INTERNATIONAL STANDARD

ISO/IEC 29167-10

Second edition
2017-09

Information technology — Automatic identification and data capture techniques —

Part 10: Crypto suite AES-128 security services for air interface communications

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

Partie 10: Services de sécurité par suite cryptographique AES-128 pour communications par interface radio

Reference number
ISO/IEC 29167-10:2017(E)

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms, definitions, symbols and abbreviated terms 1

4 Conformance 6

4.1 Air interface protocol specific information 6

4.2 Interrogator conformance and obligations 6

4.3 Tag conformance and obligations 6

5 Introduction of the AES-128 crypto suite 6

6 Parameter definitions 7

7 Crypto suite state diagram 8

8 Initialization and resetting 9

9 Authentication 9

9.1 General 9

9.2 Adding custom data to authentication process 10

9.3 Message and response formatting 12

9.4 Tag authentication (Method “00” = TAM) 13

9.4.1 General 13

9.4.2 TAM1 Message 13

9.4.3 TAM1 Response 14

9.4.4 Final Interrogator processing TAM1 14

9.4.5 TAM2 Message 14

9.4.6 TAM2 Response 16

9.4.7 Final Interrogator processing TAM2 20

9.5 Interrogator authentication (Method “01” = IAM) 21

9.5.1 General 21

9.5.2 IAM1 Message 21

9.5.3 IAM1 Response 22

9.5.4 Final Interrogator processing IAM1 22

9.5.5 IAM2 Message 22

9.5.6 IAM2 Response 23

9.5.7 Final Interrogator processing IAM2 23

9.5.8 IAM3 Message 23

9.5.9 IAM3 Response 28

9.5.10 Final Interrogator processing IAM3 29

9.6 Mutual authentication (Method “10” = MAM) 29

9.6.1 General 29

9.6.2 MAM1 Message 29

9.6.3 MAM1 Response 30

9.6.4 Final Interrogator processing MAM1 30

9.6.5 MAM2 Message 30

9.6.6 MAM2 Response 31

9.6.7 Final Interrogator processing MAM2 31

10 Communication 31

11 Key Table and KeyUpdate 31

Annex A (normative) **Crypto suite state transition table** 34

Annex B (normative) **Error conditions and error handling** 35

Annex C (normative) **Cipher description** 36
Annex D (informative) **Test vectors** 40
Annex E (normative) **Protocol specific information** 41
Annex F (informative) **Examples** 49
Bibliography 58

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*.

This second edition cancels and replaces the first edition (ISO/IEC 29167-10:2015), which has been technically revised.

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

Introduction

This document specifies the security services of an AES-128 crypto suite. AES has a fixed block size of 128 bits and a key size of 128 bits, 192 bits or 256 bits. This document uses AES with a fixed key size of 128 bits and is referred to as AES-128.

This document specifies procedures for the authentication of a Tag and or an Interrogator using AES-128 and provides the following features:

— Tag Authentication;

— Tag Authentication allows authenticated and encrypted reading of a part of the Tag's memory;

— Interrogator Authentication;

— Interrogator Authentication allows authenticated and encrypted writing of a part of the Tag's memory;

— Mutual Authentication.

Crypto suite only supports encryption on the Tag and uses encryption for "encrypting" messages sent from the Tag to the Interrogator and "decrypting" messages received from the Interrogator.

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 might 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 ISO and IEC that they are willing to negotiate licenses 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:

Impinj, Inc.
Chris Dorio **Chief Strategy and Technology Officer**

The latest information on IP that might be applicable to this document can be found at www.iso.org/patents.

Information technology — Automatic identification and data capture techniques —

Part 10: Crypto suite AES-128 security services for air interface communications

1 Scope

This document specifies the crypto suite for AES-128 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 might be referred by ISO committees for air interface standards and application standards.

This document specifies a crypto suite for AES-128 for an air interface for RFID systems. The crypto suite is defined in alignment with existing air interfaces.

