INTERNATIONAL STANDARD

ISO/IEC 29167-10

First edition
2015-05-15

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 29167-10:2015(E)

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

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*, SC 31, *Automatic identification and data capture techniques*.

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 communication*
- — *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*

The following parts are 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 an AES-128 crypto suite for Tag authentication. AES has a fixed block size of 128 bits and a key size of 128 bits, 192 bits, or 256 bits. The version specified in this crypto suite uses AES with a fixed key size of 128 bits and is referred to as AES-128.

This part of ISO/IEC 29167 defines procedures for Tag Authentication using AES-128 and provides the following functionality:

- Tag Authentication;
- Tag Authentication allows authenticated reading of a part of the Tag's memory;
- Authenticated reading might be in plain text, MAC protected, Encrypted, or Encrypted and MAC protected;
- Crypto suite uses encryption for enciphering of plain text, as well as deciphering of encrypted text.

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 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 can be obtained from:

Impinj, Inc.
701 N 34th Street, Suite 300
Seattle, WA 98103 USA

The latest information on IP that might 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 10: Crypto suite AES-128 security services for air interface communications

1 Scope

This part of ISO/IEC 29167 defines 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 part of ISO/IEC 29167 specifies a crypto suite for AES 128 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 can support one, a subset, or all of the specified options, clearly stating what is supported.

2 Conformance

2.1 Air interface protocol specific information

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 can

— 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 can

— 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 18000-63, *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
AES-CBC-ENC(IV, key, data)
AES data encryption (forward operation) in CBC mode of input data “data”, using initialization vector IV and 128 bit cryptographic key “key”

4.2
AES-ECB-ENC(key, data)
AES data encryption (forward operation) in ECB mode of input data “data”, using 128 bit cryptographic key “key”

4.3
AES-CMAC-96(key, data)
CMAC generation using AES in forward operation with 128 bit cryptographic key “key” of input data “data”, truncating the result by using only the 96 most significant bits from the 128-bit CMAC code

4.4
bit string
ordered sequence of 0’s and 1’s

4.5
block cipher
family of functions and their inverse functions that is parameterized by cryptographic keys; the functions map bit strings of a fixed length to bit strings of the same length

4.6
block size
number of bits in an input (or output) block of the block cipher

4.7
cryptographic key
string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa or to produce a message authentication code

4.8
CMAC
cipher-based MAC algorithm based on a symmetric key block cipher

Note 1 to entry: See MAC method 5 in Reference [1] for a normative reference.

4.9
Command (Message)
data that Interrogator sends to Tag with “Message” as parameter

4.10
D
number of additional 128-bit blocks with custom data that may be added to the Tag authentication response

4.11
Data Block (Block)
sequence of bits whose length is the block size of the block cipher

4.12
initialization vector
data block that some modes of operation require as an additional initial input

4.13
input block
data that is an input to either the forward cipher function or the inverse cipher function of the block cipher algorithm

4.14
Key
string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa or to produce a message authentication code

4.15
KeyID
numerical designator for a single key

4.16
Key[KeyID].ENC_key
key that shall be used for encryption

4.17
Key[KeyID].MAC_key
key that may be used for cryptographic integrity protection

4.18
MAC_key
Variable that shall contain the key that will be used for cryptographic integrity protection

4.19
Memory Profile
start pointer within the Tag’s memory for addressing custom data block

4.20
Message
part of the Command that is defined by the crypto suite

4.21
Mode of Operation (Mode)
algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm

4.22
output block
data that is an output of either the forward cipher function or the inverse cipher function of the block cipher algorithm

4.23
Plaintext
usable data that is formatted as input to a mode

4.24
Reply (Response)
data that Tag returns to the Interrogator with “Response” as parameter

4.25
Response
part of the Reply (stored or sent) that is defined by the crypto suite

4.26
word
bit string comprised of 16 bits

5 Symbols and abbreviated terms

5.1 Symbols

xxxxb binary notation of term “xxxx”, where “x” represents a binary digit.

xxxxh 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.

