PD CEN/TR 16669:2014

BSI Standards Publication

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

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 16669:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/34, Automatic identification and data capture techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 83894 1
ICS 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 June 2014.

Amendments/corrigenda issued since publication

Date	Text affected

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.

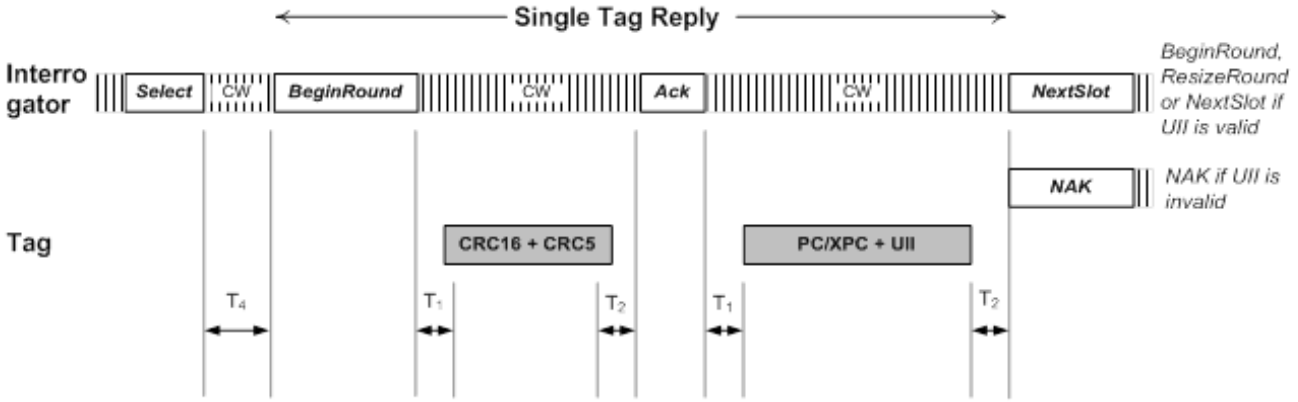

Figure 1 — Interaction between interrogator and tag

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.

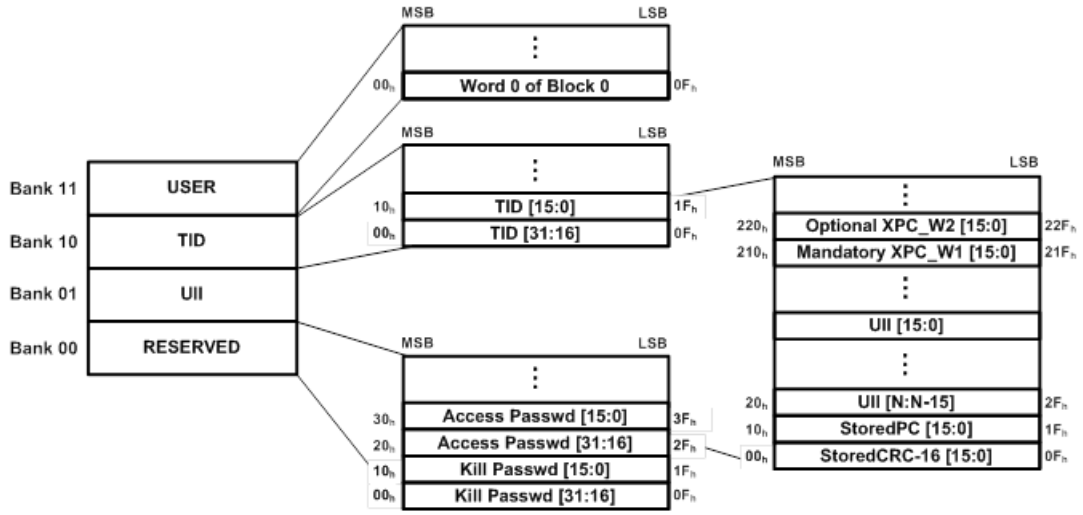

Figure 2 — Memory map of ISO/IEC 18000-3 mode 3 tags

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:

"Developing a device interface specification that encompasses the new (ISO/IEC 15693-mode3) and the older legacy technology (ISO/IEC 15693-mode1) will provide an option for migration from the legacy technology and interoperability between the two technologies."

In the exploration phase to prepare for the Technical Specification the project team encountered a challenge to translate the specifics of the required device interface features into practical specifications. 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. This clause reports the feedback from the European Library Industry on the value of the proposed device interface to improve the privacy protection of the European consumer.

