SLOVENSKI STANDARD
SIST-TP CEN/TR 16672:2014

01-september-2014

Informacijska tehnologija - Zmogljivost zaščite osebnih podatkov pri današnjih tehnologijah RFID

Information technology - Privacy capability features of current RFID technologies

Informationstechnik - Leistungsmerkmale für den Schutz der Privatsphäre in gegenwärtigen RFID-Technologien

Technologie de l'information - Fonctions de protection des données personnelles des technologies RFID actuelles

Ta slovenski standard je istoveten z: **CEN/TR 16672:2014**

ICS:

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

SIST-TP CEN/TR 16672:2014 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16672

June 2014

ICS 35.240.60

English Version

Information technology - Privacy capability features of current RFID technologies

Technologies de l'information - Fonctions de protection de la vie privée dans les technologies RFID actuelles

Informationstechnik - Leistungsmerkmale für den Schutz der Privatsphäre in gegenwärtigen RFID-Technologien

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 16672:2014 E

Contents

Page

Foreword

This document (CEN/TR 16672:2014) 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 16673, *Information technology — RFID privacy impact assessment analysis for specific sectors*

— 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 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 standardisation work programme identified in the first phase.

This Technical Report provides privacy and security characteristics that apply to the relevant standards. Furthermore it provides an overview of these standards and their respective support of the described features.

1 Scope

The scope of the Technical Report is to identify technical characteristics of particular RFID air interface protocols that need to be taken into consideration by operators of RFID systems in undertaking their privacy impact assessment. It also provides information for those operators who provide RFID-tagged items that are likely to be read by customers or other organizations.

This Technical Report provides detailed privacy and security characteristics that apply to products that are compliant with specific air interface protocols, and also to variant models that comply with such standards.

The Technical Report also identifies proprietary privacy and security features which have been added to tags, which are problematic of being implemented in open systems which depend on interoperability between different devices. Such proprietary solutions, whilst being technically sound, in fact impede interoperability. The gap analysis thus identified can be used to encourage greater standardization.

2 Terms and definitions

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

2.1
authentication
process of determining whether an entity or data is/are who or what, respectively, it claims to be.

Note 1 to entry: The types of entity authentication referred-to in this document are Tag authentication, Interrogator authentication, and Tag-Interrogator mutual authentication

2.2
key
value used to influence the output of a cryptographic algorithm or cipher

2.3
KeyID
numerical designator for a secret key

2.4
password
secret value sent by an Interrogator to a Tag to enable restricted Tag operations

2.5
permalock
lock status that is unchangeable

EXAMPLE The memory location is permanently locked or permanently unlocked.

2.6
tag authentication
means for an Interrogator to determine, via cryptographic means, that a tag's identity is as claimed

2.7
TID
tag ID
unique tag identifier

3 Symbols and abbreviations

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

UII Unique Item Identifier

4 Access protection features

4.1 General

This clause identifies several features used to protect access as part of the communication protocol between the interrogator and the tag.

4.2 contains an overview of possible access protection features.

4.3 describes how the protection features can be applied.

4.2 Overview of access protection features

4.2.1 General

This subclause contains a general overview of possible features to protect the access to "resources" on a tag, like access to data in memory, secret keys, flags, configuration settings etc.

The list is presented in an order-ranking of approximate increasing protection level.

NOTE The ranking is approximate, because not all features are available in some RFID technologies, and there are associated features that influence the degree of protection, such as read distance and timeouts.

4.2.2 No protection

The lowest protection level is no protection. If there is no protection, all resources on the tags are freely accessible and can be read and alerted by any interrogator that has access to the tag. This does depend on the interrogator and the tag supporting the same air interface protocol.

4.2.3 Password protection

4.2.3.1 General

Access to the resources on the tag can be protected with an access password. In this document the password protection should only be considered as it is protecting the consumer's privacy. To use this feature a copy of the password needs to be stored in the memory of the tag. When an interrogator requests access to a resource, it first has to provide the password. The tag will compare the password that is provided by the interrogator with the copy of the password that is stored in memory. If both copies match the interrogator is "authenticated" and the tag will provide the interrogator with access to the requested resource. The tag could also store the "authenticated" status in a flag.

A general weakness of the password feature is that for it to be functional, few stakeholders need to be aware of its value. As such, passwords have limited contribution in open systems where the organization responsible for encoding the tag (for example a product manufacturer) has limited knowledge of the specific organization that will read a particular tag (e.g. which retail store).

A technical weakness of the password feature is that the password needs to be transmitted over the air. Therefore it can easily be intercepted by an intruder, who can then use the password later to also get access

to the same resource. An increased level of protection can be provided if the password is transmitted in segments, thus requiring more than one interception to capture the entire password.

