PD CEN/TR 16670:2014

BSI Standards Publication

Information technology — RFID threat and vulnerability analysis

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 16670:2014.

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 83895 8
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 16670

June 2014

ICS 35.240.60

English Version

Information technology - RFID threat and vulnerability analysis

Technologies de l'information - RFID, analyse vulnérabilité et de menace

Informationstechnik - Analyse zur Bedrohung und Verletzlichkeit durch beziehungsweise von RFID

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 16670:2014 E

Contents

Page

Foreword

This document (CEN/TR 16670:2014) 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 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 Europesteps 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 standardization work programme identified in the first phase.

This document will provide the additional information of the RFID application that will need to be provided to a citizen by accessing the source identified on the sign where the RFID application is operating. This information will be aligned with the details set out in the Recommendation, but some of this might not be available at the outset, a Technical Report is the preferred form of initial delivery to establish basic requirements.

1 Scope

The scope of the Technical Report is to consider the threats and vulnerabilities associated with specific characteristics of RFID technology in a system comprising:

— the air interface protocol covering all the common frequencies;

— the tag including model variants within a technology;

— the interrogator features for processing the air interface;

— the interrogator interface to the application.

The Technical Report addresses specific RFID technologies as defined by their air interface specifications. The threats, vulnerabilities, and mitigating methods are presented as a toolkit, enabling the specific characteristics of the RFID technology being used in an application to be taken into consideration. While the focus is on specifications that are standardized, the feature analysis can also be applied to proprietary RFID technologies. This should be possible because some features are common to more than one standardized technology, and it should be possible to map these to proprietary technologies.

Although this Technical Report may be used by any operator, even for a small system, the technical details are better considered by others. In particular the document should be a tool used by RFID system integrators, to improve security aspects using a privacy by design approach. As such it is also highly relevant to operators that are not SME's, and to industry bodies representing SME members.

2 Terms and definitions

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

2.1
blocker tag
tag forcing the reader to enter in its singulation algorithm

Note 1 to entry: The idea of the blocker tag that looks like a tag that we can have in our pocket, is to emit both '0' and '1' creating a collision and forcing the reader to enter in its singulation algorithm. If the blocker tag emits simultaneously '0' and '1' (that requires two antennas), the reader may never complete its algorithm. The blocker tag should be seen as a hacker device that is able to generate a denial of service in a legitimate system. We can even assess that a blocker tag has always a malicious behaviour since it cannot be selective and forbids the reading of one tag whereas it authorises the reading of the others. Moreover, the blocker tag works like a tag in a passive mode. So, it requires being in the reader field and it will protect only a small volume around itself. So a blocker tag can be considered as a malicious tag, which prevents a legal system to read legal tags or as a mitigation technique preventing an illegal reader to read a legal tag.

2.2
blocking
another way to produce a denial of service is to interfere during the anti-collision sequence

Note 1 to entry: Different devices have been developed.

2.3
cloning
impersonation technique that is used to duplicate data from one tag to another

Note 1 to entry: Data acquired from the tag by whatever means is written to another tag. Unless the technology and application require the interrogator to authenticate the RFID tag, cloning is possible. Cloning the unique chip ID presents a significantly bigger challenge for the attacker, but some researchers claim that this is possible. There is also a special case of cloning that needs to be considered where the application accepts multiple AIDC technologies. Cloning data from an RFID-enabled card can be replicated in magnetic stripe. In some payment card systems, information that might be