



NSAI
Standards

Irish Standard Recommendation
S.R. CEN/TR 16672:2014

Information technology - Privacy capability features of current RFID technologies

S.R. CEN/TR 16672:2014

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:

CEN/TR 16672:2014

Published:

2014-06-04

This document was published under the authority of the NSAI and comes into effect on:

2014-06-21

ICS number:

35.240.60

NOTE: If blank see CEN/CENELEC cover page

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

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.....	4
Introduction	5
1 Scope	6
2 Terms and definitions	6
3 Symbols and abbreviations	7
4 Access protection features.....	7
4.1 General.....	7
4.2 Overview of access protection features.....	7
4.2.1 General.....	7
4.2.2 No protection.....	7
4.2.3 Password protection	7
4.2.4 Cryptographic protection.....	8
4.3 Application of access protection features	9
5 Features to protect Consumer Privacy.....	10
5.1 General.....	10
5.2 Unique chip ID or Tag ID	10
5.3 Chip selection with random number.....	10
5.4 Reduced read range on the tag	10
5.5 Untraceable	10
5.6 Hide	11
5.7 Kill	11
5.8 Destroy.....	11
5.9 Remove	11
6 Features to protect Data Security	11
6.1 Features to protect Read access to the tag data.....	11
6.1.1 Protection level	11
6.1.2 "Normal" Read access	11
6.1.3 Read (Lock) protection.....	11
6.1.4 Data protection using the TID.....	12
6.2 Features to protect Write access to the tag data	12
6.2.1 General.....	12
6.2.2 Protection level	12
6.2.3 "Normal" Write access	12
6.2.4 Write (Lock) protection	12
6.2.5 Write protection using the TID	12
6.2.6 Write protection using a digital signature in User Memory	13
7 Features for tag authentication	13
7.1 General.....	13
7.2 Verification using the Unique chip ID or Tag ID	13
7.3 Verification using the Unique chip ID or Tag ID with a digital signature	13
7.4 Verification using a password.....	13
8 Standards support of privacy capability features	13
9 Proprietary features.....	17
Bibliography	18

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*

CEN/TR 16672:2014 (E)

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

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
 - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-