7.2 General description of system architecture for Library Management Systems

This subclause provides a brief description of the LMSs that are used in the European Library Industry. Figure 3 illustrates typical system architecture of an LMS, and its connections with the RFID System Integrators Application Software (eg Self Service, Security, Automation, Inventory and Staff Services).

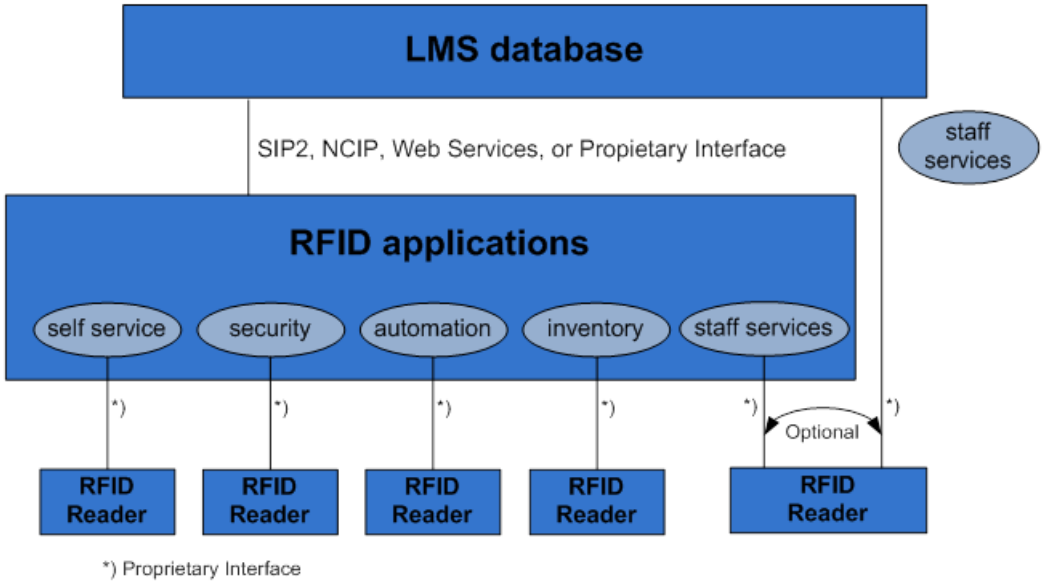

Figure 3 — System architecture of a Library Management System

Heart of the LMS is the library database and the application software that controls it. The database contains all the data that is necessary to run the LMS, including all data related to the books. The RFID tag in the book only contains a unique "book identifier" number that is used as "record locater" for the information about the book that is stored in the database.

As indicated in Figure 3 the LMS is connected with several "sub-systems" of the RFID System Integrators Application Software that provide some dedicated functionality for the libraries, like sub-systems for self-checkout, book returns, sorters etc. When comparing different LMSs and RFID Application Software, first thing that is noticed is that all are different and are build with custom architectures and proprietary interfaces. None of the LMSs or RFID Application Software have the same architecture. Only one interface, between the self-service unit and the LMS database, has a degree of standardization with either a SIP2, NCIP or a Web Services interface, but even then many have proprietary additions/features; however this has nothing to do with RFID or the privacy of the consumer, as this interface relates to any self service equipment irrespective of ID/security technology (barcode, RF, and EM are used, as well as RFID).. The sub-systems with self-service

software and RFID-reader are offered as one package delivered by one supplier, so no advantage is gained with a standard interface.

The interfaces of the RFID readers are all proprietary and customised for its various purposes. In general these interfaces support different tag protocols and use the same user commands for common tag operations like read, write and lock. So the reader protocol is identical for tags that are compliant with ISO/IEC 18000-3 Mode 1 and ISO/IEC 18000-3 Mode 3. That makes it very easy to integrate the protocol in all kinds of readers; from simple short-range (proximity, few cm) reader modules up to highly sophisticated long-range (up to 100 cm) readers. Although most reader manufacturers offer similar functionality on the reader interface, their implementation is always proprietary.

In the library industry the RFID readers have turned into a commodity, where price is the most differentiating factor. Most RFID reader manufacturers produce "general purpose" readers and customise them for specific functionality at the request of an RFID system integrator or an LMS.

With regards to the protection of the privacy of the consumer it is important to point out that RFID technology has already been in use for the libraries for many years and has already delivered effective economic & social benefits for the library markets. Safeguards have been put in place to protect access to the LMS database effectively. RFID readers have no access to the LMS! There is also no link from the "book identifier" that is stored on the RFID tag to any privacy related data. The "book identifier" is just a number that acts as a pointer to a record in the LMS database. It can only be connected to personal data through access to the LMS and its database. In summary, the Library Industry has managed to effectively protect the privacy of the European consumer.

