

FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/IEC
FDIS
29167-19

ISO/IEC JTC 1/SC 31

Secretariat: ANSI

Voting begins on:
2015-10-07

Voting terminates on:
2015-12-07

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 capture data

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

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.



Reference number
ISO/IEC FDIS 29167-19:2015(E)

© ISO/IEC 2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/a7d0c5d7-2ed4-4d54-a245-9d927dbe0a57/iso-iec-29167-19-2016>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, 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.....	12
7 Parameter definitions	13
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.....	16
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	59
Annex E	(normative) Protocol specific	62
Annex F	(informative) Non-traceable and integrity-protected Tag identification	69
Annex G	(informative) Memory Organization for Secure UHF Tags (Proposal)	72
Bibliography	76

iTeh STANDARD PREVIEW
 (standards.iteh.ai)
 Full standard:
<https://standards.iteh.ai/catalog/standards/sist/a7d0c5d7-2ed4-4d54-a245-9d927dbe0a57/iso-iec-29167-19-2016>

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/a7d0c5d7-2ed4-4d54-a245-9d927dbe0a57/iso-iec-29167-19-2016>

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

5 Symbols and abbreviated terms

5.1 Symbols

xx ₂	binary notation
xx _h	hexadecimal notation
	concatenation of syntax elements in the order written

5.2 Abbreviated terms

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CH	Challenge
CH _{I1} , CH _{I2}	Interrogator random challenge, 16 bytes
CH _T	Tag random challenge, 16 bytes
CG	Cryptogram
CMAC	Ciphered Message Authentication Code
CRC	Cyclic Redundancy Check
CRC-16	16-bit CRC
CS	Crypto Suite
CSI	Crypto Suite Identifier
DEC(key, data)	AES decryption of enciphered “data” with secret “key”
ENC(key, data)	AES encryption of plain “data” with secret “key”
EPC™	Electronic Product Code
IID	Interrogator Identifier, 8 bytes
IV	Initialization Vector for CBC-encryption, 16 bytes
KDF	Key Derivation Function
K _E	Public key for encryption stored on Tag
K _D	Private decryption key stored on Interrogator
K _V	Public signature verification key stored on Interrogator
K _S	Private signature generation key stored in the tag issuer facility
K _{ENC}	Shared secret message encryption key
K _{MAC}	Shared secret message authentication key
KESel	Key select (determines which KE will be used)
KSel	Key select (determines which pair of KENC, KMAC will be used)

MAC(key, data)	Calculation of a MAC of (enciphered) “data” with secret “key”; internal state of the tag’s state machine
MAM _{x,y}	Mutual Authentication Method x.y
MCV	MAC Chaining Value
MIX(CH, RN, SID)	RAMON mix function
PRF	Pseudorandom Function
<i>R</i>	Tag response
RAMON	Rabin-Montgomery
RFU	Reserved for Future Use
RM_ENC(key, data)	RAMON encryption of plain “data” with public “key”
RM_DEC(key, data)	RAMON decryption of enciphered “data” with private “key”
RN	Random Number
RNT	Tag Random Number, 16 bytes
<i>S_{ENC}</i>	Message encryption session key
<i>S_{MAC}</i>	Message authentication session key
SID	Secret Identifier, 8 bytes, identifying the tag
SSC	Send Sequence Counter for replay protection, 16 bytes
TAM _{x,y}	Tag Authentication Method x.y; internal state of the tag’s state machine
TLV	Tag Length Value
UHF	Ultra High Frequency
UII	Unique Item Identifier
WORM	Write once, read many

5.3 Notation

This crypto suite uses the notation of ISO/IEC 18000-63.

The following notation for key derivation corresponds to Reference [7] and [Clause 5](#).

<i>PRF(s,x)</i>	A pseudo-random function with seed <i>s</i> and input data <i>x</i> .
<i>K_I</i>	Key derivation key used as input to the KDF to derive keying material. <i>K_I</i> is used as the block cipher key, and the other input data are used as the message defined in Reference [5].
<i>K_O</i>	Keying material output from a key derivation function, a binary string of the required length, which is derived using a key derivation key.
<i>Label</i>	A string that identifies the purpose for the derived keying material, which is encoded as a binary string.

