SLOVENSKI STANDARD
SIST-TP CEN/TR 16673:2014

01-september-2014

Informacijska tehnologija - Ocenjevanje vpliva RFID na zasebnost za določene sektorje

Information technology - RFID privacy impact assessment analysis for specific sectors

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

Technologie de l'information - Évaluation de l'impact sur la vie privée de la RFID pour des secteurs spécifiques

Ta slovenski standard je istoveten z: **CEN/TR 16673:2014**

ICS:

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

SIST-TP CEN/TR 16673:2014 **en,fr,de**

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 4
Introduction 5
1 Scope 6
2 Terms and definitions 6
3 Symbols and abbreviations 8
4 Brief description of an RFID system 9
4.1 Infrastructure of an RFID system 9
4.2 Components of an RFID system 9
4.2.1 Transponder/Tag 9
4.2.2 RFID reader or writer 10
4.2.3 Backend system 10
4.3 Characteristics of RFID technology compared to other data capture techniques 10
5 Privacy concept in RFID-based applications 11
5.1 Interaction between data protection, data security and privacy 11
5.2 Data protection 12
5.3 Data security 13
5.4 Privacy 13
5.5 General privacy risks 13
5.6 Challenges for a privacy concept in context with RFID 14
5.7 Need for transparency 15
6 Library sector overview 15
6.1 Aspects of the library sector 15
6.2 RFID technology overview 16
6.3 Applications and parties involved 17
6.4 Privacy considerations 18
6.4.1 Privacy of possession 18
6.4.2 Privacy of personal data in the central system 18
6.4.3 The impact of NFC-enabled phones 19
6.5 Prospects for PIA templates 19
7 Retail sector overview 20
7.1 Aspects of the retail sector 20
7.2 RFID Technology Overview 21
7.3 Applications and parties involved 21
7.3.1 General 21
7.3.2 Use of RFID in retail logistics 21
7.3.3 The role of the solution provider 22
7.3.4 Impact of RFID technology for the consumer 22
7.4 Privacy considerations 23
7.5 Technological prospects for privacy enhancements 25
8 Transport sector overview 25
8.1 Aspects of the transport sector 25
8.2 RFID Technology Overview 25
8.3 Applications and parties involved 26
8.3.1 General 26
8.3.2 Types of tickets, features and characteristics 26

8.3.3 Characteristics of automatic fare calculation 27
8.3.4 Sales channels and their impact on the products 27
8.4 Privacy considerations 29
8.5 Other applications not covered in detail 29
8.5.1 General 29
8.5.2 Toll roads and fee collection using RFID 29
8.5.3 Event management using RFID 30

9 Banking and financial services sector overview 30
9.1 Aspects of the finance sector 30
9.2 RFID Technology Overview 31
9.2.1 General 31
9.2.2 Contactless payment cards 32
9.2.3 NFC based payment by mobile phones 32
9.2.4 Micro-tags or stick-on-tags 32
9.3 Applications and parties involved 32
9.4 Privacy considerations 32
9.4.1 General 32
9.4.2 Security of contactless payment cards 33
9.4.3 Organisations 33
9.4.4 Impact of privacy in the banking and finance sector 34
9.4.5 Vulnerabilities 34
9.4.6 Transparency, consumer information, commercial confidentiality and security 35
9.4.7 Implications for the PIA 35

10 Conclusion and recommendations 36
10.1 Diversity of RFID based applications 36
10.2 Benefits of and recommendation for sector or application specific templates 36
10.3 Recommendation for a general approach to PIA 37

Bibliography 38

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

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

2.6
monitoring
any activity carried out for the purpose of detecting, observing, copying or recording the location, movement, activities or state of an individual

2.7
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

2.8
processing of personal data
any operation or set of operations which is performed upon personal data, whether or not by automatic data means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

2.9
data processor
processor
natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

2.10
recipient
natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients

2.11
radio frequency identification
RFID
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 uniquely read the identity of a radio frequency tag or other data stored on it

2.12
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

2.13
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

2.14
RFID reader or writer
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 applications, and the term 'Proximity coupling device' and ' Vicinity coupling device' in the context of card applications. They perform the same functions for any given air interface protocol.

2.15
RFID tag
RF tag
Tag
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

Note 1 to entry: The most accurate term is technically "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.

2.16
third party
any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data

2.17
threat
physical, hardware, or software mechanism with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data and / or denial of service

2.18
vulnerability
weakness of an asset or group of assets that can be exploited by one or more threats

3 Symbols and abbreviations

AFI	Application Family Identifier
CICO	Check-In-Check-Out
CSC	Card Security Code
CVC	Card Verification Code
CVV	Card Verification Value
DPA	Data Protection Authority
EPC	Electronic Product Code
ERP	Enterprise Resource Planning
FMCG	Fast Moving Consumer Goods
EMV	Europay International, MasterCard, Visa
GDPR	General Data Protection Regulation
GS1	Global Standards One
HF	High Frequency (3-30 MHz)
IFMS	Interoperable Fare Management Systems
IOPTA	InterOperable Public Transport Applications for smart cards
ISIL	International Standard Identifier for Libraries and Related Organisations
IT	Information Technology