7.3 Feedback on various quotes to justify the development of a device interface

7.3.1 General

This subclause lists the feedback from the European Library Industry on the various quotes in the "call for experts" to justify the development of the device interface.

7.3.2 Need for a device interface standard

Quote: "Although the air interface has been standardized, there is no standardization of the device interface to the application. Instead there is a multiplicity of proprietary device interfaces."

The industry confirms that there are several different device interfaces on the market and that most of them are proprietary to the various reader vendors. The brief summary of the LMS architecture in 7.2 already shows that all interfaces of the RFID readers are proprietary. It is interesting that the requirements have not considered the impact of the changes on the LMS side. Besides the effort to develop such device interface standard, the introduction of it will cause tremendous development and implementation costs for both the manufacturers of the RFID readers and the system integrators of the LMSs.

In addition, the introduction of such interface will also lead to the need for compliancy tests, causing an even greater increase of the total cost of the introduction.

7.3.3 Migration from old to new technology

Quote: "There is the potential to assist in the migration from the older, and less secure, technology to a newer and more robust technology."

Quote: "Developing a device interface specification that encompasses the new and the older legacy technology will provide an option for migration from the legacy technology and interoperability between the two technologies."

Besides the fact that the "new technology" will not contribute to the improvement of the privacy protection (as described in Clause 6), the costs of the introduction of a new interface (as indicated in 7.3.2) will be prohibitive and therefore the device interface will have no potential to introduce new technology.

NOTE The industry confirms that the availability of such interface would we very helpful if the system design could start from scratch. However, the infrastructure that has been built up over many years has become gigantic and it is far from reality to expect that the industry will change to a standardized interface. Especially not when there are no advantages.

7.3.4 Inertia associated with any attempt to standardize the device interface

Quote: "The inertia associated with any attempt to standardize the device interface of the established technology cannot be ignored."

The inertia can easily be explained because the industry has no need for such standard. As far as the industry is concerned the lack of such standard will not have any negative implications.

Quote: "Barriers such as the inertia to change and the cost of conversion can also be greatly reduced."

7.3.2 already explains that the costs of the introduction of a new RFID reader interface would be tremendous and prohibitive.

The industry does not believe that the European library industry will develop faster in any direction when such interface would be available.

7.3.5 Additional security features built into the device interface.

Quote: "Additionally security features could be built into the device interface."

The interface of the RFID reader itself has very little impact of the potential to improve the privacy protection of the consumer that uses an RFID tag, for example in a library book. Besides that, most (if not all) of the used proprietary interface have implemented safeguards to protect the communication over the interface. Adding security features should be seen as part of the ordinary product development process and do not require the development of a standardized device interface.

7.3.6 Delaying for two years will result in a lost opportunity?

Quote: "Delaying for two years will result in a lost opportunity. Addressing this soon could result in open source solutions."

Besides the fact that the "new technology" does not offer anything new (in terms of privacy protection), the comments in the subclauses above make clear that there is also no opportunity.

7.3.7 Leaving operators to choose between the technologies

Quote: "Simply leaving operators to choose between the technologies for an entire implementation will result not only in a lag of the take up of the new air interface, but even result in new implementations being based on the older technology."

When an operator has to make a decision for a particular technology there are many aspects that will consider, like availability, costs and possibilities for a second-source. It is unlikely that the existence of a device interface standard for a RFID reader will have a large impact on that decision.

7.3.8 Standardized device interface to be incorporated into the PIA?

Quote: "The existence of a standardized device interface (through this deliverable) could also be incorporated into the PIA as a best practice solution."

It is not clear how a standard could be incorporated in a PIA. As the name suggest, the document should assess the privacy impact of an RFID application. Its purpose is to prove that the privacy and the personal data of the consumer are well protected in the RFID application that has been assessed.

The industry has great concerns if such standard would become a legal requirement in for example a PIA framework, since it will raise the need for compliancy testing and therefore increase the cost of the RFID readers.

7.3.9 Conclusion

Quote: "Providing a standard device interface solution that enables operators to interoperate with ISO/IEC 18000-3 Mode 1 tags should accelerate the take-up of a technology that provides greater privacy and security."

It is clear that a device standard for an RFID reader will not improve the protection of the privacy of the European citizen in any way. Besides that the industry and operators see no need for the proposed standard.

Quote: "Deliverable E.4 offers the prospect of a more rapid transformation to a more secure RFID technology at minimum cost to existing operators."

Besides the fact that the industry sees no need for such interface, the cost of developing and implementing such interface in the existing infrastructure of the Library Management Systems would be prohibitive.

8 Industry feedback on features of the device interface as listed in the scope

8.1 General

This clause reports the feedback from the European Library Industry on the requirements for the new device interface standard as they are listed in the "call-for experts".

8.2 Features of the device interface as listed in the scope

The scope requests 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.

As the new interface needs to replace the old functionality and, at the same time, introduce new functionality, in fact the interface would have to cover all architectures, including TCP/IP. The industry does not believe that this would be practical - maybe not even possible.

Reader vendors consider a device interface with the proposed features very complex. The proposed handling of data structures increases complexity even more. Such interface would need a PC based TCP/IP architecture and cannot be used on most of the architectures that are being used today. The vendors do not believe that such kind of high level software interfaces will help to get a more rapid transformation to more security, because it is high level and it needs a kind of PC architecture.

Given the complexity of the existing architectures, the development of such a standard will either be so high level as to not be effective or so complex that the implementation & redevelopment of these interfaces will have a significant impact on adoption (cost) and be a substantial blocker to the economic benefits.

NOTE It is interesting that the requirements have not considered the extra layer of complexities the device interface will have on all applications on the LMS side of the interface.

8.3 GS1/EPCglobal LLRP and ISO/IEC 24791

The functionality of the requirements for the new device interface standard as they are listed in the "call-for experts" are similar to the features of two existing reader interfaces; GS1 EPCglobal LLRP (Low Level Reader Protocol) and ISO/IEC 24791.

Both interfaces have been developed for readers using the UHF EPC Gen2 (or ISO/IEC 18000-63) air interface in Retail Management Systems. They are not being used in the European Library Industry.

GS1 EPCglobal LLRP is part of the EPCglobal "house" of standards. Figure 4 illustrates the EPCglobal standards overview.

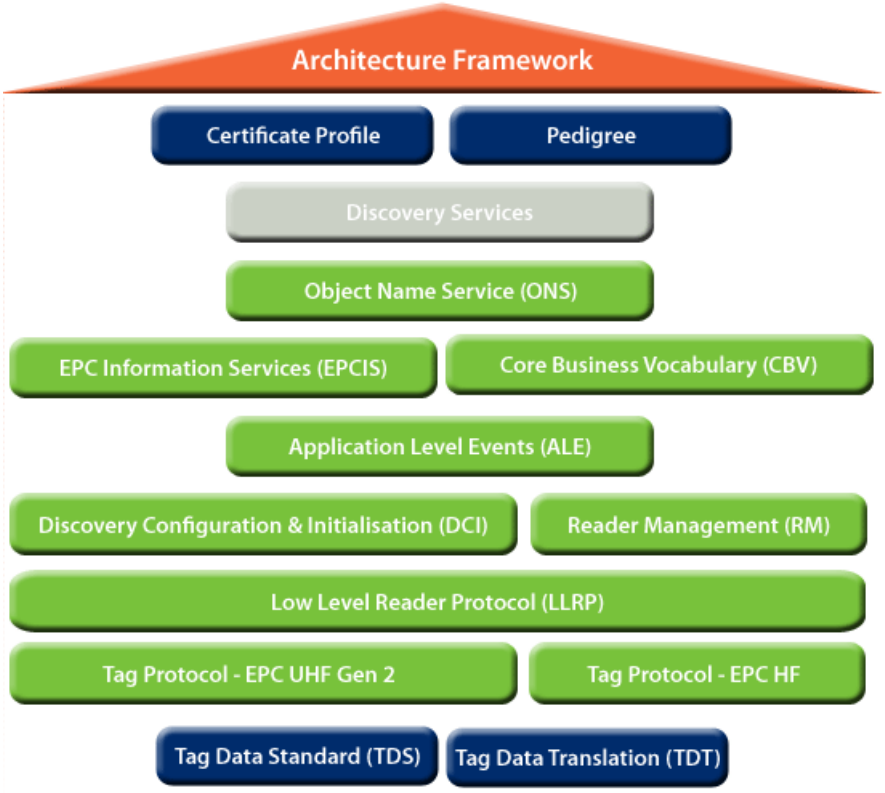

Figure 4 — EPCglobal standards overview

This "house" of standards has basically been developed "from scratch" when members of EPCglobal got together to define standards for their "EPC Information System". It allowed the members to optimise the interfaces between the various elements of the standards "house".

Later the functionality of several elements of the GS1 "house" of standards were also moved into the ISO/IEC standards and the functionality of GS1 EPCglobal LLRP moved into ISO/IEC 24791-5.

ISO/IEC 24791-5 has been developed for readers using the ISO/IEC 18000-6 Type C (meanwhile succeeded by ISO/IEC 18000-63) air interface. It is based on GS1 EPCglobal LLRP and has some ISO/IEC specific extensions.

ISO/IEC 18000-3 Mode 3 and its equivalent GS1 EPCglobal HF AI standard have been published in 2010. GS1 EPCglobal never started LLRP development for the HF AI standard.

The origin of ISO/IEC 18000-3 Mode 1, ISO/IEC 15693, has been published in 2000. As of today no national body or other organisation identified a market need in order to develop such device interface in either ISO/IEC JTC1 SC31 or ISO/IEC JTC1 SC 17.

8.4 Conclusion

The fact that no national body or other organisation identified a market need in order to develop such device interface in either ISO/IEC JTC1 SC31 or ISO/IEC JTC1 SC 17 proofs that the industry never had a need for a standard with the requirements as listed in the scope.

Therefore the project team recommends dropping the development of the proposed device interface standard.

9 Threats through memory content in library RFID tags

9.1 Analysis

Library RFID tags based on ISO/IEC 18000-3 Mode 1 or Mode 3 contain a unique identifier that allows tracking of people wearing such tags if they get close enough to a reader. For small handheld devices the reading distance is in the 10 cm range. For clearly visible RFID gates it is in the 1 m range. While such a number only allows tracking it is much more important to take care about the personal information written on the tag.

For that reason it is important to check what elements are written on a tag. The library standard ISO 28560 defines 26 user elements, extensible to 31.

The Danish library standard INF 163 only uses a subset of the elements defined in ISO 28560. This subset helps to maintain certain privacy. However ISO 28560 covers more data elements. Some of these user elements critically endanger the privacy as the information is stored unprotected and anyone can read the tag and can get information as outlined in the 3rd column of Table 1.

This is independent whether ISO 28560 is implemented on an RFID tag according to ISO/IEC 15693, ISO/EC 18000-3 Mode 1 or ISO/IEC 18000-3 Mode 3 as none of them provides read protection for any memory used for data elements of ISO 28560.

Table 1 — Excerpt of critical data elements of ISO 28560

N	Name of the data element	Privacy impact
10	Order number	Allows exact identification of owners interest if a public number is selected
13	GS1 product identifier	Allows exact identification of owner's interest
17	Title	Allows exact identification of owner's interest
18	Product identifier local	May allow partly identification of owners interests (e.g. in case of very special suppliers as cancer medical research companies)
22	Alternative item identifier	May allow partly identification of owners interests (e.g. in case of very special suppliers as cancer medical research companies)

It is therefore recommended limiting the content of the tag to data elements that do not allow extracting information about the RFID tag holder without the LMS database. It is also recommended to consider this in applications standard. As a consequence the critical data elements in ISO 28560 shall be removed or modified accordingly.

9.2 Conclusion

ISO/IEC 18000-3 Mode 1 and Mode 3 do not support any read protection for the data elements of ISO 28560. Therefore, for both Mode 1 and Mode 3 the data elements shall be chosen with the same care in respect to privacy risks.

Annex A
(Informative)

Industry representatives

A.1 Libraries

NOTE This subclause lists the representative of the Library

A.1.1 KopGroep Bibliotheken

Address:
Bernhardplein 76
1781 HK Den Helder
The Netherlands
Website: www.KopGroepBibliotheken.nl

Contact person:
Laurens Kuik
Projectcoördinator ICT
Phone: +31 223 65 00 06
Email: l.kuik@kopgroepbibliotheken.nl

KopGroep Bibliotheken has branches in:
't Zand
Anna Paulowna
Bibliobus
Callantsoog
De Schooten
Den Helder Centrale
Harenkarspel
Julianadorp
Middenmeer
Niedorp
Nieuw Den Helder
Schagen
Texel
Wieringen
Wieringerwerf

A.1.2 Stadtbibliothek Hannover

Address:
Hildesheimer Straße 12
30169 Hannover
Germany
Website: www.stadtbibliothek-Hannover.de

Contact person:
Uwe Nietiedt
Bereichsleiter Betriebsbezogene Dienste -
Phone: +49 511 168 42878
Fax: +49 511 168 45076
Email: ??

