PD ISO/IEC/TS 29167-15:2017

BSI Standards Publication

Information technology — Automatic identification and data capture techniques

Part 15: Crypto suite XOR security services for air interface communications

bsi.

National foreword

This Published Document is the UK implementation of PD ISO/IEC/TS 29167-15:2017.

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 2017

ISBN 978 0 580 94583 0

ICS 35.040.50

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 31 December 2017.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/IEC/TS 29167-15:2017

TECHNICAL SPECIFICATION

ISO/IEC TS 29167-15

First edition
2017-09

Information technology — Automatic identification and data capture techniques —

Part 15: Crypto suite XOR security services for air interface communications

Technologies de l'information — Techniques automatiques d'identification et de capture de données —

Partie 15: Services de sécurité par suite cryptographique XOR pour communications d'interface radio

Reference number
ISO/IEC TS 29167-15:2017(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the m teeaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

A list of all parts in the ISO/IEC 29167 series can be found on the ISO website.

Introduction

This document defines a coding suite based on an exclusive or (XOR) operation for the ISO/IEC 18000 air interfaces standards for radio frequency identification (RFID) devices.

XOR is a type of logical disjunction on two operands that results in a value of true if exactly one of the operands has a value of true. The primary advantage of XOR operation is that it is simple to implement and that the XOR operation is computationally inexpensive for hiding information in cases where either no particular or light security is required. The simple implementation of XOR does not require a cipher and therefore limits the security protection and attacks like eaves dropping are much easier.

The security service tag authentication is a mandatory security service. All other services in this coding suite are optional. Every manufacturer has the liberty to chose which of these services will be implemented on a tag.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning radio-frequency identification technology given in the clauses identified below.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured the ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC.

Information on the declared patents may be obtained from:

Patent holder: China IWNCOMM Co., Ltd.

Address: A201, QinFengGe, Xi'an Software Park,
No. 68, Keji 2nd Road,
Xi'an Hi-Tech Industrial Development Zone
Xi'an, Shaanxi, P. R. China 710075

The latest information on IP that may be applicable to this document can be found at www.iso.org/patents.

Information technology — Automatic identification and data capture techniques —

Part 15: Crypto suite XOR security services for air interface communications

1 Scope

This document defines a coding suite based on an exclusive or (XOR) operation for the ISO/IEC 18000 air interfaces standards for radio frequency identification (RFID) systems. In particular, it specifies the use of XOR as a basic way to hide plain data in the identity authentication and secure communication procedures. The coding suite is defined in alignment with existing air interfaces.

This document defines various authentication methods and methods of use for the XOR. A tag and an interrogator may support one, a subset, or all of the specified options, clearly stating what is supported.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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*

ISO/IEC 19762 (all parts), *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 (all parts) and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
command
<message> command that interrogator sends to tag with "Message" as parameter

3.1.2
message
part of the command that is defined by the CS