SLOVENSKI STANDARD
SIST-TP CEN/TR 16669:2014

01-september-2014

Informacijska tehnologija - Vmesnik za izvajanje ISO/IEC 18000-3

Information technology - Device interface to support ISO/IEC 18000-3

Informationstechnik - Geräteschnittstelle zur Unterstützung von ISO/IEC 18000-3 Mode 1 and Mode 3 tags

Technologie de l'information - Interface de prise en charge d'ISO/IEC 18000-3 Mode 1 pour les appareils

Ta slovenski standard je istoveten z: **CEN/TR 16669:2014**

ICS:

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

SIST-TP CEN/TR 16669:2014 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16669

June 2014

ICS 35.240.60

English Version

Information technology - Device interface to support ISO/IEC 18000-3

Technologies de l'information - Interface de prise en charge d'ISO/CEI 18000-3 pour les appareils

Informationstechnik - Geräteschnittstelle zur Unterstützung von ISO/IEC 18000-3 Mode 3 tags

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 16669:2014 E

Contents

Page

Foreword

This document (CEN/TR 16669:2014) 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 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*

— 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 is related to the development of a Technical Specification to define the device interface to support ISO/IEC 18000-3 Mode 3 tags.

The proposed Technical Specification on a device interface was intended to support two high frequency air interface protocols; ISO/IEC 18000-3 mode 1 that has been established and used for 15 years and ISO/IEC 18000-3 mode 3 that is just emerging. The assumption was that ISO/IEC 18000-3 mode 3 would offer greater security and that the protection of the privacy would be better served by it. The proposed device interface is intended as a serious attempt to bring greater control to this highly used air interface protocol. In addition, by developing a device interface that supports both air interface protocols, there is the potential to assist in the migration from the older, and (suggested) less secure, technology to a newer and (assumed) more robust technology. Robustness, in this case, is not only of benefit to the operator of the system but also to end users who come into daily contact with the technologies.

In the exploration phase to start with the preparations for the Technical Specification the project team encountered a challenge to translate the specifics of the required device interface features into practical specifications. First it was not clear why ISO/IEC 18000-3 mode 3 would offer greater security to protect the privacy of the consumers. Second it was not obvious to which "application" the reader should connect and how the proposed device interface would contribute to improving the privacy protection of the consumer. Therefore the project team decided to consult the industry to get their feedback on the proposed standard for a device interface.

The device interface is aimed at supporting ISO/IEC 18000-3 technology. The Library industry is by far the largest market for the ISO/IEC 18000-3 tags. Therefore this Technical Report will focus on the value that the proposed device could offer to improve the protection of the privacy of the consumer of the European Library Industry.

This Technical Report describes the project team's approach to resolve the challenges. Clause 6 described the evaluation of the privacy protection level of 18000-3 Mode 3. Clause 7 describes the feedback of the industry on the need for the device interface. Clause 8 describes the feedback of the industry on features of the device interface as listed in the scope. Clause 9 points to some potential threats caused by some of the memory content in library RFID tags. Annex A contains the list of industry representatives who have contributed to the creation of this report. Clause 5 draws the conclusions.

1 Scope

The scope of this Technical Report is to assess the need to develop a Technical Specification to define an interface that provides RFID system control components with low-level access to RFID interrogators for the purpose of optimising RFID data access and control operations.

2 Normative references

Not applicable.

3 Terms and definitions

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

3.1
air interface
complete communication link between an Interrogator and a Tag including the physical layer, collision-arbitration algorithm, command and response structure, and data-coding methodology

3.2
contactless
pertaining to the achievement of signal exchange with and supplying power to the card without the use of galvanic elements (i.e., the absence of an ohmic path from the external interfacing equipment to the integrated circuit(s) contained within the card)

3.3
interrogator (also known as reader)
a transmitter/receiver that reads the contents of RFID tags in the vicinity

3.4
RFID tag
an electronic identification device that is made up of a chip and antenna

4 Symbols and Abbreviations

AFI	Application family identifier
CRC-5	5 bit Cyclic redundancy check
CRC-16	16 bit Cyclic redundancy check (calculated on power-up)
CRC-16c	16 bit Cyclic redundancy check (calculated in transmission)
CW	Continuous Wave
ERC	European Radiocommunications Committee
ETSI	European Telecommunications Specifications Institute
HF	High frequency
LMS	Library Management System
PC	Protocol Control
RF	Radio frequency
SRD	Short Range Devices

TID	Tag-identification or tag identifier, depending on context
UHF	Ultra High Frequency
UID	Unique device IDentifier
UII	Unique Item Identifier
XPC	Extended Protocol Control
XTID	Extended TID indicator (see version 1.3 and above of the EPCglobal™ Tag Data Standards)

5 Executive Summary

The three "assumed" security features of ISO/IEC 18000-3 mode 3 do not provide any improvement for the protection of the consumer's privacy.