LF	Low Frequency
LMS	Library Management System
NEC	National Entitlement Card
NFC	Near Field Communication
PCI	Payment Card Industry
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
POS	Point of Sale
RF	Radio Frequency
RFID	Radio Frequency Identification
UHF	Ultra High Frequency (300 MHz – 3 GHz)
UII	Unique Item Identifier

4 Brief description of an RFID system

4.1 Infrastructure of an RFID system

RFID technology allows for the contactless transmission of data via electromagnetic fields and/or radio waves. An RFID infrastructure contains at least one RFID tag, an RFID reader or writer) and an IT backend system. In order to enable the exchange of data between the transponder and the reader, communication standards define the necessary features for the air interfaces, which have to be supported by both, transponder and reader.

4.2 Components of an RFID system

4.2.1 Transponder/Tag

The transponder or tag has a tiny computer chip which contains radio processing, data storage and data processing capabilities. This chip is attached to an antenna to create a tag. This is incorporated into a particular form factor, e. g. integrated into a self-adhesive label or into a contactless card. The information that can be stored on the tag depends on the memory and influences the speed of the data capture process. The tag generally contains a code, which points to information stored in a data base.

Depending on the application, the choice between different characteristics of tags can be made:

— Energy supply: The energy supply is not directly correlated to the communication modes. Passive tags reflect, backscatter or use the load modulation of an incoming wave from the reader in order to communicate. Active tags have their own transmitter on board to send information or answer to a reader's commands. With today's technology, the link budget requires the use of a battery for the active tags whereas for passive tags, the incoming wave can be used to supply the tag's chip with energy. Nevertheless, even for passive tags, batteries can be used to supply the tag's chip or peripherals like sensors. In that case, we speak of Battery Assisted Passive tags which communicate with the readers through backscattering or load modulation of an incident wave but use the battery to supply energy to the chip and/or embedded sensors.

— The form factor of a tag depends on the purpose of its use and the environment it is used in. Tags can be attached to or integrated into a product, and therefore appear in multiple variations. Examples of tags include, but are not limited to: hard-tags, woven- in tags, glass capsule tags, foil tags, smart labels, personal identification cards (e. g. access cards or library cards), transport cards, contactless payment cards.

— The frequency at which a tag operates is defined by its antenna and the chip design. The choice for Low Frequency (LF), High Frequency (HF) or Ultra High Frequency (UHF) depends on the application and the environment the tags are used in.

— The reading distance depends e.g. on the frequency used, the energy consumption and the environmental circumstances in which the tag is used. Thus, the read range varies from few centimetres up to several meters. The purpose of the use of an RFID application determines the read range to choose (e. g. large distance reading for inventory, short distance reading for contactless cards).

— The chip memory varies from a few bits to several hundred Kbytes, Furthermore, the distinction can be made between read only tags (information on tag stored by tag producer), write-once-read-multiple, write-and-read-multiple (reusable) tags. Contactless cards and active tags might be equipped with a microprocessor that supports the management of data files in a flexible way.

4.2.2 RFID reader or writer

Depending on the application, an RFID reader or writer activates, reads or writes information from or on a tag. It sends or receives the information to or from the tag via its antenna and processes the data on to a backend system. The reader can add information such as time of reading or its own ID to the data read from the tag and transfers it to the software in the backend system. Readers can capture data from several tags in very short time (bulk reading) when these get into its operation field.

The purpose of use of the RFID application defines the type of readers that might be used:

— Mobile readers such as handhelds (e. g. used for inventory in shops, warehouses, hospitals)

— Semi-mobile readers such as on forklifts (e. g. used in large warehouse management systems)

— Fixed readers such as gates or tunnel readers (e. g. used in goods entry or exit area of a warehouse, transit points within a warehouse, access points in public transport systems, access to buildings)

For certain applications additional security features are part of the reader. Secure readers are used e. g. for contactless payment cards or NFC applications. They are equipped with a protected key and data storage and security functions in order to support secure communication with contactless smartcards, the back office system and the key management system.

4.2.3 Backend system

The information captured from an RFID tag is transferred to and stored in the backend system. It is in the backend system where the linking of the identification number from the tag and the corresponding information is done. The information can only be processed where access is provided for the user of the system, ideally in combination with automated systems of authorisation and authentication.

Additionally, the backend system can also provide functions for card- or key management systems as an additional or required security feature of the specific application. This could be relevant in applications using contactless cards, e. g. payment cards or multi-application cards for public institutions or transport systems.

4.3 Characteristics of RFID technology compared to other data capture techniques

Where other data capture technology requires optical (1- or 2-dimensional barcodes) or physical contact (magnetic stripe) between data carrier and reader, RFID-based applications do not need this. Additionally, the possibility of reading several data carriers sequentially in a very short time with the long distance read range of one reader accelerates data capture processes considerably.

While adding or changing information on optical or physical contact data carriers would require the reproduction of the carrier, tags provide for the possibility of changing or adding information on the same data carrier. In return, this requires managing access authorisations as content on the data carrier should only be