

Infotehnoloogia. RFID privaatsuse mõju kaalutlemise protsess

Information technology - RFID privacy impact assessment process

This document is a preview generated by EVS

EESTI STANDARDI EESSÕNA

See Eesti standard EVS-EN 16571:2014 sisaldab Euroopa standardi EN 16571:2014 ingliskeelset teksti.

Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.

Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 25.06.2014.

Standard on kättesaadav Eesti Standardikeskusest.

NATIONAL FOREWORD

This Estonian standard EVS-EN 16571:2014 consists of the English text of the European standard EN 16571:2014.

This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.

Date of Availability of the European standard is 25.06.2014.

The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.240.60

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Aru 10, 10317 Tallinn, Eesti; www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:
Aru 10, 10317 Tallinn, Estonia; www.evs.ee; phone 605 5050; e-mail info@evs.ee

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.....	5
Introduction.....	6
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Symbols and abbreviations	11
5 Structure of this European Standard.....	12
6 Field of reference for this European Standard	12
6.1 'RFID' as defined by the EU RFID Recommendation	12
6.2 'RFID application' as defined by the EU RFID Recommendation	13
6.3 'RFID operator' as defined by the EU RFID Recommendation.....	13
6.4 Relationship between the RFID PIA and data protection and security	14
6.5 Relevant inputs for the PIA process	17
6.5.1 General.....	17
6.5.2 The privacy capability statement	17
6.5.3 The Registration Authority	17
6.5.4 RFID PIA templates.....	17
7 RFID operator's organizational objectives of the RFID PIA	17
7.1 Overview	17
7.2 Meeting and exceeding legal requirements	18
7.3 When to undertake the RFID PIA.....	19
7.3.1 General.....	19
7.3.2 Undertaking a PIA at the design stage before the RFID system becomes operational	19
7.3.3 Undertaking a PIA at a review and update the design-based PIA	19
7.3.4 Undertaking a PIA to contribute to the development of a template	19
7.3.5 Undertaking a PIA with an established template.....	20
7.3.6 Undertaking a PIA at the introduction of a new function within the RFID application.....	20
7.3.7 Undertaking a PIA based on changes in RFID technology	20
7.3.8 Undertaking a PIA when a privacy breach has been reported.....	20
8 Tools to simplify the process	21
8.1 RFID operator responsibility	21
8.2 RFID technology privacy capability tools - overview.....	21
8.3 Registration of RFID privacy capability statements by RFID product manufacturers	21
8.3.1 General.....	21
8.3.2 Obligations of the Registration Authority	21
8.3.3 Appointment.....	22
8.3.4 Resignation	22
8.3.5 Responsibilities of the RFID product manufacturers	22
8.4 RFID technology privacy capability tools - details.....	23
8.4.1 RFID integrated circuit privacy capabilities	23
8.4.2 RFID tag privacy capabilities.....	23
8.4.3 RFID interrogator privacy capabilities.....	23
8.4.4 The default privacy capability statement	23
8.4.5 Using CEN/TR 16672 to construct privacy capabilities for products using proprietary protocols.....	24
8.5 Templates	24
8.5.1 General.....	24

