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 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 meaning 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

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

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:

Bitwise operation:

- $1 \oplus 1 = 0$
- $1 \oplus 0 = 1$
- $0 \oplus 1 = 1$
- $0 \oplus 0=0$
- $a \oplus b = a + b \pmod 2$

The XOR operator is extremely common as a component in complex ciphers. By itself, using a constant repeating key, a simple XOR crypto can trivially be broken using frequency analysis. If the content of any message can be guessed or otherwise known then the key can be revealed (the XOR crypto is vulnerable to a known-plaintext attack, since plaintext ⊕ ciphertext = key). Its primary advantage is that it is simple to implement and that the XOR operation is computationally inexpensive. A simple repeating XOR crypto is therefore sometimes used for hiding information in cases where either no particular or light security is required. For detailed cipher descriptions, see Annex C. For some security considerations of this coding suite, see Annex G.

6 Parameter definitions

Table 1 — Definition of parameters

Parameter	Description
Command Code [7:0]	The values of security commands (See 3.1.1 for the definition of Command)
RFU[7:0]	The reserved values for future use
Coding Suite ID [7:0]	CSI: coding suite identifier
Length[Variable]	The length of message with extensive bit vector format
Payload[Variable]	Message data (See 3.1.2 for the definition of Message)
CRC-16[15:0]	The cyclic redundancy check value
Message	See 3.1.2
Reply	See 3.1.3
Response	See 3.1.4
RN[63:0]	64-bit random number
Header[1:0]	The value of header
AuthType[1:0]	This shows the authentication type in the authentication procedure. The values are as follows: — 00: mutual authentication — 01: interrogator authentication — 10: tag authentication — 11: RFU
AuthStep[2:0]	This shows the step number in the authentication procedure. The values are as follows: — 000: RFU — 001: Step 1 of Authenticate command — 010: Step 2 of Authenticate command — 011-111: RFU

Table 1 *(continued)*

Parameter	Description
Key ID[4:0]	The key identifier that the tag and interrogator used in the authentication procedure.
AuthData[Variable]	This shows the data computed in the authentication procedure. The values are as follows: — $\text{SORNi} = (\text{RNi}' + \text{O}_n) \oplus \text{PSK}'$ — $\text{SORNt} = (\text{RNt}' + \text{O}_n) \oplus \text{PSK}'$ — $\text{SRNi} = \text{RNi} \oplus \text{PSK}$ — $\text{SRNt} = \text{RNt} \oplus \text{PSK}$ — NULL where — RNi′ : RNi′ means bit-wise ROTATE RNi left for n bits, where RNi is a 64-bit random number generated by an interrogator, n is the number of binary value 1 of RNi — RNt : RNt′ means bit-wise ROTATE RNt left for n bits, where RNt is a 64-bit random number generated by a tag, n is the number of binary value 1 of RNt — O_n : 5555 5555 5555 5555h — PSK′: PSK′ means bit-wise ROTATE PSK left for n bits, PSK is a value of pre-shared key (64-bit), n is the number of binary value 1 of RNi or RNt
MAC[127:0]	The value of message authentication code

7 State diagram

Figure 1 shows the state machine of XOR coding suite. The state diagram for this coding suite consists of four states. For state transition tables, Annex A shall be consulted.