<i>Context</i>	A binary string containing the information related to the derived keying material. It may include identities of parties who are deriving and/or using the derived keying material and, optionally, a nonce known by the parties who derive the keys.
<i>L</i>	An integer specifying the length (in bits) of the derived keying material K_0 . L is represented as a binary string when it is an input to a key derivation function. The length of the binary string is specified by the encoding method for the input data.
<i>h</i>	An integer that indicates the length (in bits) of the output of the PRF.
<i>i</i>	A counter that is input to each iteration of the PRF.
<i>r</i>	An integer, smaller or equal to 32, that indicates the length of the binary representation of the counter i , in bits.
<i>00h</i>	An all zero octet. An optional data field used to indicate a separation of different variable length data fields.
$\lceil X \rceil$	The smallest integer that is larger than or equal to X . The ceiling of X .
$\{X\}$	Indicates that data X is an optional input to the key derivation function.
$[T]_2$	An integer T represented as a binary string (denoted by the "2") with a length specified by the function, an algorithm, or a protocol which uses T as an input.
\emptyset	The empty binary string.

6 Crypto suite introduction

6.1 Overview

The RAMON Crypto Suite permits two levels of implementation. The first level provides secure identification and tag authentication, while the second level extends the functionality by mutual authentication to securely communicate between Interrogator and Tag, e.g. for secure reading and writing non-volatile memory.

Basic RAMON Tags may provide only the first level of implementation, while more sophisticated Tags also provide the second level. See [Figure 1](#) for the different implementation levels for the RAMON crypto suite.

