INTERNATIONAL STANDARD

ISO/IEC 19823-10

Second edition
2020-01

Information technology — Conformance test methods for security service crypto suites —

Part 10: Crypto suite AES-128

Technologies de l'information — Méthodes d'essai de conformité pour les suites cryptographiques des services de sécurité —
Partie 10: Suite cryptographique AES-128

Reference number
ISO/IEC 19823-10:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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).

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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.

This document was prepared by Joint 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 19823-10:2017), which has been technically revised.

The main changes compared to the previous edition are as follows:

— In addition to Tag Authentication, this edition also defines support for Interrogator authentication and Mutual Authentication. This version describes the test methods for the additional functionality.

A list of all parts in the ISO/IEC 19823 series can be found on the ISO website.

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.

Introduction

The ISO/IEC 29167 series describes security services as applicable for the ISO/IEC 18000 series. The various parts of ISO/IEC 29167 describe crypto suites that are optional extensions to the ISO/IEC 18000 series air interfaces.

The ISO/IEC 19823 series describes the conformance test methods for security service crypto suites. It is related to the ISO/IEC 18047 series, which describes the radio frequency identification device conformance test methods, in the same way as the ISO/IEC 29167 series is related to the ISO/IEC 18000 series.

These relations mean that for a product that is claimed to conform to a pair of ISO/IEC 18000 and ISO/IEC 29167 documents, then the test methods of the ISO/IEC 18047 and ISO/IEC 19823 documents apply. If a product supports more than one part of ISO/IEC 18000 or ISO/IEC 29167, all related parts of ISO/IEC 18047 and ISO/IEC 19823 apply.

NOTE 1 The conformance test requirements of ISO/IEC 18000-6, ISO/IEC 18000-61, ISO/IEC 18000-62, ISO/IEC 18000-63, ISO/IEC 18000-64 are currently all in ISO/IEC 18047-6.

This document describes the test methods for the AES-128 crypto suite as standardized in ISO/IEC 29167-10.

NOTE 2 Test methods for interrogator and tag performance are covered by the ISO/IEC 18046 series.

Information technology — Conformance test methods for security service crypto suites —

Part 10: Crypto suite AES-128

1 Scope

This document describes test methods for determining the conformance of security crypto suites defined in ISO/IEC 29167-10.

This document contains conformance tests for all mandatory and applicable optional functions.

The conformance parameters are the following:

— parameters that apply directly affecting system functionality and inter-operability;

— protocol including commands and replies;

— nominal values and tolerances.

Unless otherwise specified, the tests in this document are intended to be applied exclusively to RFID Tags and Interrogators defined in the ISO/IEC 15693 series and in the ISO/IEC 18000 series using ISO/IEC 29167-10.

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 17025, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC/TR 18047-3:2011, *Information technology — Radio frequency identification device conformance test methods — Part 3: Test methods for air interface communications at 13,56 MHz*

ISO/IEC 18047-6:2017, *Information technology — Radio frequency identification device conformance test methods — Part 6: Test methods for air interface communications at 860 MHz to 960 MHz*

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

ISO/IEC 29167-10:2017, *Information technology — Automatic identification and data capture techniques — Part 10: Crypto suite AES-128 security services for air interface communications*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and ISO/IEC 29167-10 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

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

3.2 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 19762 apply.

4 Test methods

4.1 General

This clause describes the general test methods for ISO/IEC 29167-10. As the parts of ISO/IEC 19823 are always tested in relation with the ISO/IEC 18047 series, a duplication of information requirements and specifications should be avoided.

Clause 5 defines elements that are assumed to be covered in the respective part of the ISO/IEC 18047 series and, therefore, shall not be addressed in the ISO/IEC 19823 series. They may only be defined in the ISO/IEC 19823 series if ISO/IEC 18047 does not define them, although a revision of the respective part of the ISO/IEC 18047 series is the preferred option.

