PD CEN/TR 16672:2014

BSI Standards Publication

Information technology — Privacy capability features of current RFID technologies

National foreword

This Published Document is the UK implementation of CEN/TR 16672:2014.

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 83897 2
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 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

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.

Access to a resource on the tag will only be granted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

5 Features to protect Consumer Privacy

5.1 General

This clause identifies features associated with the protection of consumer privacy. The list is presented in an order-ranking of approximate increasing protection level.

5.2 Unique chip ID or Tag ID

A unique chip ID feature is a factory programmed unique identification number of a tag that enables different tags to be reliably distinguished. The tag is traceable when the unique chip ID is accessible without protection and can then be linked to an individual that can then be tracked as well.

For some tags, the unique chip ID is an essential part of the air interface protocol to ensure that communication is with one tag and not others in the read range.

Access to the unique chip ID feature can be protected and might only be granted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

5.3 Chip selection with random number

The random number for access is only valid for one communication session between interrogator and tag and does change for the next session. Therefore it prevents tracking. The feature can be turned off or on. Access to the feature will only be granted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

Some tags that use a random number for access also have a unique chip ID, which can be protected as described in 5.2.

5.4 Reduced read range on the tag

The reduced read range feature allows a tag essentially reduce the distance it can communicate with an interrogator, compared to the distance when the feature is not enabled. An essential reduction could be down to 25 %. The feature can be turned off or on. Access to the feature will only be granted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

5.5 Untraceable

The Untraceability feature allows a tag to modify the amount of identifying information it exposes. The tag's reply could consist of configurable "fixed" and "variable" part. The feature can be turned off or on. Access to the feature will only be granted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

EXAMPLE In a tag that has no hardware feature of a permanent unique chip ID, there is still the possibility that data can be traced by the application of some form of serialisation, making the associated item an instance of a product. This is certainly a requirement in some applications. If the tagged is to remain in the possession of a person and the product identity needs to remain readable, all or part of the serialised component can be overwritten with a string of zero bits. This then renders the tag still readable, but reduces the uniqueness. Removing 16 bits makes the tag and the item the same as 65,535 other instances of the same product and less traceable.

5.6 Hide

The Hide feature allows a tag to be unresponsive until it gets authenticated by an interrogator. The feature can be turned off or on. Access to the feature will only be granted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

5.7 Kill

The Kill feature allows an interrogator to Kill the tag and render it unreadable, even though it remains attached to its associated item. The Kill feature can only be used after the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

After a successful execution of a Kill command the tag will remain permanently silent and can never be activated or turned on again.

5.8 Destroy

All previous features are associated with the functionality of the chip. The Destroy feature will render a tag permanently silent by physically destroying the chip or the antenna, which is essential for communication. If the antenna is cut, on certain types the tag might not function anymore.

5.9 Remove

A tag may be removed from an object. Although the tag remains readable, the associated link with a person or item is broken.

6 Features to protect Data Security

6.1 Features to protect Read access to the tag data

6.1.1 Protection level

The features in this clause are listed in order of increased protection level.

6.1.2 "Normal" Read access

"Normal" Read access allows data to be read from the tag's memory. In fact memory with "normal" Read access contains no protection and is considered as the lowest protection level.

6.1.3 Read (Lock) protection

6.1.3.1 General

Read, or Read Lock protection prevents all or part of the memory of a tag can be read by an interrogator. Read access to all or part of the tags memory will only be granted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

The read lock feature can be temporary or permanent.

6.1.3.2 Temporary read Lock protection

A temporary lock can be lifted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

6.1.3.3 Permanent (or Perma) read Lock protection

A permanent lock cannot be changed. Data that has been written to a permanently locked memory can never be read again.

6.1.4 Data protection using the TID

The TID can be used to protect the data on the tag against interpreting. The data can be encrypted with a combination of the TID and a secret key, before it is written on the tag. When the data is read from the tag is has no meaning unless the interrogator can decrypt it with the right secret key.

6.2 Features to protect Write access to the tag data

6.2.1 General

The features in this clause are listed in order of increased protection level.

