INTERNATIONAL STANDARD

ISO/IEC 29167-19

Second edition
2019-06

Information technology — Automatic identification and data capture techniques —

Part 19: Crypto suite RAMON security services for air interface communications

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

Partie 19: Services de sécurité par suite cryptographique RAMON pour communications par interface radio



Reference number
ISO/IEC 29167-19:2019(E)

© ISO/IEC 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Conformance **2**
4.1 Claiming conformance 2
4.2 Interrogator conformance and obligations 2
4.3 Tag conformance and obligations 2

5 Symbols and abbreviated terms **3**
5.1 Symbols 3
5.2 Abbreviated terms 3
5.3 Notation 4

6 Crypto suite introduction **5**
6.1 Overview 5
6.2 Authentication protocols 6
6.2.1 Tag identification 6
6.2.2 Symmetric mutual authentication 7
6.3 Send sequence counter 8
6.4 Session key derivation 9
6.4.1 General 9
6.4.2 KDF in counter mode 9
6.4.3 Key derivation scheme 10
6.5 IID, SID, used keys and their personalization 11
6.6 Key table 13

7 Parameter definitions **14**

8 State diagrams **14**
8.1 General 14
8.2 State diagram and transitions for Tag identification 15
8.2.1 General 15
8.2.2 Partial result mode 15
8.2.3 Complete result mode 16
8.3 State diagram and transitions for mutual authentication 17
8.3.1 General 17
8.3.2 Partial result mode 17
8.3.3 Complete result mode 18
8.3.4 Combination of complete and partial result mode 19

9 Initialization and resetting **20**

10 Identification and authentication **20**
10.1 Tag identification 20
10.1.1 General 20
10.1.2 Partial result mode 20
10.1.3 Complete result mode 20
10.2 Mutual authentication 21
10.2.1 General 21
10.2.2 Partial result mode 21
10.2.3 Complete result mode 22
10.3 The Authenticate command 23
10.3.1 General 23
10.3.2 Message formats for Tag identification 23

© ISO/IEC 2019 – All rights reserved

10.3.3 Message formats for Mutual Authentication 24
10.4 Authentication response 25
10.4.1 General 25
10.4.2 Response formats for Tag identification 25
10.4.3 Response formats for mutual authentication 26
10.4.4 Authentication error response 28
10.5 Determination of result modes 29

11 Secure communication 30
11.1 General 30
11.2 Secure communication command 30
11.3 Secure Communication response 31
11.3.1 General 31
11.3.2 Secure communication error response 31
11.4 Encoding of Read and Write commands for secure communication 31
11.5 Application of secure messaging primitives 32
11.5.1 General 32
11.5.2 Secure Communication command messages 33
11.5.3 Secure Communication response messages 34
11.5.4 Explanation of cipher block chaining mode 37
11.6 Padding for Symmetric Encryption 38

Annex A (informative) **State transition tables 39**

Annex B (informative) **Error codes and error handling 42**

Annex C (normative) **Cipher description 43**

Annex D (informative) **Test vectors 53**

Annex E (informative) **Protocol specifics 56**

Annex F (informative) **Non-traceable and integrity-protected Tag identification 64**

Annex G (normative) **Description of the TLV record 67**

Annex H (informative) **Memory Organization for Secure UHF Tags 72**

Bibliography 76

 © ISO/IEC 2019 – 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.

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

For an explanation of 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 www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO/IEC 29167-19:2016), which has been technically revised.

The main changes compared to the previous edition are as follows:

— It was thought that the fixed RAMON key length (KE) of 1 024 bits for tag authentication, defined in the first edition of this document, would maybe not be sufficient for all future uses. The method proposed in this edition allows extending the length of the cryptographic RAMON key by discrete steps of 128 bits. Beyond the previously defined key length of 1 024 bits, key lengths of 1 152, 1 280, 1 408, 1 536, 1 664 bits and beyond become feasible. The current method does not limit the possible key length in any way. The key length only is limited by the ability to send the cryptographic authentication response, which is of equal length to the cryptographic key, back to the interrogator. Allowing extended key length makes sure that the RAMON encryption is future-proofed and security can be improved as needed.

— To support different key lengths in a generic approach, the mix function has been revised.

— To improve the readability and consistency of this document, the specification of the cipher and the description of the TLV record have been separated into independent subclauses.

— A new TLV-Structure, supporting data identifiers according to ASC MH 10, was added.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2019 – All rights reserved

Introduction

This document specifies the security services of a Rabin-Montgomery (RAMON) crypto suite. It is important to know that all security services are optional. The crypto suite provides Tag authentication security service.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standard 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 ensured 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:

NXP B.V.

411 East Plumeria
San Jose
CA-95134 1924
USA

Impinj, Inc.

400 Fairview Ave N, # 1200
Seattle, WA 98109
USA

Giesecke & Devrient GmbH

Prinzregentenstrasse 159
D-81607 Munich
Germany

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

© ISO/IEC 2019 – All rights reserved

Information technology — Automatic identification and data capture techniques —

Part 19: Crypto suite RAMON security services for air interface communications

1 Scope

This document defines the Rabin-Montgomery (RAMON) crypto suite for the ISO/IEC 18000 series of air interfaces standards for radio frequency identification (RFID) devices. Its purpose is to provide a common crypto suite for security for RFID devices that can be referred to by ISO/IEC for air interface standards and application standards.

This document specifies a crypto suite for Rabin-Montgomery (RAMON) for air interface for RFID systems. The crypto suite is defined in alignment with existing air interfaces.

This document defines various authentication methods and methods of use for the cipher. A Tag and an Interrogator can 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 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

ISO/IEC 15962:2013, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: data encoding rules and logical memory functions*

ISO/IEC 18000-3, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

ISO/IEC 18000-4, *Information technology — Radio frequency identification for item management — Part 4: Parameters for air interface communications at 2,45 GHz*

ISO/IEC 18000-63:2015, *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, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

3 Terms and definitions

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

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

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

© ISO/IEC 2019 – All rights reserved

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

3.1
authentication
service that is used to establish the origin of information

3.2
confidentiality
property whereby information is not disclosed to unauthorized parties

3.3
integrity
property whereby data have not been altered in an unauthorized manner since they were created, transmitted or stored

3.4
non-traceability
protection ensuring that an unauthorized interrogator is not able to track the tag location by using the information sent in the tag response

3.5
secure communication
communication between the tag and the interrogator by use of the *Authenticate* command, assuring authenticity, *integrity* (3.3) and *confidentiality* (3.2) of exchanged messages

4 Conformance

4.1 Claiming conformance

An Interrogator or Tag shall comply with all relevant clauses of this document, except those marked as "optional".

4.2 Interrogator conformance and obligations

An Interrogator shall implement the mandatory commands defined in this document and conform to ISO/IEC 18000-3, ISO/IEC 18000-4 or ISO/IEC 18000-63, as relevant.

An Interrogator may implement any subset of the optional commands defined in 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

A Tag shall implement the mandatory commands defined in this document for the supported types and conform to ISO/IEC 18000-3, ISO/IEC 18000-4 or ISO/IEC 18000-63, as relevant

A Tag may implement any subset of the optional commands defined in 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.

© ISO/IEC 2019 – All rights reserved