RFID applications will be published in 2014.

0.2 Purpose of this PAS

This PAS acts as a bridging document until the European Standards are published, and is also intended to stimulate input to the public enquiry stage of the European Standards which will take place between March 2013 and July 2013. This input will be channelled through the secretariat of the relevant BSI technical committee IST/34, Automatic identification and data capture techniques.

The guidance is designed to help an organization achieve and maintain compliance with existing national legislation on data and personal privacy protection.

This page deliberately left blank.

1 Scope

This PAS gives guidance on implementing privacy impact assessment (PIA) frameworks in radio frequency identification (RFID) applications. It explains:

a) how to carry out a PIA to:
   i) evaluate potential risks to personal privacy;
   ii) mitigate these risks;
   iii) record any residual risk;
b) how to design and place signage to notify the public that:
   i) they are entering an area where RFID readers might be operating;
   ii) an item is carrying a RFID tag.

Together with the public notification sign, the PIA process provides a common approach within the European Union (EU) to achieve compliance with public privacy and data protection principles.

The RFID application operator is responsible for carrying out the PIA process.

This PAS is relevant where RFID readers are located in spaces where the public might have access, and/or where items carrying RFID tags might pass through areas to which the public might have access.

This PAS is intended for use by general managers and by ICT specialists in all economic sectors and all sizes of organization, and is written in the context of the introduction of the RFID PIA methodology within Europe.

This PAS is applicable to all public and private organizations within the EU operating, or considering the implementation of, a RFID system.