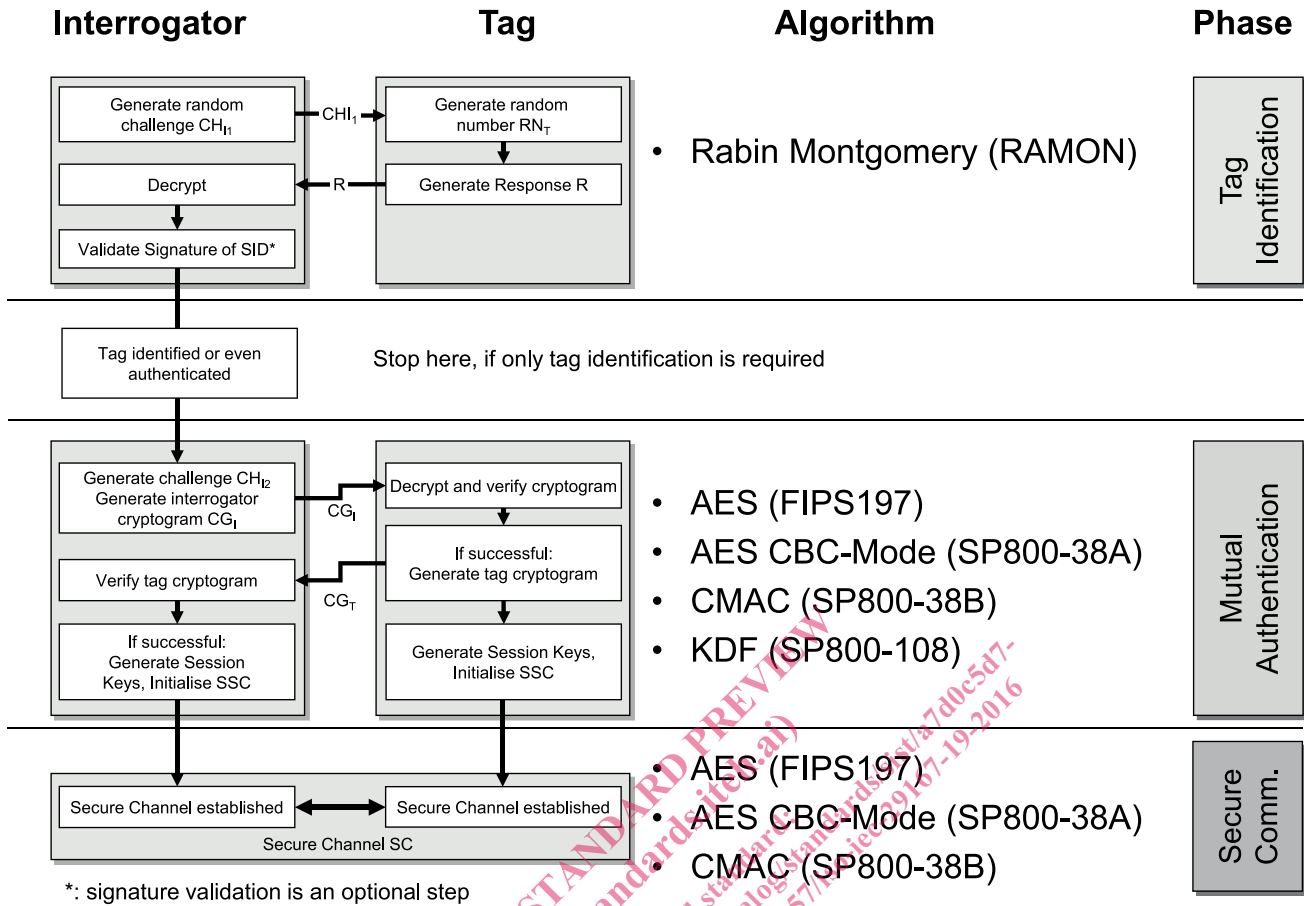


Figure 1 — Overview of the different implementation levels for the RAMON crypto suite

6.2 Authentication protocols

6.2.1 Tag Identification

The Rabin-Montgomery crypto suite provides non-traceable and confidential Tag identification. Confidentiality and privacy for the Tag’s identifier are provided without requiring the Tag to store a private key.

The crypto suite is based on the asymmetric cryptosystem developed by Michael O. Rabin[3]. The original algorithm is augmented by a method detected by Peter Montgomery[2], which avoids the division of long numbers in modular arithmetic. Combining Rabin encryption with the concept of Montgomery multiplication advantage is taken of the fact that no “costly” division is required.

The Tag performs only public key operations. The Interrogator performs the “expensive” private key operation. The steps necessary to carry out RAMON are outlined in Table 1. RAMON encryption performed by the Tag and decryption performed by the Interrogator are specified in C.3 and C.4. The cryptographic keys are specified in 6.6.

This specification also includes in C.1 the structure of the clear text record used for authentication of the Tag, comprising the Tag identity record and random data originating in part from the Tag and from the Interrogator for the other part.

Table 1 — Protocol steps for Tag identification

Interrogator (K_D, K_V)		Tag (SID, K_E)
a) Generate random challenge CH_{I1} and send it to the Tag. b) Decrypt Tag response and apply the inverse of the MIX function to get the plaintext P : $P = \text{MIX}^{-1}[\text{RM_DEC}(K_D, R)].$ c) Obtain CH_{I1} , RN_T and SID from plaintext P . d) Compare previously generated Interrogator challenge with the value received from Tag. If successful, Tag is identified. e) If a signature is provided along with the SID , use K_V to validate the signature. If successful, Tag is authenticated.	(CH_{I1}) \rightarrow (R) \leftarrow	a) Generate random number RN_T . b) Generate response cryptogram: $R = \text{RM_ENC}[K_E, \text{MIX}(CH_{I1}, RN_T, \text{TLV record})]$.

6.2.2 Symmetric mutual authentication

This crypto suite allows combining the Rabin-Montgomery scheme for Tag identification with symmetric mutual authentication. The mutual authentication specified by this crypto suite is based on AES, according to Reference [8]. The CBC mode for encryption is specified in Reference [4]. For MAC generation CMAC according to Reference [5] is used. For derivation of secure messaging keys, the KDF in counter mode specified in 5.1 of Reference [7] is used.

The protocol steps for mutual authentication are outlined in [Table 2](#).

Table 2 — Protocol steps for mutual authentication

Phase	Interrogator ($IID, \text{Database}, K_D, K_V$)		Tag ($SID, K_E, K_{ENC}, K_{MAC}$)
a) Tag Identification	a) Generate random challenge CH_{I1} and send it to the Tag. b) Decrypt Tag response and apply the inverse of the MIX function to get the plaintext P : $P = \text{MIX}^{-1}[\text{RM_DEC}(K_D, R)].$ c) Obtain CH_{I1} , RN_T and SID from plaintext P . d) Compare previously generated Interrogator challenge with the value received from Tag. If successful, Tag is identified. e) If a signature is provided along with the SID , use K_V to validate the signature. If successful, Tag is authenticated. f) Set $CH_T = RN_T$.	(CH_{I1}) \rightarrow (R) \leftarrow	a) Generate random number RN_T . b) Generate response: $R = \text{RM_ENC}[K_E, \text{MIX}(CH_{I1}, RN_T, \text{TLV record, '00' byte})]$.
The Interrogator has successfully identified (and authenticated) the Tag.			
In the following phase, CH_T and SID are used in the mutual authentication.			