International Standard

ISO/IEC 29167-10

Third edition
2026-03

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 29167-10:2026(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

This third edition cancels and replaces the second edition (ISO/IEC 29167-10:2017), which has been technically revised.

The main change is as follows: requirements in Clause E.4 have been updated to reflect changes to the corresponding over-the-air protocol.

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

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 and www.iec.ch/national-committees.

Introduction

This document provides a common crypto suite for security for radio frequency identification (RFID) devices. The crypto suite is defined in alignment with existing air interfaces and specifies a variety of security services provided by the symmetric block cipher AES-128.

A crypto suite only supports the encryption on the Tag and use the encryption for “encrypting” messages sent from the Tag to the Interrogator and “decrypting” messages received from the Interrogator.

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 interface standards for radio frequency identification (RFID) devices.

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 allowing authenticated and encrypted reading of part of the Tag's memory;
- Interrogator authentication;
- Interrogator authentication allowing authenticated and encrypted writing of part of the Tag's memory;
- Mutual authentication.

In this document, 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 18000-3:2010, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 930 MHz Type C*

ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Vocabulary*

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

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 terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1 Terms and definitions

3.1.1
AES-CMAC-96 (key, data)
cipher-based message authentication code (CMAC) (3.1.13) generation with input data "data", using *initialization vector* (3.1.20) "IV" and 128-bit *key* (3.1.21) "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)
advanced encryption standard in Electronic Codebook decryption mode of input data "data" and 128-bit *key* (3.1.21) "key"

3.1.3
AES-ENC (key, data)
advanced encryption standard in Electronic Codebook encryption mode of input data "data" and 128-bit *key* (3.1.21) "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* (3.1.21)

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* (3.1.6)

3.1.8
$\mathbf{CBC_{ENC}}$_AES (IV, key, data)
advanced encryption standard in cipher block chaining encryption mode of input data "data", using *initialization vector* (3.1.20) "IV" and 128-bit *key* (3.1.21) "key", according to NIST/SP 800-38A[9]

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: Clause C.2 describes cipher block chaining.

3.1.9
CBC$_{DEC}$–AES$_{INV}$ (IV, key, data)
advanced encryption standard in cipher block chaining decryption mode of input data "data", using *initialization vector* (3.1.20) "IV" and 128-bit *key* (3.1.21) "key", according to NIST/SP 800-38A[9]

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)
cipher block chaining in encryption mode using *initialization vector* (3.1.20) "IV" and 128-bit *key* (3.1.21) "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)
cipher block chaining in decryption mode using *initialization vector* (3.1.20) "IV" and 128-bit *key* (3.1.21) "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* (3.1.30)

3.1.13
cipher-based message authentication code
CMAC
algorithm based on a symmetric *key* (3.1.21)*block cipher* (3.1.6)

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 conform 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* (3.1.32) as custom data and *header* (3.1.19)

3.1.16
data block
block
sequence of bits whose length is the block size of the *block cipher* (3.1.6)

3.1.17
ENC_key
variable that contains the *key* (3.1.21) that is 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)

3.1.19
header
H bits composed of *BlockSize* (3.1.7), Offset, Profile and BlockCount

3.1.20
initialization vector
IV
input block that some *modes of operation* (3.1.28) require as an additional initial input

3.1.21
key
string of bits used by a cryptographic algorithm to transform *plaintext* (3.1.30) into *ciphertext* (3.1.12) or vice versa or to produce a *message* (3.1.21) authentication code

3.1.22
KeyID
numerical designator for a single *key* (3.1.21)

3.1.23
Key[KeyID].ENC_key
variable that contains the *key* (3.1.21) that is used for encryption

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

3.1.24
Key[KeyID].MAC_key
key (3.1.21) that can be used for cryptographic integrity protection

3.1.25
MAC_key
variable that contains the *key* (3.1.21) that is used for cryptographic integrity protection

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

3.1.26
memory profile
start pointer within the Tag's memory for addressing custom *data block* (3.1.16)

3.1.27
message
part of the command that is defined by the crypto suite

3.1.28
mode of operation
mode
algorithm for the cryptographic transformation of data that features a symmetric *key* (3.1.21) block cipher algorithm

3.1.29
output block
data that is an output of either the forward cipher function or the inverse cipher function of the block cipher algorithm

3.1.30
plaintext
ordinary readable text before being encrypted into *ciphertext* (3.1.12) or after being decrypted from ciphertext

3.1.31
reply
data that the Tag returns to the Interrogator with "Response" as parameter

3.1.32
response
part of the reply (stored or sent) that is defined by the crypto suite

3.1.33
word
bit string (3.1.5) comprised of 16 bits

3.2 Symbols

Field[a:b] selection of bits "a" through to, and including, bit "b" from a string of bits denoted Field where Field [0] represents the least significant or rightmost bit

EXAMPLE 1 Field [2:0] represents the selection of the three least significant bits of Field.

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

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

NOTE 2 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.

EXAMPLE 2 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)

EXAMPLE 3 "123456" || "ABCDEF" results in "123456ABCDEF", where the byte "12" is the most significant byte and the byte "EF" is the least significant byte.