Clause 6 defines elements that are not expected to be covered by the ISO/IEC 18047 series and, therefore, shall be addressed in the respective parts of the ISO/IEC 19823 series.

4.2 By demonstration

"By demonstration" means laboratory testing of one or, if required for statistical reasons, multiple products, processes or services to ensure conformance.

A test laboratory meeting the requirements of ISO/IEC 17025 shall be selected for the performance of the indicated testing to ensure conformance of the component or system.

For protocol requirements that are verified **by demonstration**, the test conditions are specified by this document. The detailed test plan is at the discretion of the test laboratory.

4.3 By design

"By design" means design parameters and/or theoretical analysis that ensure conformance. A vendor submitting a component or system for conformance testing shall provide the necessary technical information, in the form of a technical memorandum or similar. A test laboratory shall issue a test certificate indicating whether the technical analysis was sufficient to ensure conformance of the component or system.

For protocol requirements that are verified **by design**, the method of technical analysis is at the discretion of the submitting vendor and is not specified by this document. In general, the technical analysis shall have sufficient rigor and technical depth to convince a test engineer knowledgeable of the protocol that the particular requirement has been met.

5 Test methods with respect to the ISO/IEC 18000 series

5.1 Test requirements for ISO/IEC 18000-3 Interrogators and Tags

The following mandatory requirements and applicable optional requirements of ISO/IEC TR 18047-3:2011 shall be fulfilled:

— 5.2 Default conditions applicable to the test methods

Before a DUT is tested according to this document, it shall successfully pass the following prerequisite from ISO/IEC TR 18047-3:2011:

— 5.3 Conformance tests for ISO/IEC 18000-3 Mode 1

5.2 Test requirements for ISO/IEC 18000-63 Interrogators and Tags

The following mandatory requirements and applicable optional requirements of ISO/IEC 18047-6:2017 shall be fulfilled:

— Clause 4 Default conditions applicable to the test methods

— Clause 5 Set up of test equipment

Before a DUT is tested according to this document, it shall successfully pass the following prerequisite from ISO/IEC 18047-6:2017:

— Clause 8 Conformance tests for ISO/IEC 18000-63

6 Test methods with respect to the ISO/IEC 29167-10 Interrogators and Tags

6.1 Test map for optional features

Table 1 lists all optional features of this crypto suite and shall be used as a template to report the test results.

Table 1 — Test map for optional features

#	Feature	Additional requirements	Mark items to be tested for supplied product	Test results
1	TAM2	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
1.1	Memory profiles and MPI	Shall be tested for all the declared memory profiles and for every supported key.		
		MAX_Profiles=Number of memory profiles.		
		MAX_KeyID=Number of keys supported.		
1.21	ProtMode=0000_b	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
1.22	ProtMode=0001_b	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
1.23	ProtMode=0010_b	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
1.24	ProtMode=0011_b	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
2	IAM1	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		

Table 1 *(continued)*

#	Feature	Additional requirements	Mark items to be tested for supplied product	Test results
3	IAM2	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
4	IAM3	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
5.1	Memory profiles and MPI	Shall be tested for all the declared memory profiles and for every supported key.		
		MAX_Profiles=Number of memory profiles.		
		MAX_KeyID=Number of keys supported.		
5.21	ProtMode=0000_b	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
5.22	ProtMode=0001_b	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
5.23	ProtMode=0010_b	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
5.24	ProtMode=0011_b	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
6	MAM1	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		
7	MAM2	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 15693 or ISO/IEC 18000.		

Table 3 lists all crypto suite requirements that shall be tested in dependence of the features of Table 1 as supported by the DUT. Items marked with M are mandatory and shall be tested for each DUT.

6.2 Additional parameters required as input for the test

Table 2 lists all additional test parameters of this crypto suite.