This document specifies various authentication methods and methods of use for the encryption algorithm. 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 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

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, *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*

3 Terms, definitions, symbols and abbreviated terms

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 http://www.iso.org/obp

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

3.1 Terms and definitions

3.1.1
AES-CMAC-96 (key, data)
CMAC generation with input data "data", using initialization vector "IV" and 128-bit key "key", truncating the result by using only the 96 most significant bits from the 128-bit CMAC code

3.1.2
AES-DEC (key, data)
AES in ECB decryption mode of input data "data" and 128-bit key "key"

3.1.3
AES-ENC (key, data)
AES in ECB encryption mode of input data "data" and 128-bit key "key"

3.1.4
AuthenticationBlock
variable that contains information to verify the authenticity of the Tag or the Interrogator

3.1.5
bit string
ordered sequence of 0s and 1s

3.1.6
block cipher
family of functions and their inverse functions that is parameterized by keys

Note 1 to entry: The functions map bit strings of a fixed length to bit strings of the same length.

3.1.7
blocksize
number of bits in an input (or output) block of the block cipher

3.1.8
CBC_{ENC}_AES (IV, key, data)
AES in CBC encryption mode of input data "data", using initialization vector "IV" and 128-bit key "key", according to NIST/SP 800-38A

Note 1 to entry: Output blocks (O_i) are obtained from input blocks (I_i) as follows:

— O_1 = AES-ENC(key, I_1 XOR IV), and

— O_n = AES-ENC(key, I_n XOR $O_{(n-1)}$).

Note 2 to entry: C.2 describes the cipher block chaining.

3.1.9
CBC_{DEC}_AES_{INV} (IV, key, data)
AES in CBC decryption mode of input data "data", using initialization vector "IV" and 128-bit key "key", according to NIST/SP 800-38A

Note 1 to entry: Output blocks (O_i) are obtained from input blocks (I_i) as follows:

— O_1 = AES-DEC(key, I_1) XOR IV, and

— O_n = AES-DEC(key, I_n) XOR $I_{(n-1)}$).

3.1.10
CBC_{ENC}_AES_{INV} (IV, key, data)
CBC in encryption mode using initialization vector "IV" and 128-bit key "key"

Note 1 to entry: Output blocks (O_i) are obtained from input blocks (I_i) as follows:

— O_1 = AES-DEC(key, I_1 XOR IV), and

— O_n = AES-DEC(key, I_n XOR $O_{(n-1)}$).

3.1.11
CBC_{DEC}_AES (IV, key, data)
CBC in decryption mode using initialization vector "IV" and 128-bit key "key"

Note 1 to entry: Output blocks (O_i) are obtained from input blocks (I_i) as follows:

— O_1 = AES-ENC(key, I_1) XOR IV, and

— O_n = AES-ENC(key, I_n) XOR $I_{(n-1)}$)

3.1.12
ciphertext
encrypted plaintext

3.1.13
cipher-based message authentication code
CMAC
algorithm based on a symmetric key block cipher

Note 1 to entry: In this document, data is systematically padded with zero bits before computing the MAC, resulting in the last block of MAC inputs is always complete. Therefore, K1-MAC is always used. It makes the computation of K2-MAC useless.

Note 2 to entry: The computation of the MAC shall comply with the requirements of MAC method 5 in ISO/IEC 9797-1.

3.1.14
Command (Message)
data that the Interrogator sends to a Tag with "Message" as parameter

3.1.15
D
number of 128-bit blocks that can be added to the authentication response as custom data and header

3.1.16
data block
block
sequence of bits whose length is the block size of the block cipher

3.1.17
ENC_key
variable that contains the key that will be used for cryptographic confidentiality protection

Note 1 to entry: This variable shall be used for cryptographic confidentiality protection.

3.1.18
H
number of bits of the header

3.1.19
Header
H bits composed of BlockSize, Offset, Profile and BlockCount

3.1.20
Initialization Vector
IV
input block that some modes of operation require as an additional initial input

3.1.21
input block
data that is an input to either the forward cipher function or the inverse cipher function of the block cipher algorithm

3.1.22
Key
string of bits used by a cryptographic algorithm to transform plaintext into ciphertext or vice versa or to produce a message authentication code

3.1.23
KeyID
numerical designator for a single key

3.1.24
Key[KeyID].ENC_key
variable that contains the key that will be used for encryption

Note 1 to entry: This variable shall be used for encryption.

3.1.25
Key[KeyID].MAC_key
key that can be used for cryptographic integrity protection

3.1.26
MAC_key
variable that contains the key that will be used for cryptographic integrity protection

Note 1 to entry: This variable shall be used for cryptographic integrity protection.