The differences between ISO/IEC 18000-3 Mode 1 and Mode 3 are on the physical layer and on the memory addressing. Mode 3 in comparison to Mode 1 does not provide any additional feature that could be used to improve consumer privacy.

The device interface will not help to improve the privacy protection of the European citizen.

The feedback from the representatives of the European Library Industry in Clause 7 makes clear that the industry sees neither an advantage nor a need for the proposed standard for it will not improve the privacy protection of the citizen in any way.

Besides the fact that the proposed standard will not help to improve the privacy protection of the citizen, the cost of developing and implementing such interface in the existing infrastructure of the RFID Application Software or Library Management Systems would be prohibitive.

Therefore CEN/TC 225 Project Team E recommends dropping the development of the proposed device interface standard.

6 Evaluation privacy protection level of ISO/IEC 18000-3 Mode 3

6.1 General

The description of Deliverable Task E.4 states:

There is one event that might completely change the situation: the introduction of ISO/IEC 18000-3 Mode 3 air interface protocol and tags. This technology is still in its infancy, but has been developed as the high frequency 'equivalent' of the ISO/IEC 18000-6 Type C technology. It offers higher performance, greater security, and the attributes of medium range reading that has proved acceptable for many applications. As examples ISO/IEC 18000-3 Mode 3 offers three features not supported by the established high frequency RFID tags:

1) the technology does not depend on a persistent tag id for air interface communications;

2) it supports standardized access passwords;

3) it supports a kill function.

This is remarkable, because key difference of ISO/IEC 18000-3 Mode 3 versus ISO/IEC 18000-3 Mode 1 is the speed of reading so that more items could be scanned per second. Mode 3 does not offer any more features that can be used to protect the privacy of the consumer. This clause describes the evaluation if the assumed security features.

6.2 Technology does not depend on a persistent tag id for air interface communications

ISO/IEC 18000-3 Mode 1 and ISO/IEC 18000-3 Mode 3 have a different way of collision resolution, but in both case the end result is a constant reply that always returns the same number for the tag. Mode 1 tags always return the UID, Mode 3 tags always return the UII. Figure 1 illustrates the interaction between an interrogator and a tag for mode 3 tags.

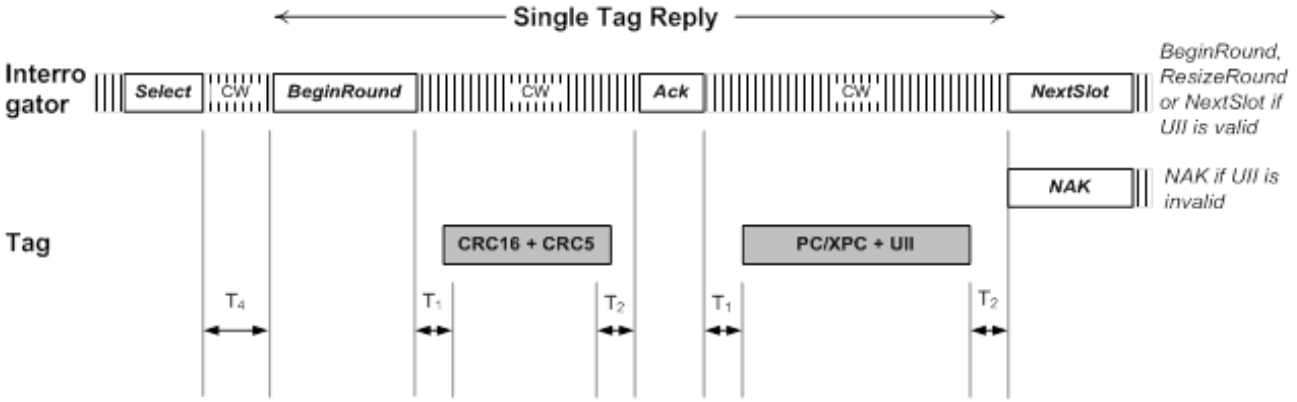

Figure 1 — Interaction between interrogator and tag

While the UII could be empty for the purpose of the anti-collision the TID memory is defined to contain unique information, where read access cannot be prevented.

