PD CEN/TR 16673:2014

BSI Standards Publication

Information technology — RFID privacy impact assessment analysis for specific sectors

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 16673:2014.

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

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

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

Published by BSI Standards Limited 2014

ISBN 978 0 580 83898 9
ICS 35.240.60

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

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

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16673

June 2014

ICS 35.240.60

English Version

Information technology - RFID privacy impact assessment analysis for specific sectors

Technologies de l'information - Évaluation d'impact sur la vie privée des applications RFID dans des secteurs spécifiques

Informationstechnik - Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID für spezifische Sektoren

This Technical Report was approved by CEN on 20 January 2014. It has been drawn up by the Technical Committee CEN/TC 225.

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

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

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

Ref. No. CEN/TR 16673:2014 E

Contents

Page

Foreword

This document (CEN/TR 16673:2014) has been prepared by Technical Committee CEN/TC 225 “AIDC Technologies”, the secretariat of which is held by NEN.

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

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

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

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

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

— CEN/TR 16684, *Information technology — Notification of RFID — Additional information to be provided by operators*

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

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

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

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

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

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

Introduction

In response to the growing deployment of RFID systems in Europe, the European Commission published in 2007 the Communication COM(2007) 96 'RFID in Europe: steps towards a policy framework'. This Communication proposed steps which needed to be taken for a wider take up of RFID whilst respecting the basic legal framework safeguarding fundamental values such as health, environment, data protection, privacy and security.

In December 2008, the European Commission addressed Mandate M/436 to CEN, CENELEC and ETSI in the field of ICT as applied to RFID systems. The Mandate M/436 was accepted by the ESOs in the first months of 2009. The Mandate addresses the data protection, privacy and information aspects of RFID, and is being executed in two phases. Phase 1, completed in May 2011, identified the work needed to produce a complete framework of future RFID standards. The Phase 1 results are contained in the ETSI Technical Report TR 187 020, which was published in May 2011.

Phase 2 is concerned with the execution of the standardisation work programme identified in the first phase.

This Technical Report is one of eleven deliverables for M/436 Phase 2. Its focus is on four major sectors that have a number of implementations of RFID that currently impact European society. Using these as detailed case studies will assist in addressing the development of the standard on the Privacy Impact Assessment. For the purpose of this work, the definitions of "RFID Operator" and "RFID Application" will be those provided in the EC RFID Recommendation of 2009-05-12.

1 Scope

The scope of this Technical Report is to use the RFID PIA Framework as the basis for exploring issues with four major sectors involved with RFID:

— libraries;

— retail;

— e-Ticketing, toll roads, fee collection, events management;

— banking and financial services.

After specific sector research and consolidation of the results of industry workshops and seminars that take place in several EU Member States, this Technical Report will identify the characteristics that need to be taken into consideration by operators of RFID systems in the example sectors. In addition it will provide advice to operators in the sector on significant variants both in terms of technology and application data. This will enable the appropriate risk factors to be taken into account.

Based on the synthesis of the applications in the chosen sectors, this Technical Report will also identify a set of factors relevant to specific RFID technologies and features that will need to be taken into account in preparing a Privacy and Data Protection Impact Assessment for many RFID applications.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE Definitions are derived from EU Recommendation C(2009) 3200 final, EU Directive 95/46/EC, ISO/IEC 19762 (all parts)

2.1
data controller
controller
natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law

2.2
data subject's consent
any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed

2.3
identified or identifiable person
person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

2.4
individual
natural person who interacts with or is otherwise involved with one or more components of an RFID application (e.g., back-end system, communications infrastructure, RFID tag), but who does not operate an RFID application or exercise one of its functions. In this respect, an individual is different from a user. An individual may not be directly involved with the functionality of the RFID application, but rather, for example, may merely possess an item that has an RFID tag

2.5