3.1.27
Memory Profile
start pointer within the Tag's memory for addressing custom data block

3.1.28
Message
part of the command that is defined by the crypto suite

3.1.29
Mode of Operation
Mode
algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm

3.1.30
output block
data that is an output of either the forward cipher function or the inverse cipher function of the block cipher algorithm

3.1.31
Plaintext
ordinary readable text before being encrypted into ciphertext or after being decrypted from ciphertext

3.1.32
Reply (Response)
data that the Tag returns to the Interrogator with "Response" as parameter

3.1.33
Response
part of the reply (stored or sent) that is defined by the crypto suite

3.1.34
word
bit string comprised of 16 bits

3.2 Symbols and abbreviated terms

AES Advanced Encryption Standard

CBC Cipher Block Chaining

CMAC Cipher-based Message Authentication Code

DIV integral part of a division

Field[a:b] selection from a string of bits in Field

For a > b, selection of a string of bits from the bit string Field. Selection ranges from bit number a until and including bit number b from the bits of the string in Field, whereby Field[0] represents the least significant bit. For selecting one single bit from Field a=b.

For example, Field[2:0] represents the selection of the three least significant bits of Field.

FIPS Federal Information Processing Standard

IV Initialization Vector

LSB Least Significant Byte

MAC Message Authentication Code

MPI Memory Profile Indicator

MSB Most Significant Byte

NIST National Institute of Standards and Technology (United States)

RFU Reserved for Future Use

TID Tag-IDentification or Tag IDentifier (depending on context)

UII Unique Identification ID

$xxxx_b$ binary notation of term "xxxx", where "x" represents a binary digit

$xxxx_h$ hexadecimal notation of term "xxxx", where "x" represents a hexadecimal digit

In this crypto suite, the bytes in the hexadecimal numbers are presented with the most significant byte at the left and the least significant byte at the right. The bit order per byte is also presented with the most significant bit at the left and the least significant bit at the right.

For example, in "ABCDEF" the byte "AB" is the most significant byte and the byte "EF" is the least significant byte.

|| concatenation of syntax elements, transmitted in the order written (from left to right)

For example, "123456" || "ABCDEF" results in "123456ABCDEF", where the byte "12" is the most significant byte and the byte "EF" is the least significant byte.

Note 1 to entry This protocol uses the following notational conventions:

— States and flags are denoted in bold. Some command parameters are also flags; a command parameter used as a flag will be bold. Example: **ready**.

— Command parameters are underlined. Some flags are also command parameters; a flag used as a command parameter will be underlined. Example: <u>Pointer</u>.

— Commands are denoted in italics. Variables are also denoted in italics. Where there might be confusion between commands and variables, this protocol will make an explicit statement. Example: *Query*.

4 Conformance

4.1 Air interface protocol specific information

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 can 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 can 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 Introduction of the AES-128 crypto suite

The Advanced Encryption Standard (AES) is an open, royalty-free, symmetric block cipher based on so-called substitution-permutation networks. AES is highly suitable for efficient implementation in both software and hardware, including extremely constrained environments such as RFID Tags. The AES cipher is standardized as ISO/IEC 18033-3.

AES is approved by the National Institute of Standards and Technology (NIST). It was approved as a standard in 2001 following a 5-year standardization process that involved a number of competing encryption algorithms and published as FIPS PUB 197 in November 2001.

AES was published, along with design criteria and test vectors, in Reference [2].

NOTE AES normally uses encryption to encrypt plaintext and decryption to decrypt ciphertext. This crypto suite uses encryption both to encrypt plaintext as well as to decrypt ciphertext. This allows the use of an encryption-only implementation on the Tag.

References for AES test vectors are provided in Annex D.

Annex F provides examples for the implementation of the functionality that is specified in this document.

6 Parameter definitions

Table 1 describes all the parameters that are used in this document.