6.3 Support of standardized access passwords

6.3.1 ISO/IEC 18000-3 Mode 3 tags

ISO/IEC 18000-3 Mode 3 tags do support passwords, but they have no relevance for the protection of the consumer's privacy. The memory of a Mode 3 tag is logically separated into four distinct banks, as shown in Figure 2.

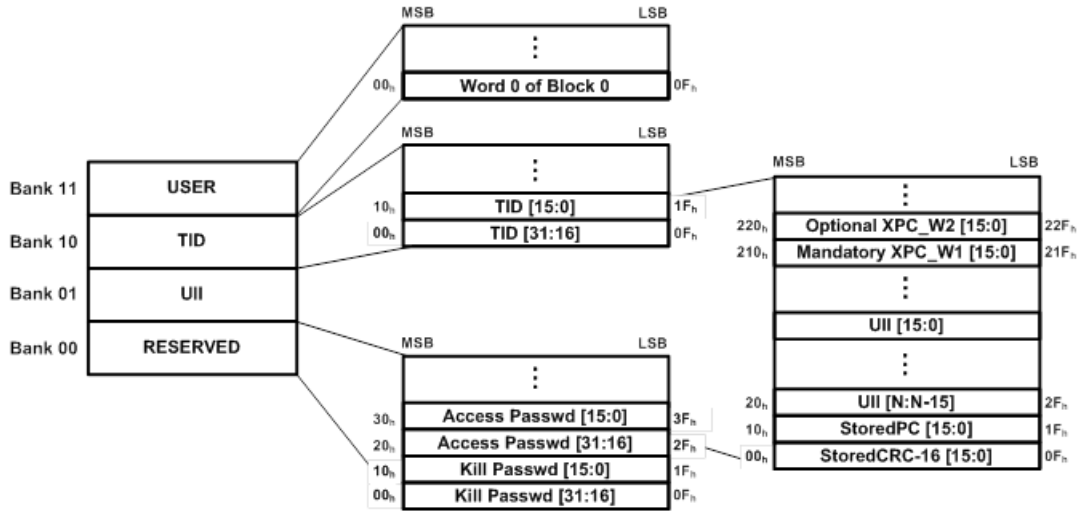

Figure 2 — Memory map of ISO/IEC 18000-3 mode 3 tags

The memory banks are:

— Reserved memory contains the kill and and/or access passwords.

— UII memory contains the UII that identifies the object to which the tag is or shall be attached.

— TID memory contains the TID that identifies the tag.

— USER memory is optional and might contain user data.

6.3.2 Kill password

The Kill password is a 32-bit value that an Interrogator may use to kill a tag and render it nonresponsive thereafter. See also 6.4.

6.3.3 Access password

The Access password is a 32-bit value that an Interrogator needs to submit before the tag will transition to the secured state. In the secured state the interrogator can change the Access password and the write lock bits.

The Access password does not prevent the Interrogator from reading the UII, TID or User Memory. In other words, the Access password cannot be used for read-protection.

6.4 Support of the Kill function.

ISO/IEC 18000-3 Mode 3 supports a Kill function to render a tag nonresponsive after the execution of the Kill command. This feature is implemented to protect the privacy of the consumer when he or she purchases a product that has an RFID tag attached to it. The tag can be killed before the consumers leave the store, which practically eliminates any privacy risk.

For applications where a tag cannot be killed because it needs to be re-used, for example an RFID tag in a library book, the Kill feature does not offer any improvement to protect the consumer's privacy.

6.5 Conclusion

From a privacy protection perspective the differences in air interfaces communications offer no difference in privacy protection of an ISO/IEC 18000-3 Mode 1 versus an ISO/IEC 18000-3 Mode 3 tag.

The passwords on the ISO/IEC 18000-3 Mode 3 tags can only be used to protect the Reserved Memory and the lock functions of the tag. They do not offer any feature to improve the protection of the privacy.

For the library industry the Kill feature does not offer any improvement to protect the consumer's privacy.

Compared to ISO/IEC 18000-3 Mode 1 tags the three additional security features of ISO/IEC 18000-3 Mode 3 do not provide any improvement for the protection of the consumer's privacy.

As a conclusion the statement in the description of the deliverable that "the introduction of ISO/IEC 18000-3 Mode 3 air interface protocol and tags might completely change the situation" does not apply and is not useful for the improvement of the protection of the consumers' privacy.

7 Industry feedback on the need for the device interface

7.1 General

The description of Deliverable Task E.4 states: