SLOVENSKI STANDARD
SIST EN 16571:2014

01-december-2014

Informacijska tehnologija - Postopek ocenjevanja vpliva RFID na zasebnost

Information technology - RFID privacy impact assessment process

Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID

Processus d'évaluation de l'impact en termes de respect de la vie privée de l'identification RFID

Ta slovenski standard je istoveten z: **EN 16571:2014**

ICS:

35.020	Informacijska tehnika in tehnologija na splošno	Information technology (IT) in general

SIST EN 16571:2014 **en,fr,de**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 16571

June 2014

ICS 35.240.60

English Version

Information technology - RFID privacy impact assessment process

Technologies de l'information - Processus d'évaluation d'impact sur la vie privée des applications RFID

Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID

This European Standard was approved by CEN on 14 May 2014.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

Contents

Page

Foreword

This document (EN 16571:2014) has been prepared by Technical Committee CEN/TC 225 “AIDC technologies”, the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by December 2014, and conflicting national standards shall be withdrawn at the latest by December 2014.

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 document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

This European Standard is one of a series of related deliverables, which together comprise M/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 16656, *Information technology — Radio frequency identification for item management — RFID Emblem (*ISO/IEC 29160:2012*, modified)*;

— 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 [1)], *Information technology — RFID privacy impact assessment analysis for specific sectors*;

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

— CEN/TR 16684[2)], *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*.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: 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 the United Kingdom.

1) CEN/TR 16673 contains practical examples of PIA systems.

2) CEN/TR 16684 contains practical examples of notification signage systems.

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, and 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 programme identified in the first phase.

This European Standard is one of 11 deliverables for M/436 Phase 2. It builds on the research undertaken in the two related Technical Reports:

— CEN/TR 16673 provides an insight into how RFID privacy issues have been addressed in four sectors: libraries; retail; e-ticketing, toll roads, fee collection, events management; and banking and financial services.

— CEN/TR 16674 considers formal PIAs that are already in place, but not necessarily presented as formal national standards.

The procedures defined in this European Standard are intended to be used by individual RFID operators or entire sectors for conducting a PIA for RFID. As such, it will cite as references other deliverables included in M/436 Phase 2. A sector-based PIA can act as a template to assist in the development of a specific PIA.

1 Scope

This European Standard has been prepared as part of the EU RFID Mandate M/436. It is based on the Privacy and Data Protection Impact Assessment Framework for RFID Applications, which was developed by industry, in collaboration with the civil society, endorsed by Article 29, Data Protection Working Party, and signed by all key stakeholders, including the European Commission, in 2011.

It defines aspects of that framework as normative or informative procedures to enable a common European method for undertaking an RFID PIA.

It provides a standardized set of procedures for developing PIA templates, including tools compatible with the RFID PIA methodology.

In addition, it identifies the conditions that require an existing PIA to be revised, amended, or replaced by a new assessment process.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

3 Terms and definitions

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

3.1
competent authority
organization called for in the RFID Recommendation to receive the PIA 6 weeks before deployment of the RFID application

Note 1 to entry: The Recommendation in Point 5 (d) provides no details of the credentials of the competent authority.

3.2
controlled domain
part of an of an application that is under the direct control of the RFID operator (or data controller), including the data on the tag that is processed by the application and the RFID air interface communications

Note 1 to entry: This has close analogies with data processing under Directive 95/46/EC.

3.3
countermeasure
action, device, procedure, or technique that meets or opposes (i.e. counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause

3.4
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

[SOURCE: Directive 95/46/EC]

3.5
Data Protection Authority
DPA
organization, or organizations, responsible for the administration of Directive 95/46/EC in a Member State

3.6
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

[SOURCE: Directive 95/46/EC]

3.7
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

Note 1 to entry: 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.

3.8
information security
preservation of the confidentiality, integrity and availability of information

[SOURCE: Recommendation C(2009) 3200 final]

3.9
monitoring
activity carried out for the purpose of detecting, observing, copying or recording the location, movement, activities or state of an identified or identifiable person

[SOURCE: RFID Recommendation C(2009) 3200 final, modified — The definition itself has been adapted.]

3.10
personal behaviour information
data that identifies an individual's behaviour or behavioural characteristics

3.11
personal data
information relating to an identified or identifiable natural person ('data subject') inasmuch as 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

[SOURCE: Directive 95/46/EC, modified — The definition has been grammatically changed.]

3.12
personal identifier
data that can be used to directly or indirectly identify an individual to whom such data refers

3.13
personal privacy asset
anything that has value to the person associated with a particular RFID tag

Note 1 to entry: The loss of such an asset therefore requires protection.

3.14
privacy
right of the identified or identifiable person to have his identity and action protected from any unwanted scrutiny and interference

Note 1 to entry: Privacy reinforces the individual's right to decisional autonomy and self-determination which are fundamental rights accorded to individuals within Europe.