8.5.2	Developing a template	24
8.5.3	Who should prepare the templates?	25
8.5.4	The role of stakeholders in template development	25
9	RFID PIA - a process approach	26
9.1	Introduction	26
9.2	Process Steps	26
9.3	Achieving the correct level of detail	27
9.3.1	General	27
9.3.2	Level 0 – no PIA	27
9.3.3	Level 1 – small scale PIA	27
9.3.4	Level 2 – PIA focussed on the controlled domain of the application	27
9.3.5	Level 3 – Full scale (complete) PIA of the application	28
9.3.6	Reducing the effort for the SME organization	28
9.4	Process methodology	29
10	Preparing the RFID functional statement	30
11	Preparing the description of the RFID applications	31
11.1	Introduction	31
11.2	Multiple applications	31
11.3	RFID application overview	32
11.3.1	General	32
11.3.2	Determine which RFID technology is intended or being used	32
11.3.3	Determine the RFID components used in the application	33
11.3.4	RFID applications on portable devices	34
11.4	Data on the RFID tag	36
11.4.1	General	36
11.4.2	Determine what inherent identifiable features are possessed by the RFID tag	36
11.4.3	Listing the data elements encoded on the RFID tag	37
11.4.4	Determine whether encoded data can be considered identifiable	37
11.4.5	Determine whether personal data is encoded on the tag	38
11.5	Additional data on the application	38
11.6	RFID data processing	38
11.7	Internal transfer of RFID data	39
11.8	External transfer of RFID data	39
11.9	RFID application description sign off	39
12	Risk Assessment	40
12.1	Procedural requirements derived from the RFID Recommendation	40
12.1.1	Common procedure requirements for all RFID operators	40
12.1.2	Requirements for retailers that are RFID operators	41
12.1.3	Procedure requirements for manufacturers of products eventually sold to consumers	42
12.2	Asset identification and valuation	42
12.2.1	General	42
12.2.2	Identification of assets	43
12.2.3	Valuing assets	44
12.3	Threat identification and evaluation	47
12.3.1	General	47
12.3.2	Identification and classification of threats	48
12.3.3	Evaluating threats	49
12.3.4	The process for the SME organization	50
12.4	Identifying vulnerabilities and enumerating the associated risk levels	50
12.4.1	Basic procedure	50
12.4.2	Procedure to account for exposure time	51
12.5	Initial risk level	51
12.6	Countermeasures	53
12.6.1	General	53
12.6.2	Identifying countermeasures	53

12.6.3	Reassessing risk levels	55
12.7	Residual risks.....	55
12.8	RFID PIA endorsement.....	56
13	Worked example of the risk assessment process	56
14	The PIA summary report	56
14.1	PIA report date	56
14.2	RFID application operator	56
14.3	RFID application overview	56
14.4	Data on the RFID tag	56
14.5	RFID Privacy Impact Assessment score	57
14.6	RFID countermeasures	57
15	Revision control.....	57
16	Monitoring and incident response	58
Annex A	(normative) Details of Registration Authority.....	59
Annex B	(informative) RFID manufacturer's product privacy capability statements	60
B.1	RFID integrated circuit (chip) privacy features.....	60
B.2	RFID interrogator privacy features	62
Annex C	(informative) RFID Privacy Impact Assessment flowchart.....	65
Annex D	(informative) Template development	67
Annex E	(informative) Flowchart to determine the RFID PIA level.....	68
Annex F	(informative) RFID functional statement.....	69
Annex G	(normative) RFID application description.....	70
Annex H	(informative) Identification and valuation of personal privacy assets	71
H.1	Individually held personal privacy asset.....	71
H.2	Assets that apply to the organization.....	76
Annex I	(informative) RFID threats	77
I.1	Threats associated with the data encoded on the RFID tag and the RFID tag (or RF card) itself.....	77
I.2	Threats associated with the air interface or the device interface communication	80
I.3	Threats associated with the interrogator (or reader)	85
I.4	Threats associated with the host application.....	85
Annex J	(informative) Countermeasures	88
J.1	List of countermeasures	88
J.2	Threat and countermeasure mappings	90
Annex K	(informative) PIA risk assessment example.....	94
K.1	Introduction	94
K.2	Ranking the assets	94
K.3	Considering threats at the tag layer and air interface layer	95
K.4	Considering threats at the interrogator layer	96
K.5	Considering threats at the device interface layer	97
K.6	Considering threats at the application layer.....	97
K.7	Considering vulnerabilities.....	98
K.8	Risk scores after considering all the threats and vulnerabilities	98
K.9	Applying countermeasures	99
K.10	Overall risk	99
Annex L	(informative) RFID Privacy Impact Assessment summary	101
Bibliography	102

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 16673¹⁾, *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 16684²⁾, *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