6.2.2 Protection level

6.2.3 "Normal" Write access

"Normal" Write access allows data to be written, erased and rewritten into memory. In fact memory with "Normal" Write access contains no protection and is, in this document, considered as the lowest protection level.

6.2.4 Write (Lock) protection

6.2.4.1 General

Write, or Write Lock protection prevents that all or part of the memory of a tag can be written, erased and rewritten into memory by an interrogator. Write access to all or part of the tags memory will only be granted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

This feature can provide protection against writing the content of the UII or part of the user memory.

The write lock feature can be temporary or permanent.

6.2.4.2 Temporary write Lock protection

A temporary lock can be lifted when the interrogator has received the "authenticated" state, through a successful authentication with either a password or cryptographic key.

6.2.4.3 Permanent (or Perma) write Lock protection

A permanent lock cannot be changed. Data that has been written to a permanently locked memory can never be changed again.

6.2.5 Write protection using the TID

Before it is written to the memory, the data can be protected by encrypting it with a combination of a secret key and the TID. Incorporating the TID into the encryption process protects the data for unwanted altering, because altering the data makes it meaningless after decrypting it with the TID and the secret key. Incorporating the TID also prevents cloning of a tag, for when the data of a tag is copied onto another tag, the data cannot be decrypted because the TID will be different.

6.2.6 Write protection using a digital signature in User Memory

The interrogator can use a secret key to generate a digital signature of the data that is stored on the tag (using a cryptographic algorithm). The digital signature can be stored in user memory. After reading the data, its validity can be verified by generating a new digital signature and verifying it with the signature that is stored in user memory.

Since TID is unique for every tag, it can be used to tie the data to the tag if it is combined with the secret key to generate the digital signature. Tying the TID to the digital signature also prevents cloning of the tag by copying the data and the digital signature to another tag.

7 Features for tag authentication

7.1 General

Tag authentication can be used to verify ownership or origin.

The features in this clause are listed in order of increased protection level.

7.2 Verification using the Unique chip ID or Tag ID

The Unique chip ID or Tag ID can be used to verify the authenticity of a tag if the Unique chip ID or Tag ID of all authentic tags is stored in a database. Authenticity can then be verified by reading the Unique chip ID or Tag ID and performing a look-up in the database to verify if the Unique chip ID or Tag ID is present.

7.3 Verification using the Unique chip ID or Tag ID with a digital signature

The owner of a tag can use a secret key to generate a digital signature of the tag's Unique chip ID or Tag ID (using a cryptographic algorithm) and store that signature in the tag's user memory. The authenticity of the tag can be verified by reading the Unique chip ID or Tag ID, generating the digital signature with the secret key and verifying the result with the digital signature that is stored in the tag's user memory.

A practical application would be to authenticate the originality of the product that the tag is attached to. As an example, the owner of a pallet pool can authenticate his ownership by encrypting the TID of the tag that is attached to one of his pallets, with his secret key.

7.4 Verification using a password

The issuer of a tag can store a password on the tag. Authenticity can then be verified by reading authenticating the tag with the right password. The tag is authentic if the authentication is successful.

8 Standards support of privacy capability features

This clause provides an overview on how standards support the privacy capability features. Details for each standard are then described in the subsequent subclauses.

The relevant standards are listed in Table 1. Table 2 provides a list of additional standards that are already covered through standards listed in Table 1.

The abbreviations in Table 1 have the following meaning:

N	not supported by standard
Y	supported by standard; can be used by application
O	supported by standard, but it is only optional
A	application dependent

Table 1 — Overview on standards support of privacy capability features

REF	PRIVACY CAPABILITY FEATURE	ISO/IEC 14443 **(Note 3**	ISO/IEC 15693	ISO/IEC 18000-2	ISO/IEC 18000-3, M2	ISO/IEC 18000-3, M3	ISO/IEC 18000-4, M1	ISO/IEC 18000-4, M2	ISO/IEC 18000-61:2012	ISO/IEC 18000-62:2012	ISO/IEC 18000-6:2004 **Am1: 2006**	ISO/IEC 18000-63:2013	ISO/IEC 18000-63, REV1 **(Note 5)**	ISO/IEC 18000-64:2012	ISO/IEC 18000-7	ISO/IEC 18092 **(Note 3)**	ISO/IEC 21481 **(Note 3)**
5.2.2	Password protection (See NOTE 2)	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
5.2.2.1	Password protection with security timeout	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
5.2.2.2	Password protection with cover coding (See NOTE 2)	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
5.2.3	Cryptographic protection	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
5.2.3.2	Symmetric-key cryptography	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
5.2.3.3	Public-key cryptography	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
5.3	Application of access protection features (See NOTE 2)	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
6.2	Unique chip ID or Tag ID (See NOTE 4)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
6.3	Chip selection with random number	Y	N	N	N	N	N	N	N	N	N	N	Y	N	N	Y	Y
6.4	Reduced read range on the tag	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
6.5	Untraceable	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N

6.6	Hide	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
6.7	Kill	N	N	N	N	O	N	N	N	N	O	O	O	N	N	N	N
6.8	Destroy (See NOTE 1)	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
6.9	Remove	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
7.1.3	Read (Lock) protection	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
7.1.3.1	Temporary read Lock protection	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
7.1.3.2	Permanent (or Perma) read Lock protection	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
7.1.4	Data protection using the TID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
7.2.3	Write (Lock) protection	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
7.2.3.1	Temporary write Lock protection	N	N	N	N	Y	N	N	N	N	Y	Y	Y	N	Y	N	N
7.2.3.2	Permanent (or Perma) write Lock protection	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
7.2.4	Write protection using the TID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
7.2.5	Write protection using a digital signature in User Memory	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
8.1	Verification using the Unique chip ID or Tag ID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
8.2	Verification using the Unique chip ID or Tag ID with a digital signature	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
8.3	Verification using a password	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

NOTE 1 Cutting the antennas of tags based on wave propagation as it is usually above 100 MHz usually substantially reduces the communication distance, but a few millimetres or centimetres may remain.

NOTE 2 In ISO/IEC 18000-3 Mode 3 and ISO/IEC 18000-6:2004 Am1: 2006 the password only protects the reserved memory bank. The cover coding does not help in protecting the consumer privacy as it only applies for protecting the password.

NOTE 3 For ISO/IEC 14443, ISO/IEC 18092 and ISO/IEC 21481 security is defined outside the air interface standard in for example. ISO/IEC 7816-4.

NOTE 4 For ISO/IEC 18000-6:2004 Am1: 2006, ISO/IEC 18000-63:2013 the TID may not be unique as it is no requirement in the standard, however, most product vendors provide serialisation.

NOTE 5 For ISO/IEC 18000-63, REV1 is not published yet and is expected for 2014.