Table 2 — Additional test parameters

#	Feature	Additional requirement	Value
1	Maximum BlockSize	Shall be provided to ensure that only test results for supported parameters are taken into consideration.	
2	TAM2 Revision	Shall be provided to ensure that only test results for supported parameters are taken into consideration.	0 or 1

6.3 Crypto suite requirements

6.3.1 General

This clause contains all requirements of ISO/IEC 29167-10.

6.3.2 Crypto suite requirements of ISO/IEC 29167-10:2017, Clauses 1 to 6

All the requirements of ISO/IEC 29167-10:2017, Clauses 1 to 6 are mandatory, inherently by design only.

6.3.3 Crypto suite requirements of ISO/IEC 29167-10:2017, Clauses 7 to 12

Table 3 contains all requirements of ISO/IEC 29167-10:2017, Clauses 7 to 12.

Table 3 — Crypto suite requirements of ISO/IEC 29167-10:2017, Clauses 7 to 12

Item	Protocol subclause[a]	Requirement[a]	M/O[b]	Applies to	How verified[c]
0020	7 Crypto suite state diagram	The Tag shall transition from the Start State to the Next State conforming to the requirements specified in Annex A.	M	Tag	By design
0030	8 Initialization and resetting	After power-up and after a reset, the crypto suite shall transition into the **Initial** state.	M	Tag	By design
0040	8	After the Tag encounters an error condition, it shall transition into the **Initial** state.	M	Tag	By design
0050	8	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.	M	Tag	By design
0060	8	A transition to **Initial** state shall also cause a reset of all variables used by the crypto suite.	M	Tag	By design
0070	8	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.	M	Tag	By design
0080	9.2 Adding custom data	The authentication message shall include the reference KeyID to select an encryption key in Table 27 (see Clause 11).	M	Interrogator	By design
0090	9.2	If protection of integrity and authenticity of the data is requested, the selected reference KeyID shall also contain a MAC key.	M	Interrogator	By design
0100	9.2	A Tag that supports including custom data in the authentication process shall define at least one and at most 16 memory profiles.	M	Tag	By demonstration using test pattern 08
0110	9.2	The memory profiles may also be linked to a key in Table 27 that shall be used for the encryption process to protect the data.	M	Tag	By demonstration using test pattern 07
0120	9.2	The custom data block shall be defined by the parameters BlockSize, Profile, Offset and BlockCount.	M	Interrogator / Tag	By design
0130	9.2	The mode of operation that shall be used for the encryption and/or protection of the custom data is specified by ProtMode.	M	Interrogator / Tag	By design

Table 3 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	M/O[b]	Applies to	How verified[c]
0140	9.2	BlockSize shall select the size of the custom data block; "0_b" specifies custom data in 64-bit blocks, "1_b" specifies custom data as 16-bit blocks.	M	Interrogator / Tag	By design
0150	9.2	Profile shall select one of the memory profiles that are supported by the Tag. The memory profiles are specified in Annex E.	M	Interrogator / Tag	By design
0160	9.2	Maximum binary value is "1111_b", or decimal 15, corresponding to a maximum number of 16 blocks of custom data that shall be included.	M	Tag	By design
0170	9.2	If the number of included bits of the custom data including the header is not a multiple of 128, then padding with zeroes shall be applied to the least significant bits of the last block that has a non-zero block size of less than 128 bits.	M	Tag	By design
0180	9.2	The Interrogator shall maintain the value of BlockCount for use as part of the MAC verification process.	M	Interrogator	By design
0190	9.2	The Tag manufacturer shall specify the number of custom data blocks that can be included.	M		By design
0200	9.2	The minimum value of D shall be 1. The maximum value of D supported by the Tag is specified by the Tag manufacturer.	M		By design
0210	9.2	ProtMode specifies the mode of operation that shall be used for the encryption and/or protection of the custom data.	M	Interrogator / Tag	By design
0220	9.3 Message and response formatting	The crypto suite shall parse the Messages and process the data based on the value of AuthMethod, which is the first parameter (first two bits) of all Messages.	M	Tag	By design
0230	9.3	The Messages for Tag Authentication, Interrogator Authentication and Mutual Authentication shall be distinguished by AuthMethod.	M	Interrogator / Tag	By design
0240	9.3	If AuthMethod = "00_b", the Tag shall parse the Message for Tag Authentication as described in 9.4.	M	Tag	By design
0250	9.3	If AuthMethod = "01_b", the Tag shall parse Message for Interrogator Authentication as described in 9.5.	M	Tag	By design
0260	9.3	If AuthMethod = "10_b", the Tag shall parse Message for Mutual Authentication as described in 9.6.	M	Tag	By design

Table 3 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	M/O[b]	Applies to	How verified[c]
0270	9.3	If AuthMethod = "11_b", then the Tag shall return a "Not Supported" error condition.	M	Tag	By demonstration, using the test pattern 01
0280	9.4.1 TAM	If CustomData = "0_b", the Tag shall parse the TAM1 Message for Tag Authentication without custom data as described in 9.4.2.	M	Tag	By demonstration, using the test pattern 03
0280	9.4.1 TAM	If CustomData = "1_b", the Tag shall parse the TAM2 Message for Tag Authentication with custom data as described in 9.4.5.	M	Tag	By demonstration, using the test pattern 08
0280	9.4.2 TAM1	For Tag authentication, the Interrogator shall generate an 80-bit random TAM1 Interrogator challenge and include that in the TAM1 message. The TAM1 message shall also include the reference KeyID to select an encryption key in Table 27 (see Clause 11). KeyID: 8-bit value that specifies the key that shall be used for TAM1.	M	Interrogator / Tag	By demonstration, using the test pattern 03
0310	9.4.2	The Tag shall accept this message in any state. If the value of the parameters of the message is invalid, then the Tag shall transition to the **Initial** state, thereby aborting any cryptographic protocol that has not yet been completed.	M	Tag	By design
0330	9.4.2	If the length of the TAM1 message is <> 96 bits, then the Tag shall return an "Other Error" error condition.	M	Tag	By demonstration, using the test pattern 02
0340	9.4.2	If TAM1_RFU[4:0] is <> "00000_b", then the Tag shall return a "Not Supported" error condition.	M	Tag	By demonstration, using the test pattern 02
0350	9.4.2	If the Tag does not support key[KeyID].*ENC_key*, then the Tag shall return a "Not Supported" error condition.	M	Tag	By demonstration using test pattern 02 (test pattern 5)
0360	9.4.3	If all parameters have been successful verified, then the Tag shall generate a response as specified in Table 5. The Tag shall generate the random data *TRnd_TAM1*[31:0] and encrypt the concatenation of the constant C_TAM1[15:0], the random data *TRnd_TAM1*[31:0] and the challenge IChallenge_TAM1[79:0] using Key[KeyID].*ENC_key.*	M	Tag	By demonstration using test pattern 03
0380	9.4.3	After returning the TAM1 Response (TResponse), the Tag shall remain in the **Initial** state.	M	Tag	By design