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

5.2 Abbreviated terms

AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CMAC	Cipher-based MAC
ECB	Electronic Code Book
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	(United States) National Institute of Standards and Technology
RFU	Reserved for Future Use
TID	Tag-IDentification or Tag IDentifier, depending on context
UII	Unique Identification ID

6 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.[2]

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

AES was originally published, along with design criteria and test vectors, in reference document [5] in the Bibliography.

NOTE AES normally uses encryption for the enciphering of plain text and decryption for the deciphering of encrypted text. This crypto suite uses encryption for enciphering of plain text as well as deciphering of encrypted text. This allows the use of an encryption-only implementation on the Tag.

7 Parameter definitions

Table 1 describes all the parameters that are used in this part of ISO/IEC 29167.

Table 1 — Definition of AES-128 crypto suite parameters

Parameter	Description
C_TAM1[15:0]	16-bit predefined constant for TAM1 with the value “96C5h” (for Tag to Interrogator response)
C_TAM2[15:0]	16-bit predefined constant for TAM2 with the value “96C5h” (for Tag to Interrogator response)
Ciphertext[n]	Temporary storage for encryption result
CUSTOMDATA(D*128)	Part of the Tag’s memory that may be returned with the Tag authentication response
IChallenge_TAM1[79:0]	80-bit challenge that the Interrogator generates for use in TAM1
IChallenge_TAM2[79:0]	80-bit challenge that the Interrogator generates for use in TAM2
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

Table 1 *(continued)*

Parameter	Description
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

8 Crypto suite state diagram

After power-up or reset the crypto suite transitions to its **Initial** state.

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

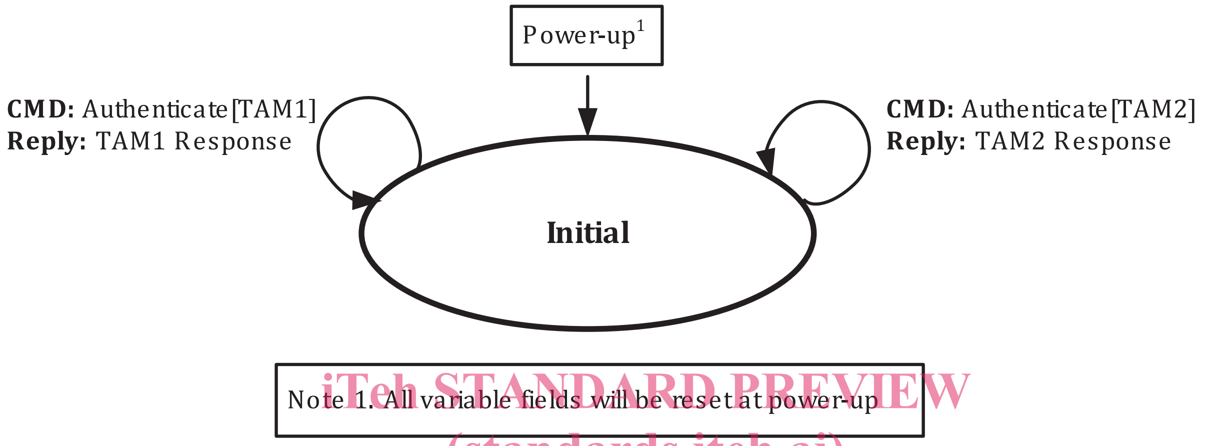

Figure 1 — Crypto suite Tag state diagram

9 Initialization and resetting

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

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.

10 Authentication

10.1 Introduction

This part of ISO/IEC 29167 supports only Tag Authentication. All functions are implemented using a message-response exchange. This section describes the details of the messages and responses that are exchanged between the Interrogator and Tag.

All message and response exchanges are listed in Table 2.

Table 2 — message and response functions

Command	Function
TAM1 message	Send Interrogator challenge and request Tag authentication response
TAM1 response	Return Tag authentication response
TAM2 message	Send Interrogator challenge and request Tag authentication response plus custom data
TAM2 response	Return Tag authentication response and custom data