A practical limitation of password protection is the possibility to find the password with a "brute force" attack; the interrogator can simply try to find the password starting with binary "0" and then increase the password by "1" after the tag rejects the request, until it has found the right password.

The protection level of the password feature is a function of its length given that all the communication is at the binary level. A brute force attack on an 8-bit password can be achieved in 255 attempts, while a 32-bit password requires 4.3 billion attempts, or over 2 billion attempts on average. While modern computers can process tens of thousands of passwords a second, a brute force attack on an RFID tag requires a new command to be generated each time and is therefore limited by the air interface speed. Also, unlike cracking a password to access a computer system, a password found in one RFID tag might have limited value.

Practically this means that the password features has the best value if it needs to be used only once.

4.2.3.2 Password protection with security timeout

The protection level of the password feature can be improved by implementing a security timeout. The tag can introduce a time delay before it replies to the interrogator. A long delay will result in a brute force attack taking a long time.

There are various possibilities, like a configurable delay or a delay that increases with the number of failed requests.

4.2.3.3 Password protection with cover coding

Cover coding can be used to improve the protection against incepting the password over the air. It obscures information that it is transmitting to a tag. To cover-code a password, an interrogator first requests a random number from the tag. The interrogator then performs a bit-wise XOR of the password with this random number, and transmits the cover-coded string to the tag. The tag uncovers the password by performing a bit-wise XOR of the received cover-coded string with the original random number and then compares the values of both copies. XOR based cover coding can be implemented in a state machine, and therefore in a passive tag.

4.2.4 Cryptographic protection

4.2.4.1 General

Cryptographic protection can be used if the tag is equipped with a processor to perform a cryptographic calculation and has memory to store a secret key. Before requesting access to a resource, an interrogator first needs to request a random number from the tag. The interrogator needs to encrypt the random number with the secret key and return the encrypted secret key to the tag. The tag will use the on-board cryptographic processor to decrypt the received data with the secret key that is stored in its memory and compare the result with the random number that it has initially generated. If the numbers match the interrogator is "authenticated" and the tag will provide the interrogator with access to the resource. The tag could also store the "authenticated" status in a flag.

An inverse process is that the interrogator sends a random challenge, the tag encrypts it and sends back the encrypted data to the interrogator. In this case the interrogator decrypts it and can check the originality of the tag.

A tag could have several secret keys stored on the tag. In that case an interrogator needs to indicate which key needs to be used for authentication and after a successful authentication the tag could store the number that has been used.

There are several forms of cryptography. The chief ones are Symmetric-key and Public-key.

4.2.4.2 Symmetric-key cryptography

In Symmetric-key cryptography the interrogator and the tag share the same secret key to encrypt and decrypt the data.

The main disadvantage of Symmetric-key cryptography is that the secret keys need to be stored in a secret manner in the infrastructure.

Symmetric key cryptography is also referred to as shared-key, single-key, secret-key, and private-key or one-key cryptography.

4.2.4.3 Public-key cryptography

Public-key cryptography uses two keys: a public key and a private key. The public and the private key are different, but mathematically linked. One key encrypts the random number and the other decrypts the cypher text. Neither key can perform both functions. For authentication of the:

— Tag, the public key is made publicly available and is used by the interrogator to decrypt messages. The private key is stored in the tag and kept secret;

— Interrogator, the interrogator holds a private key and sends the encrypted message to the tag, which will decrypt it with the public key to authenticate the interrogator.

For further encryption of the communication it is common to derive the session key from the exchanged random numbers and use that session key to encrypt/decrypt the message received from / sent to the interrogator.

Public-key cryptography is also referred to as Asymmetric cryptography.

4.3 Application of access protection features

The right to get access to a resource can be obtained by exchanging a shared-secret, usually a password or a secret key. After a successful exchange of the shared secret, the interrogator will gain the "authenticated" status and be granted access to the requested resource. The "authenticated" status could also be stored in a flag (for later use in the same session), as long as the tag remains in the field of the interrogator.

A tag might have the capability to support several secret keys, for example if there are separately accessible areas of memory using appropriately set commands for reading and writing to the tag. In these more sophisticated tags different access protection features might be applied by the design of the tag and an RFID operator's option to invoke the feature. The access protection features can also differ.

EXAMPLE An RFID tag has the following features:

— an area of memory used to identify a product, although password protected this has not been set to enable the code to be read by any interrogator

— an area of memory that control the destination of the item in a supply chain, where read access is permitted, but write access is protected

— an area of memory containing data used by field service engineers where read access is protected, and write access only permitted by a service engineer in the factory when the item has to be returned

In the case where a tag has stored several secret keys on the tag, access to a particular resource could also be linked to a specific key. In that case an interrogator needs to indicate which key needs to be used for authentication and after a successful authentication the tag needs to store the number that has been used.