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)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms, definitions, symbols and abbreviated terms ... **1**
3.1 Terms and definitions ... 1
3.2 Symbols and abbreviated terms ... 2
3.2.1 Symbols ... 2
3.2.2 Abbreviated terms ... 2
4 Conformance ... **3**
4.1 Claiming conformance ... 3
4.2 Interrogator conformance and obligations ... 3
4.3 Tag conformance and obligations ... 3
5 Cipher introduction ... **3**
6 Parameter definitions ... **4**
7 State diagram ... **5**
8 Initialization and resetting ... **5**
9 Authentication ... **6**
9.1 General ... 6
9.2 Authentication procedure ... 6
9.2.1 Protocol requirements ... 6
9.2.2 Procedure ... 6
10 Secure communication (optional) ... **8**
11 Key update (optional) ... **9**
Annex A (normative) **State transition tables** ... **10**
Annex B (normative) **Error codes and error handling** ... **11**
Annex C (informative) **Cipher Description** ... **12**
Annex D (informative) **Test vectors** ... **13**
Annex E (normative) **Protocol specific** ... **14**
Annex F (normative) **Authentication procedure pseudo-code** ... **18**
Annex G (informative) **Security considerations** ... **21**
Bibliography ... **22**

© ISO/IEC 2017 – All rights reserved

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.

© ISO/IEC 2017 – All rights reserved

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.

© ISO/IEC 2017 – All rights reserved

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

© ISO/IEC 2017 – All rights reserved

3.1.3
reply
<response> reply that tag returns to the interrogator with "Response" as parameter

3.1.4
response
part of the reply (stored or sent) that is defined by the CS

3.2 Symbols and abbreviated terms

3.2.1 Symbols

$\oplus$	exclusive or
#	number
$xxxx_h$	hexadecimal notation
||	concatenation
O_n	fixed value
+	a + b means a addition b mod 2^n, the length of a and b is n.
–	a – b means binary subtraction operation. Given two binary numbers a and b, the operation a – b outputs the result of subtracting b from a. NOTE The easiest way to subtract the second binary number from the first one is to make the second number negative and then add it with the first number.
mod	modulo operation

3.2.2 Abbreviated terms

CRC	cyclic redundancy check
CS	coding suite
CSI	coding suite identifier
EBV	extensive bit vector (see ISO/IEC 18000-63)
ID	identifier
MAC	message authentication code
PSK	pre-shared key
RFID	radio frequency identification
RFU	reserved for future use
RN	random number
SK	session key

© ISO/IEC 2017 – All rights reserved

TRAIS tag and reader air interface security

TRAIS-X tag and reader air interface security based on XOR

XOR exclusive or

4 Conformance

4.1 Claiming conformance

To claim conformance with this document, an interrogator or tag shall comply with all relevant clauses of this document, except those marked as “optional”.

4.2 Interrogator conformance and obligations

To conform to this document, an interrogator shall

— implement the mandatory commands defined in this document, and conform to the relevant part of ISO/IEC 18000.

To conform to this document, an interrogator may

— implement any subset of the optional commands defined in this document.

To conform to this document, the interrogator shall not

— implement any command that conflicts with this document, or

— require the use of an optional, proprietary or custom command to meet the requirements of this document.

4.3 Tag conformance and obligations

To conform to this document, a tag shall

— implement the mandatory commands defined in this document for the supported types and conform to the relevant part of ISO/IEC 18000.

To conform to this document, a tag may

— implement any subset of the optional commands defined in this document.

To conform to this document, a tag shall not

— implement any command that conflicts with this document, or

— require the use of an optional, proprietary or custom command to meet the requirements of this document.

5 Cipher introduction

The logical operation exclusive disjunction, also called eXclusive OR (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 and often used for bitwise operations or algebra computing. For example:

© ISO/IEC 2017 – All rights reserved