A.2 Library RFID System Integrators

NOTE This subclause lists the representatives of the major European vendors

A.2.1 Bibliotheca

Address
Landmark House
Station Road
Cheadle Hulme
Stockport
SK8 7BS
United Kingdom
Web: www.bibliotheca.com

Contact persons
Jim Hopwood
President Europe & CTO
Phone: +44 (161) 498 1140
Email: j.hopwood@bibliotheca.com

Chadbourne, Andy
Director Marketing
Phone: +44 (161) 498 1140
Email: a.chadbourne@bibliotheca.com

A.2.2 Nedap

Address
Parallelweg 2
NL-7141 DC Groenlo
The Netherlands
Web: www.nedaplibrix.com

Contact person
Gerben Heinen
Technical Library Specialist
Phone: +31 544 471 550
Email: gerben.heinen@nedap.com

A.3 Providers of ISO/IEC 18000-3 readers

A.3.1 Feig

Address:
Lange Straße 4
D-35781 Weilburg-Waldhausen
Germany
Website: www.feig.de

Contact person:
Markus Desch
Phone: +49 6471 3109 426
Bus Fax: +49 6471 / 3109-99
E-mail: Markus.Desch@feig.de

A.3.2 Tagsys Europe

Address
785 Voie Antiope
Z.I. Athélia III
13600 La Ciotat
France
Website: www.tagsysrfid.com

Contact person
Pierre Matignon
Phone: +33 (4) 42188928
E-mail: pierre.matignon@tagsysrfid.com

Franck Dannunzio
Head of development group
E-mail: franck.dannunzio@tagsysrfid.com

Bibliography

[1] ISO/IEC 15693-1:2010, *Identification cards — Contactless integrated circuit cards — Vicinity cards — Part 1: Physical characteristics*

[2] ISO/IEC 15693-2:2006, *Identification cards — Contactless integrated circuit cards — Vicinity cards — Part 2: Air interface and initialization*

[3] ISO/IEC 15693-3:2009, *Identification cards — Contactless integrated circuit cards — Vicinity cards — Part 3: Anticollision and transmission protocol*

[4] ISO/IEC 18000-3, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

[5] ISO/IEC 18000-6, *Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General*

[6] ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

[7] ISO/IEC 24791-5, *Information technology — Radio frequency identification (RFID) for item management — Software system infrastructure — Part 5: Device interface*

[8] ISO 28560-1:2011, *Information and documentation — RFID in libraries — Part 1: Data elements and general guidelines for implementation*

[9] ISO 28560-2:2011, *Information and documentation — RFID in libraries — Part 2: Encoding of RFID data elements based on rules from ISO/IEC 15962*

[10] ISO 28560-3:2011, *Information and documentation — RFID in libraries — Part 3: Fixed length encoding*

[11] COMMISSION RECOMMENDATION 2009 on the implementation of privacy and data protection principles in applications

[12] EPCglobal UHF C1G2 V1.0.9, Specification for Air Interface EPCglobal EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.0.9, January 2005

[13] EPCglobal UHF C1G2 V1.1.0, Specification for Air Interface EPCglobal EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.1.0, 17 December 2005

[14] EPCglobal UHF C1G2 V1.2.0, Specification for Air Interface EPCglobal EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.2.0, 23 October 2008

[15] EPCglobal HF C1 V2.0.3, Specification for EPC HF Air Interface EPCglobal EPC™ Radio-Frequency Identity Protocols EPC Class-1 HF RFID Air Interface Protocol for Communications at 12.56 MHz Version 2.0.3, 5 September 2011

[16] EPCglobal Low Level Reader Protocol (LLRP) Version 1.1 Ratified Standard October 13, 2010, interface betwen RFID Readers and Clients

[17] ERC RECOMMENDATION 70-03, relating to the use of SRDs. Recommendation adopted by the Frequency Management, Regulatory Affairs and Spectrum Engineering Working Groups

[18] ISO/IEC 15961, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: application interface*

[19] ISO/IEC 15962, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: data encoding rules and logical memory functions*

[20] ISO/IEC 15963, *Information technology — Radio frequency identification for item management — Unique identification for RF tags*

[21] RFID Mandate ESOS_m436_EN (2).pdf

[22] SPECIFIC GRANT AGREEMENT for an ACTION; SA/CEN/ENTRJ000/2011-36 RFID (Radio Frequency Identification) 20111219 file "2011-36 RFID Grant Agreement EC.pdf"

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™