NOTE 3 This document 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 formatted in bold (e.g. **ready**).
- Command parameters are underlined. Some flags are also command parameters; a flag used as a command parameter will be underlined (e.g. Pointer).
- Commands are denoted in italics. Variables are also denoted in italics. Where there can be confusion between commands and variables, this protocol will make an explicit statement (e.g. *Query*).

3.3 Abbreviated terms

AES	advanced encryption standard
CBC	cipher block chaining
CMAC	cipher-based message authentication code
CSI	crypto suite identifier
DIV	integral part of a division
FIPS	federal information processing standard

IAM	Interrogator authentication
IV	initialization vector
LSB	least significant byte
MAC	message authentication code
MAM	mutual authentication
MPI	memory profile indicator
MSB	most significant byte
NIST	national institute of standards and technology
RFU	reserved for future use
TA	Tag authentication
TID	Tag-IDentification or Tag IDentifier (depending on context)
UII	unique identification ID

4 Conformance

4.1 Air interface protocol specific information

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

The implementation of this crypto suite shall conform to the protocol specific information provided in Annex E.

4.2 Interrogator conformance and obligations

An Interrogator shall implement the mandatory commands described in this document and conform to the relevant part of the ISO/IEC 18000 series.

An Interrogator can implement any subset of the optional commands described 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 described in this document for the supported types and conform to the relevant part of the ISO/IEC 18000 series.

A Tag can implement any subset of the optional commands described 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.

5 Overview of the AES-128 crypto suite

The 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 [8].

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.

The implementation of this crypto suite shall conform to the algorithm-specific information provided in Annex C.

References for AES test vectors are provided in Annex D.

The implementation of this crypto suite shall conform to the protocol -specific information provided in Annex E.

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

6 Parameter description

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

Table 1 — 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)

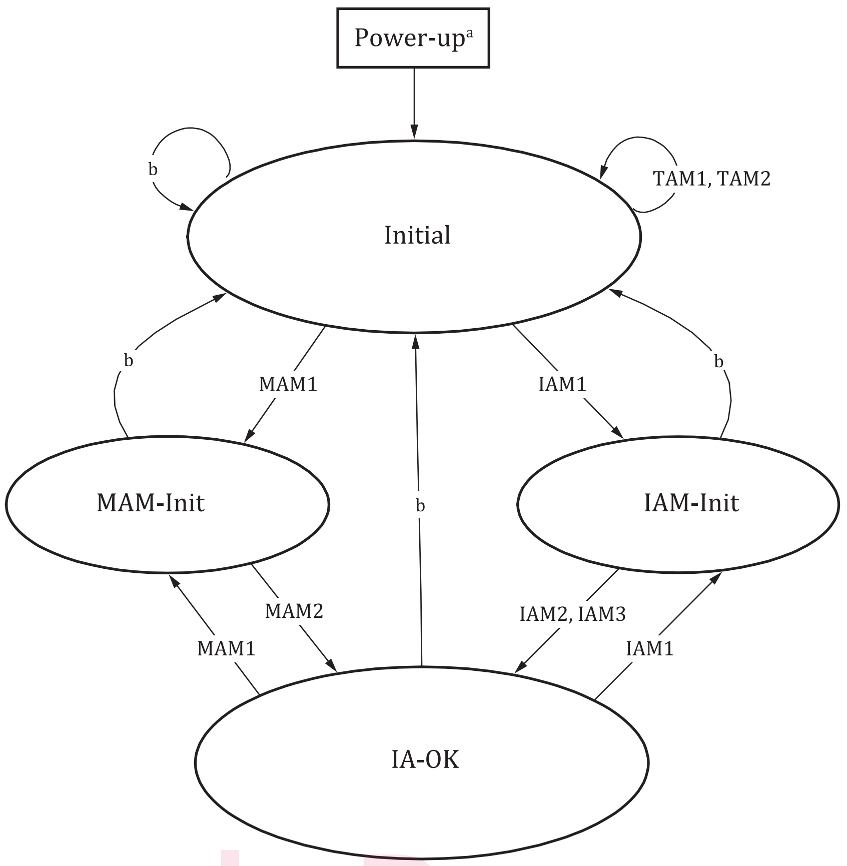
Table 1 *(continued)*

Parameter	Description
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
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 is 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.



[a] All variable fields will be reset at power-up.

[b] All errors result in a transition to **Initial** state.

Figure 1 — Crypto suite Tag state diagram

The Interrogator is considered authenticated only in the **IA-OK state**.

8 Initialization and resetting

After power-up and after a reset, the crypto suite shall transition into the **Initial** state.

After the Tag encounters an error condition, it shall transition into the **Initial** state.

After the Tag encounters an error condition, it may send an error reply to the Interrogator, but in that case the Tag shall select one error condition from the list that is specified in Annex B.

A transition to **Initial** state shall also cause a reset of all variables used by the crypto suite.

Implementations of this crypto 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 supports Tag authentication, Interrogator authentication and Mutual authentication. All functions are implemented using a message-response exchange. This clause describes the details of the messages and responses that are exchanged between the Interrogator and Tag.