
**Information technology — Automatic
identification and data capture
techniques —**

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

*Technologie informative — Identification automatique et technique
capturé data —*

*Partie 19: Air interface pour les services de sécurité suite de crypto
RAMON*

This document is a preview generated by EBS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, 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	v
Introduction	vi
1 Scope	1
2 Conformance	1
2.1 Claiming conformance	1
2.2 Interrogator conformance and obligations	1
2.3 Tag conformance and obligations	1
3 Normative references	2
4 Terms and definitions	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 KDF in counter mode	9
6.4.2 Key Derivation Scheme	10
6.5 IID, SID, Used Keys and Their Personalisation	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 Partial Result Mode	15
8.2.2 Complete Result Mode	16
8.3 State diagram and transitions for mutual authentication	17
8.3.1 Partial Result Mode	17
8.3.2 Complete Result Mode	18
8.3.3 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 Partial Result Mode	20
10.1.2 Complete Result Mode	20
10.2 Mutual authentication	21
10.2.1 Partial Result Mode	21
10.2.2 Complete Result Mode	22
10.3 The Authenticate command	23
10.3.1 Message formats for Tag identification	23
10.3.2 Message formats for Mutual Authentication	24
10.4 Authentication response	25
10.4.1 Response formats for Tag identification	25
10.4.2 Response formats for mutual authentication	26
10.4.3 Authentication error response	28
10.5 Determination of Result Modes	29

11	Secure communication	30
11.1	Secure communication command	30
11.2	Secure Communication response	31
11.2.1	Secure communication error response	31
11.3	Encoding of Read and Write commands for secure communication	31
11.4	Application of secure messaging primitives	32
11.4.1	Secure Communication command messages	32
11.4.2	Secure Communication response messages	34
11.4.3	Explanation of cipher block chaining mode	37
Annex A	(normative) State transition tables	39
Annex B	(normative) Error codes and error handling	42
Annex C	(normative) Cipher description	43
Annex D	(informative) Test Vectors	58
Annex E	(normative) Protocol specific	61
Annex F	(informative) Non-traceable and integrity-protected Tag identification	68
Annex G	(informative) Memory Organization for Secure UHF Tags (Proposal)	71
Bibliography		75

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: [Foreword — Supplementary information](#).

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture*.

ISO/IEC 29167 consists of the following parts, under the general title *Information technology — Automatic identification and data capture techniques*:

- *Part 1: Security services for RFID air interfaces*
- *Part 10: Crypto suite AES-128 security services for air interface communications*
- *Part 11: Crypto suite PRESENT-80 security services for air interface communications*
- *Part 12: Crypto suite ECC-DH security services for air interface communications*
- *Part 13: Crypto suite Grain-128A security services for air interface communications*
- *Part 14: Crypto suite AES OFB security services for air interface communications*
- *Part 16: Crypto suite ECDSA-ECDH security services for air interface communications*
- *Part 17: Crypto suite cryptoGPS security services for air interface communications*
- *Part 19: Crypto suite RAMON security services for air interface communications*
- *Part 20: Crypto suite Algebraic Eraser security services for air interface communications*

The following part is under preparation:

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

Introduction

This part of ISO/IEC 29167 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**

The latest information on IP that may be applicable to this part of ISO/IEC 29167 can be found at www.iso.org/patents.

Information technology — Automatic identification and data capture techniques —

Part 19:

Crypto suite RAMON security services for air interface communications

1 Scope

This part of ISO/IEC 29167 defines the Rabin-Montgomery (RAMON) crypto suite for the ISO/IEC 18000 air interfaces standards for radio frequency identification (RFID) devices. Its purpose is to provide a common crypto suite for security for RFID devices that may be referred by ISO committees for air interface standards and application standards.

This part of ISO/IEC 29167 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 part of ISO/IEC 29167 defines various authentication methods and methods of use for the cipher. A Tag and an Interrogator may support one, a subset, or all of the specified options, clearly stating what is supported.

2 Conformance

2.1 Claiming conformance

To claim conformance with this part of ISO/IEC 29167, an Interrogator or Tag shall comply with all relevant clauses of this part of ISO/IEC 29167, except those marked as “optional”.

2.2 Interrogator conformance and obligations

To conform to this part of ISO/IEC 29167, an Interrogator shall implement the mandatory commands defined in this part of ISO/IEC 29167, and conform to the relevant part of ISO/IEC 18000.

To conform to this part of ISO/IEC 29167, an Interrogator may implement any subset of the optional commands defined in this part of ISO/IEC 29167.

To conform to this part of ISO/IEC 29167, the Interrogator shall not

- implement any command that conflicts with this part of ISO/IEC 29167, or
- require the use of an optional, proprietary, or custom command to meet the requirements of this part of ISO/IEC 29167.

2.3 Tag conformance and obligations

To conform to this part of ISO/IEC 29167, a Tag shall implement the mandatory commands defined in this part of ISO/IEC 29167 for the supported types, and conform to the relevant part of ISO/IEC 18000.

To conform to this part of ISO/IEC 29167, a Tag may implement any subset of the optional commands defined in this part of ISO/IEC 29167.

To conform to this part of ISO/IEC 29167, a Tag shall not

- implement any command that conflicts with this part of ISO/IEC 29167, or
- require the use of an optional, proprietary, or custom command to meet the requirements of this part of ISO/IEC 29167.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18000-3, *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, *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*

ISO/IEC 29167-1, *Information technology — Automatic identification and data capture techniques — Part 1: Security services for RFID air interfaces*

4 Terms and definitions

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

4.1

authentication

service that is used to establish the origin of information

4.2

confidentiality

property whereby information is not disclosed to unauthorized parties

4.3

integrity

property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored

4.4

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

4.5

secure communication

communication between the tag and the interrogator by use of the *Authenticate* command, assuring authenticity, integrity and confidentiality of exchanged messages