[SOURCE: ETSI/TR 187 020 V1.1.1 (2011-05), modified — The definition itself has been adapted.]

3.15
privacy breach
situation where personal data in an RFID application is processed in violation of one or more relevant privacy safeguarding requirements

[SOURCE: ISO/IEC 29100:2011, modified — The definition itself has been adapted.]

3.16
privacy capability statement
declaration by an RFID technology provider of RFID tags or readers of the privacy features inherent in the specified product

Note 1 to entry: Based on CEN/TR 16672, the privacy capability statement identifies in a consistent manner the extent that the features in a product support enhancements to privacy. The privacy capability statement is a more precise input to the PIA process than the generic protocol standard because it is product-specific.

3.17
privacy risk
potential that a given threat will exploit vulnerabilities of personal privacy asset and thereby cause harm to the attacked system or organization

[SOURCE: ETSI/TR 187 020 V1.1.1 (2011-05), modified — The definition itself has been adapted and the defined term was "risk" originally.]

3.18
Registration Authority
RA
organization appointed by CEN to maintain a publicly accessible register of factors associated with a standard

Note 1 to entry: For EN 16571, the RA is responsible for maintaining a register of privacy capability statements.

3.19
residual risk
risk remaining after countermeasures have been implemented to reduce the risk associated with a particular threat

[SOURCE: ETSI/TR 187 020 V1.1.1 (2011-05)]

3.20
RFID
radio frequency identification
use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to read from or write to an RFID tag

[SOURCE: RFID Recommendation C(2009) 3200 final]

3.21
RFID application
application that processes data through the use of tags and readers, and which is supported by a back-end system and a networked communication infrastructure

[SOURCE: Recommendation C(2009) 3200 final]

3.22
RFID application operator
RFID operator
natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an application, including controllers of personal data using an RFID application

[SOURCE: RFID Recommendation C(2009) 3200 final]

3.23
RFID interrogator
RFID reader
interrogator
reader
fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags

Note 1 to entry: The term 'interrogator' is often used in the context of RFID item management standards and the term 'RFID reader' in general applications. The term 'Proximity coupling device' and 'Vicinity coupling device' are used in the context of card applications. They perform the same functions for any given air interface protocol.

3.24
RFID PIA report
detailed internal report of the results of the PIA process

Note 1 to entry: Except for the reference in Recommendation, in Point 5 (d), of making the assessment available to a competent authority, the RFID PIA report is considered a confidential document.

3.25
RFID PIA summary
part of the RFID PIA process that is publicly available in the interests of transparency

3.26
RFID tag
RF tag
tag
transponder
RFID device having the ability to produce a radio signal or a RFID device which re-couples, back-scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer

[SOURCE: RFID Recommendation C(2009) 3200 final]

Note 1 to entry: The most technically accurate term is “transponder”. The most common and preferred term is ‘tag’ or ‘RFID tag’ in the context of RFID item management applications and 'Proximity integrated circuit card' or 'Vicinity integrated circuit card' in the context of card applications.

3.27
RFID threat
physical, hardware, or software mechanism with the potential to adversely impact a personal privacy asset and associated data types or a data subject through unauthorized access, destruction, disclosure, modification of data and / or denial of service

3.28
RFID vulnerability
weakness of an asset or group of assets that can be exploited by one or more threats

[SOURCE: ISO/IEC 27005:2011, modified — The definition itself has been adapted and the defined term was "information security risk" originally.]

3.29
template
input information and data intended to assist in reducing the effort required to complete a PIA, where a number of RFID applications share some common features

Note 1 to entry: The degree of detail of a template is a matter of decision for the originator of such a document. It may vary from a description of the application to a more sophisticated analysis, and can be used as a generic tool to prepare the PIA report, but is never a substitute for a PIA report, which is the responsibility of each RFID operator.

3.30
uncontrolled domain
part of an of an application that the RFID operator (or data controller) cannot control, including the capability of a third party legitimately or illicitly reading data from the RFID tag in any form factor, whether with reading devices conform to the air interface protocol or circumvent it

4 Symbols and abbreviations

For the purposes of this document, the following symbols and abbreviations apply.

— AIDC Automatic Identification and Data Capture
— AFI Application Family Identifier
— CEN European Committee for Standardization (French = Comité Européen de Normalisation)
— DSFID Data Storage Format Identifier
— EN European Standard
— EPC Electronic Product Code
— ETSI European Telecommunications Standards Institute
— GS1 Global Standards One
— HF High Frequency
— IEC International Electrotechnical Commission
— ISO International Organization for Standardization
— NFC Near Field Communication
— PIA Privacy Impact Assessment
— RF Radio Frequency
— RFID Radio Frequency Identification
— SME Small and medium-sized enterprise
— TR Technical Report
— TS Technical Specification
— UHF Ultra High Frequency