Table 2 — Standard cross references

Standard	Reference	Remark
EPCglobal HF C1 V2.0.3	ISO/IEC 18000-3, M3	
EPCglobal UHF C1G2 V1.0.9 (2005)	EPCglobal UHF C1G2 V1.1.0	EPCglobal UHF C1G2 V1.1.0 covers all elements relevant for EPCglobal UHF C1G2 V1.0.9 The EPCglobal version is equivalent to Type C in the ISO standard
EPCglobal UHF C1G2 V1.1.0 (2006)	ISO/IEC 18000-6:2004, AM1:2006	The EPCglobal version has been the input for ISO Type C in the ISO standard and the modification required became
EPCglobal UHF v 1.2.0 (2008)	ISO/IEC 18000-6:2010	The EPCglobal version is equivalent to Type C in the ISO standard
EPCglobal UHF C1G2 V1.2.0 (2008)	ISO/IEC 18000-63:2013	The EPCglobal version is equivalent to Type C in the ISO standard
ISO 11784/85	ISO/IEC 18000-2	
ISO 14223	ISO/IEC 18000-2	
ISO/IEC 18000-3, M1	ISO/IEC 15693	For RFID for item management, ISO/IEC 18000-3, M1 defines a number of features as required. These include obvious features such as the need to be able to read and write data. In contrast ISO/IEC 15693 defines these as optional.
ISO/IEC 18000-6:2004		The update from ISO/IEC 18000-6:2004 Type A to ISO/IEC 18000-61 does not contain any relevant change The update from ISO/IEC 18000-6:2004 Type B to ISO/IEC 18000-62 does not contain any relevant change
ISO/IEC 18000-6:2010	ISO/IEC 18000-6:2012, ISO/IEC 18000-61:2012, ISO/IEC 18000-62:2012, ISO/IEC 18000-63:2013, ISO/IEC 18000-64:2012	This document has been split into ISO/IEC 18000-6:2012 (General), ISO/IEC 18000-61:2012 (Type A), ISO/IEC 18000-62:2012 (Type B), ISO/IEC 18000-63:2013 (Type C), ISO/IEC 18000-64:2012 (Type D),
ISO/IEC 18000-6:2012		Since the 2012 issue this standard only contains general information and references to ISO/IEC 18000-61, 62, -63 and -64
NF C IP1	ISO/IEC 18092	
NF C IP2	ISO/IEC 21481	
NOTE See Bibliography for full title of the listed standards.		

9 Proprietary features

Some products on the marked offer proprietary features, that help to improve privacy. However, using such features means a deviation from the standard and means at least loosing compliance temporarily.

Bibliography

[1] ISO/IEC 14443-1:2008, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 1: Physical characteristics*

[2] ISO/IEC 14443-1. *Amd*. 2008, **1** p. 2012 [Additional PICC classes]

[3] ISO/IEC 14443-2:2010, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 2: Radio frequency power and signal interface*

[4] ISO/IEC 14443-2. *Amd*. 2010, **1** p. 2011 [Limits of electromagnetic disturbance levels parasitically generated by the PICC]

[5] ISO/IEC 14443-2. *Amd*. 2010, **2** p. 2012 [Additional PICC classes]

[6] ISO/IEC 14443-2:2010/Amd, 3:2012, *Bits rates of fc/8, fc/4 and fc/2*

[7] ISO/IEC 14443-3:2011, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 3: Initialization and anticollision*

[8] ISO/IEC 14443-3. *Amd*. 2011, **1** p. 2011 [Electromagnetic disturbance handling and single-size unique identifier]

[9] ISO/IEC 14443-4:2008, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 4: Transmission protocol*

[10] ISO/IEC 14443-4. *Amd*. 2008, **1** p. 2012 [Exchange of additional parameters]

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

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

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

[14] ISO/IEC 18000-1, *Information technology — Radio frequency identification for item management — Part 1: Reference architecture and definition of parameters to be standardized*

[15] ISO/IEC 18000-2, *Information technology — Radio frequency identification for item management — Part 2: Parameters for air interface communications below 135 kHz*

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

[17] ISO/IEC 18000-4, *Information technology — Radio frequency identification for item management — Part 4: Parameters for air interface communications at 2,45 GHz*

[18] 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*

[19] ISO/IEC 18000-61, *Information technology — Radio frequency identification for item management — Part 61: Parameters for air interface communications at 860 MHz to 960 MHz Type A*

[20] ISO/IEC 18000-62, *Information technology — Radio frequency identification for item management — Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B*

[21] 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*

[22] ISO/IEC 18000-64, *Information technology — Radio frequency identification for item management — Part 64: Parameters for air interface communications at 860 MHz to 960 MHz Type D*

[23] ISO/IEC 18000-7, *Information technology — Radio frequency identification for item management — Part 7: Parameters for active air interface communications at 433 MHz*

[24] ISO/IEC 18092:2013, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)*

[25] ISO/IEC 21481:2012, *Information technology — Telecommunications and information exchange between systems — Near Field Communication Interface and Protocol -2 (NFCIP-2)*

[26] 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*

[27] 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*

[28] 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*

[29] 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*

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.

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 Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™