PD CEN/TR 16674:2014
Incorporating corrigendum March 2016

BSI Standards Publication

Information technology — Analysis of privacy impact assessment methodologies relevant to RFID

bsi.

National foreword

This Published Document is the UK implementation of CEN/TR 16674:2014.

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 2016

ISBN 978 0 580 92901 4
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
31 May 2016	Implementation of CEN Correction Notice 25 June 2014: Title modified

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16674

June 2014

ICS 35.240.60

English Version

Information technology - Analysis of privacy impact assessment methodologies relevant to RFID

Technologies de l'information - Analyse des méthodes d'évaluation de l'impact sur la vie privée adaptées à la RFID

Informationstechnik - Analyse zur RFID-Datenschutzfolgenabschätzung für bezifische 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 16674:2014 E

Contents

Page

Foreword

This document (CEN/TR 16674:2014) 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

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

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

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

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

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 to reduce barriers to adoption of RFID whilst respecting the basic legal framework safeguarding fundamental values such as health, environment, data protection, privacy and security.

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

Phase 2 is concerned with the execution of the standardization work program identified in the first phase.

This Technical Report is one of eleven deliverables for M/436 Phase 2. From a current point of view, and despite their name, most Privacy Impact Assessments in the world have a narrow focus, namely data protection rather than privacy protection. The result is that many PIAs are restricted to legal compliance checks and do not include societal aspects. That is reflected in the form of some PIAs, which are limited to checklists. Increasingly, however, PIA methodologies include narrative descriptions of the systems assessed and the environments in which they will operate, which help to understand better the potential privacy and data protection risks.

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

This deliverable will begin with research of methodologies used for wireless technologies and the risks associated at within that part of the wireless system from the data carrier to the communication from the 'interrogator' or data capture device to the application system. The reason for this approach is to understand approaches used by security experts and that are not incorporated into any existing standards. This approach makes sense because it moves from the generic wireless towards the specific RFID issues. The intention is to draw relevant 'lessons' from a range of wireless technologies that can be applied to RFID technologies and applications. Risk management will focus on areas that accept the inherent risks of the given technology.

1 Scope

The scope of this Technical Report (TR) is to identify methodologies that are used for, or have been considered applicable to, wireless technologies. These methodologies are analyzed to identify features that are applicable to RFID.

Based on the Industry RFID PIA Framework endorsed by the Article 29 Data Protection Working Party, the Technical Report focuses on proposing risk analysis methodologies suitable for the data capture area of an RFID system. This includes the RFID tag, the interrogator, the air interface protocol used for communication between them, and the communication from the interrogator to the application.

The Technical Report also proposes risk management features based on the inherent capabilities of a number of RFID technologies that conform to standardized RFID air interface protocols. This should provide enough information to enable the proposed privacy control features to be applied to other RFID technologies including those with proprietary air interface protocols and tag architectures. The risk management features exclude fundamental privacy by design features because these should be the subject of revisions and enhancements to technology standards. The risk management features defined in this Technical Report are considered applicable to current and future implementations of RFID based on existing technology. As such, this Technical Report is considered as input into a standard procedure for undertaking an RFID Privacy Impact Assessment.

2 Terms and definitions

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

2.1
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
identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

2.3
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

2.4
personal data
any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one 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

2.5
PIA process
process based on a privacy and data protection risk management approach focusing mainly on the implementation of the EU RFID Recommendation and consistent with the EU legal framework and best practices

2.6