Table 1 — Definition of AES-128 crypto suite parameters

Parameter	Description
AuthenticationBlock	Parameter used in IResponse of IAM3 Message with the parameters: AES-DEC(Key[KeyID].*ENC_key*, *C_IAM3*[11:0] || *Purpose_IAM3*[3:0] || *IRnd_IAM3*[31:0] || *TChallenge_IAM1*[79:0]) This parameter is only introduced to make the content of the IResponse of IAM3 Message easier to read.
C_MAM1[15:0]	16-bit predefined constant for MAM1 with the value "DA83$_h$" (for Tag to Interrogator response)
C_MAM2[11:0]	12-bit predefined constant for MAM2 with the value "DA8$_h$" (for Tag to Interrogator response)
C_TAM1[15:0]	16-bit predefined constant for TAM1 with the value "96C5$_h$" (for Tag to Interrogator response)
C_TAM2[15:0]	16-bit predefined constant for TAM2 with the value "96C5$_h$" (for Tag to Interrogator response)
C_TAM2_0[15:0]	16-bit predefined constant for TAM2 with the value "96C0$_h$" (for Tag to Interrogator response)
C_TAM2_1[15:0]	16-bit predefined constant for TAM2 with the value "96C1$_h$" (for Tag to Interrogator response)
C_TAM2_2[15:0]	16-bit predefined constant for TAM2 with the value "96C2$_h$" (for Tag to Interrogator response)
C_TAM2_3[15:0]	16-bit predefined constant for TAM2 with the value "96C3$_h$" (for Tag to Interrogator response)
C_IAM2[11:0]	12-bit predefined constant for IAM2 with the value "DA8$_h$" (for Interrogator to Tag response)
C_IAM3_0[11:0]	12-bit predefined constant for IAM3 with the value "DA8$_h$" (for Interrogator to Tag response)
C_IAM3_1[11:0]	12-bit predefined constant for IAM3 with the value "DA9$_h$" (for Interrogator to Tag response)
C_IAM3_2[11:0]	12-bit predefined constant for IAM3 with the value "DAA$_h$" (for Interrogator to Tag response)
C_IAM3_3[11:0]	12-bit predefined constant for IAM3 with the value "DAB$_h$" (for Interrogator to Tag response)
CUSTOMDATA(D*128-*H*)	Part of the Tag's memory that may be included in the authentication process
HEADER(*H*)	Header of *H* bits preceding the custom data
IChallenge_MAM1[79:0]	80-bit challenge generated by the Interrogator for use in MAM1
IChallenge_TAM1[79:0]	80-bit challenge generated by the Interrogator for use in TAM1
IChallenge_TAM2[79:0]	80-bit challenge generated by the Interrogator for use in TAM2

Table 1 *(continued)*

Parameter	Description
IRnd_IAM2[31:0]	32-bit random data generated by the Interrogator for use in IAM2
IRnd_IAM3[31:0]	32-bit random data generated by the Interrogator for use in IAM3
Key[KeyID]	Keyset identified by KeyID, consisting of *ENC_key* for encryption and (optional) *MAC_key* for integrity protection
MAC_key[127:0]	Variable that shall contain the key that will be used for cryptographic integrity protection
Purpose_IAM2[3:0]	Authentication purpose bits for IAM2 If *Purpose_IAM2*[3:3] = 0_b the bits [2:0] are RFU with value 000_b If *Purpose_IAM2*[3:3] = 1_b the bits [2:0] are manufacturer defined
Purpose_IAM3[3:0]	Authentication purpose bits for IAM3 If *Purpose_IAM3*[3:3] = 0_b the bits [2:0] are RFU with value 000_b If *Purpose_IAM3*[3:3] = 1_b the bits [2:0] are manufacturer defined
Purpose_MAM2[3:0]	Authentication purpose bits for MAM2 If *Purpose_MAM2*[3:3] = 0_b the bits [2:0] are RFU with value 000_b If *Purpose_MAM2*[3:3] = 1_b the bits [2:0] are manufacturer defined
TChallenge_IAM1[79:0]	80-bit challenge that the Tag generates for use in IAM1
TChallenge_MAM1[79:0]	80-bit challenge that the Tag generates for use in MAM1
TRnd_TAM1[31:0]	32-bit random data provided by the Tag for TAM1
TRnd_TAM2[31:0]	32-bit random data provided by the Tag for TAM2

7 Crypto suite state diagram

The transitions between the crypto suite states are specified in Figure 1.

The Tag shall transition from the Start State to the Next State conforming to the requirements specified in Annex A.