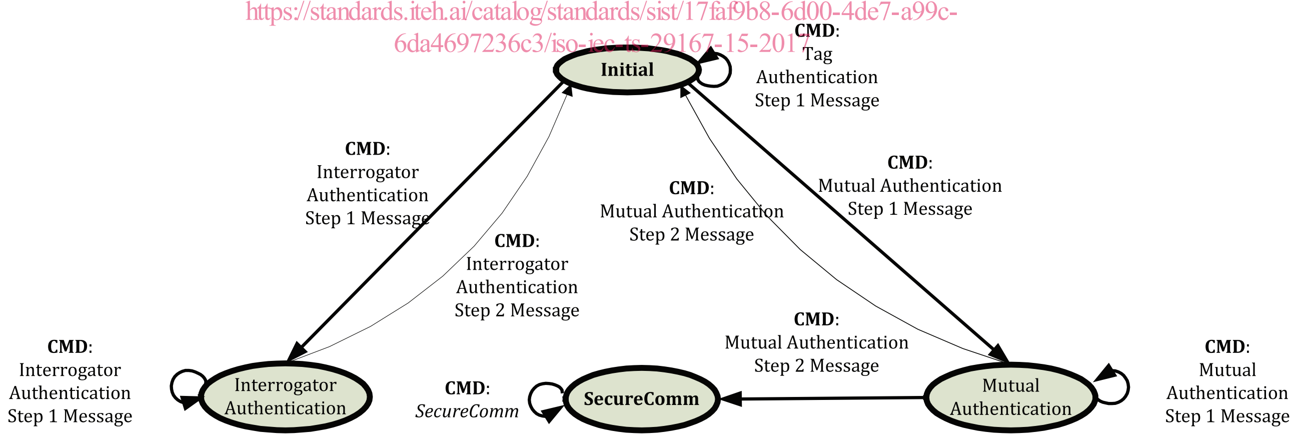
Initial
CMD: Tag Authentication Step 1 Message
CMD: Interrogator Authentication Step 1 Message
CMD: Mutual Authentication Step 2 Message
CMD: Mutual Authentication Step 1 Message
CMD: Interrogator Authentication Step 2 Message
CMD: Mutual Authentication Step 2 Message
CMD: Interrogator Authentication Step 1 Message
Interrogator Authentication
CMD: SecureComm
SecureComm
Mutual Authentication
CMD: Mutual Authentication Step 1 Message

Figure 1 — State diagram

8 Initialization and resetting

This document shall implement an **Initial** state.

After power-up and after a reset of the coding suite the tag moves into the **Initial** state.

Implementations of this suite shall assure that all memory used for intermediate results is cleared after each operation (message-response pair) and after reset.

9 Authentication

9.1 General

This document describes additions to the ISO/IEC 18000 series of standards protocol to support the tag and reader air interface security (TRAIS) based on XOR (TRAIS-X). Specially, it defines

— the use of XOR crypto for mutual, interrogator and tag authentication procedures;

— the use of XOR crypto for secure communication;

— the encoding in the related commands and the processing of those messages.

Figures 2 and 3 shows protocol flows of mutual and interrogator, and tag authentication procedures, respectively.

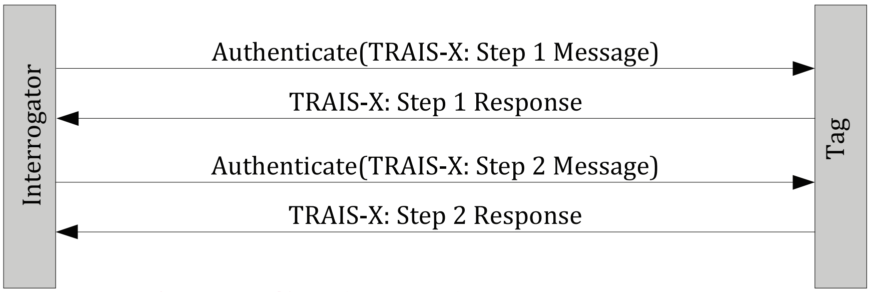
Interrogator
Authenticate(TRAIS-X: Step 1 Message)
TRAIS-X: Step 1 Response
Authenticate(TRAIS-X: Step 2 Message)
TRAIS-X: Step 2 Response
Tag

Figure 2 — TRAIS-X mutual and interrogator authentication protocol flows

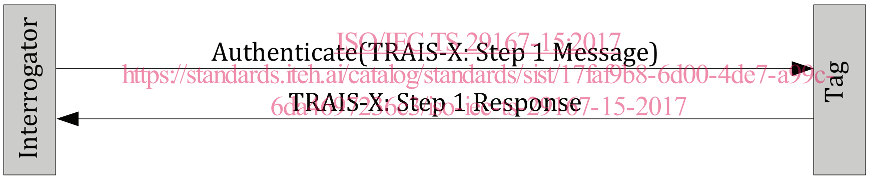

Figure 3 — TRAIS-X tag authentication

The formats of authenticate and response commands are shown in Table E.1 and Table E.2, respectively.

9.2 Authentication procedure

9.2.1 Protocol requirements

The authentication protocol requires that a tag and interrogator should have a PSK before they start the authentication procedure. How to generate and set a high quality PSK is out of the scope of this document. A key update function is supported and described in Clause 11. For error codes and error handling, the process in Annex B shall be followed.

9.2.2 Procedure

9.2.2.1 Mutual authentication

The mutual authentication procedure is as follows.

a) The interrogator

1) generates a random number RNi,