Table 3 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	M/O[b]	Applies to	How verified[c]
0390	9.4.4	The Interrogator (or the external application controlling the Interrogator) decrypts the TAM1 Response (TResponse) and shall verify whether C_TAM1 and IChallenge_TAM1 have the correct value.	M	Interrogator	By demonstration using test pattern 03
0400	9.4.5 TAM2 Message	The Interrogator shall generate an 80-bit random number for use as TAM2 Interrogator challenge.	M	Interrogator	By design
0410	9.4.5	BlockCount[3:0]: number that defines the size of the custom data as a number of 16-bit or 64-bit blocks. If the number of included bits of the custom data including header is not a multiple of 128, then padding with zeroes shall be applied to the least significant bits of the last block that has a non-zero block size of less than 128 bits.	M	Interrogator	By design
0420	9.4.5	The Interrogator shall maintain the value of BlockCount for use as part of the MAC verification process.	M	Interrogator	By design
0430	9.4.5	The Tag manufacturer shall specify the number of custom data blocks that can be included.	M	Tag	By design
0440	9.4.5	ProtMode[3:0]: value to select the mode of operation that shall be used to process the custom data as specified in Table 3.	M	Interrogator	By design
0450	9.4.5	The Tag shall accept this message in any state.	M	Tag	By design
0460	9.4.5	If the parameters of the message are invalid, then the Tag shall transition to the **Initial** state, thereby aborting any cryptographic protocol that has not yet been completed.	M	Tag	By design
0470	9.4.5	If the length of the TAM2 message is <> 120 bits, then the Tag shall return an "Other Error" error condition.	M	Tag	By demonstration using test pattern 06
0480	9.4.5	If BlockSize = "1_b" and the Tag does not support value "1_b", then the Tag shall return a "Not Supported" error condition.	M	Tag	By design
0490	9.4.5	If TAM2_Rev specifies a TAM2 message format that is not supported by the Tag, then the Tag shall return a "Not Supported" error condition.	M	Tag	By design
0500	9.4.5	If TAM2_RFU[2:0] is <> "000_b", then the Tag shall return a "Not Supported" error condition.	M	Tag	By demonstration using test pattern 06
0510	9.4.5	If the Tag does not support key[KeyID].*ENC_key*, then the Tag shall return a "Not Supported" error condition.	M	Tag	By demonstration using test pattern 06

Table 3 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	M/O[b]	Applies to	How verified[c]
0520	9.4.5	If the memory profile specified in Profile is not supported by the Tag, then the Tag shall return a "Not Supported" error condition.	M	Tag	By demonstration using test pattern 06
0530	9.4.5	The Tag shall check if the specified memory profile has the right to use KeyID for further processing: else key[KeyID] is not authorized for this memory profile and the Tag shall return a "Not Supported" error condition.	M	Tag	By demonstration using test pattern 07
0550	9.4.5	If the block of custom data specified by BlockSize, Profile, Offset and BlockCount is not supported by the Tag, then the Tag shall return a "Memory Overrun" error condition.	M	Tag	By demonstration using test pattern 06
0560	9.4.5	If the ProtMode value is not supported by the Tag, then the Tag shall return a “Not Supported” error condition.	M	Tag	By design
0570	9.4.6.1 TAM2 Response	If all parameters have been successfully verified, then the Tag shall proceed with parsing the TAM2 message.	M	Tag	By demonstration using test pattern 08
0580	9.4.6.1	After returning the TAM2 Response (TResponse), the Tag shall remain in the **Initial** state.	M	Tag	By design
0590	9.4.6.2 TAM2_Rev = "0_b" and ProtMode = "0000_b"	The Tag shall add custom data in plaintext to the authentication block and generate a response as specified in Table 7.	O	Tag	By demonstration using test pattern 08, with profile that is supported by the Tag and ProtMode = "0000_b"
0600	9.4.6.3 TAM2_Rev = "0_b" and ProtMode = "0001_b"	The Tag shall add custom data with confidentiality protection to the authentication block and generate a response as specified in Table 8. The Tag shall use AES encryption in CBC mode to encrypt all *D* custom data blocks.	O	Tag	By demonstration using test pattern 08, with profile that is supported by the Tag and ProtMode = "0001_b"
0620	9.4.6.4 TAM2_Rev = "0_b" and ProtMode = "0010_b"	The Tag shall add custom data with integrity protection to the authentication block and generate a response as specified in Table 9. The Tag shall use AES-CMAC-96 to calculate the truncated 96-bit CMAC over the authentication block and the *D* following plaintext custom data blocks.	O	Tag	By demonstration using test pattern 08, with profile that is supported by the Tag and ProtMode = "0010_b"