INTERNATIONAL STANDARD

ISO/IEC 19823-10

First edition
2017-11

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 19823-10:2017(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

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. 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*.

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

Introduction

The ISO/IEC 29167 series of standards describes security services as applicable for the ISO/IEC 18000 series of standards. 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 of standards describes the conformance test methods for security service crypto suites. The ISO/IEC 19823 series is related to the ISO/IEC 18047 series of standards, 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 be compliant to a pair of ISO/IEC 18000-n and ISO/IEC 29167-m, then the test methods of ISO/IEC 18047-n and ISO/IEC 19823-m 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 multiple parts of ISO/IEC 18046.

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 related to RFID tags and interrogators defined 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 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 18047-6:2012, *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 (all parts), *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

ISO/IEC 29167-10:2015, *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:

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

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

3.2 Symbols

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

3.3 Abbreviated terms

For the purposes of this document, the 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 ISO/IEC 18047 part and therefore, shall not be addressed in an ISO/IEC 19823 part. Only if ISO/IEC 18047 does not define them, then they may be defined in ISO/IEC 19823, although a revision of ISO/IEC 18047 should be the preferred option.

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

4.2 By demonstration

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

A test laboratory that meets ISO/IEC 17025 shall perform 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 compliance. A vendor submitting a component or system for compliance 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 in respect to the ISO/IEC 18000 parts

5.1 Test requirements for ISO/IEC 18000-3 interrogators and tags

The following mandatory requirements and applicable optional requirements of ISO/IEC 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 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 18047-6:2012 shall be fulfilled:

— 3.4 Default conditions applicable to the test methods

— Clause 4 Set up of test equipment

Before a DUT is tested according to this document, it shall successfully pass the following prerequisite from ISO/IEC 18047-6:2012:

— Clause 7 Conformance tests for ISO/IEC 18000-63

6 Test methods in 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. Furthermore, it is used to refer to the test requirements in 7.3.

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 declared ISO/IEC 18000 part		
1.1	Memory profiles and MPI	Shall be tested with the *Authenticate* command of the declared memory profiles and every key MAX_Profiles=Number of memory profiles MAX_KeyID=Number of keys supported		
1.2	ProtMode=0000_b	Shall be tested with the *Authenticate* command of the declared ISO/IEC 18000 part		
1.3	ProtMode=0001_b	Shall be tested with the *Authenticate* command of the declared ISO/IEC 18000 part		
1.4	ProtMode=0010_b	Shall be tested with the *Authenticate* command of the declared ISO/IEC 18000 part		
1.5	ProtMode=0011_b	Shall be tested with the *Authenticate* command of the declared ISO/IEC 18000 part		

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 in order to ensure that only test results for supported parameters are taking into consideration.	

6.3 Crypto suite requirements

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

6.3.1 Crypto suite requirements of ISO/IEC 29167-10:2015, Clauses 1 to 6

All the requirements of ISO/IEC 29167-10:2015, Clauses 1 to 6 are mandatory, inherently by design only.

6.3.2 Crypto suite requirements of ISO/IEC 29167-10:2015, Clauses 7 to 12

Table 3 contains all requirements of ISO/IEC 29167-10:2015, Clauses 7 to 12.

The column MO (Mandatory/Optional) has the following content:

— M (Mandatory): Items marked with “M” are mandatory and shall be tested for all devices;

— O (Optional): Items marked with “O” are optional and shall be tested only for devices that support the feature that is indicated by the requirement.

Table 3 — Crypto suite requirements

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0010	7	MAC_key[127:0] Variable that shall contain the key that will be used for cryptographic integrity protection.	O	Interrogator Tag	By design
0020	8	A transition to **Initial** state shall also cause a reset of all variables used by the crypto suite.	M	Tag	By design
0030	9	Implementations of this crypto suite shall ensure that all memory used for intermediate results is cleared after each operation (message-response pair) and after reset.	M	Tag	By design

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0040	10.2	The crypto suite shall parse the Messages and process the data based on the value of AuthMethod, which is the first parameter of all Messages.	M	Tag	By demonstration using test patterns for ISO/IEC 18000-3 mode 1 This subclause is reserved to define the test patterns for ISO/IEC 18000-3 mode 1. **Test patterns for ISO/IEC 18000-3 mode 3** This subclause is reserved to define the test patterns for ISO/IEC 18000-3 mode 3. **Test patterns for ISO/IEC 18000-63** This subclause defines the test patterns for ISO/IEC 18000-63. That document also contains the descriptions of the terms used in the test patterns. Miller2 stands for "Miller Subcarrier Sequence M=2" Miller4 stands for "Miller Subcarrier Sequence M=4" Test pattern 1
0050	10.2	The following sections of this document describe the formatting of Message and Response for Tag Authentication. AuthMethod shall be "00_b" for Tag Authentication.	M	Tag	By demonstration using test patterns for ISO/IEC 18000-33 mode 1 This subclause is reserved to define the test patterns for ISO/IEC 18000-3 mode 1. **Test patterns for ISO/IEC 18000-3 mode 3** This subclause is reserved to define the test patterns for ISO/IEC 18000-3 mode 3. **Test patterns for ISO/IEC 18000-63** This subclause defines the test patterns for ISO/IEC 18000-63. That document also contains the descriptions of the terms used in the test patterns. Miller2 stands for "Miller Subcarrier Sequence M=2" Miller4 stands for "Miller Subcarrier Sequence M=4" Test pattern 1

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0060	10.2	If AuthMethod="00_b" the Tag shall parse Message as described in 10.3.	M	Tag	By demonstration using test patterns for ISO/IEC 18000-3 mode 1 This subclause is reserved to define the test patterns for ISO/IEC 18000-3 mode 1. **Test patterns for ISO/IEC 18000-3 mode 3** This subclause is reserved to define the test patterns for ISO/IEC 18000-3 mode 3. **Test patterns for ISO/IEC 18000-63** This subclause defines the test patterns for ISO/IEC 18000-63. That document also contains the descriptions of the terms used in the test patterns. Miller2 stands for "Miller Subcarrier Sequence M=2" Miller4 stands for "Miller Subcarrier Sequence M=4" Test pattern 1
0070	10.2	If AuthMethod="01_b", "10_b" or "11_b" then the Tag shall return a "Not Supported" error condition and shall transition to the **Initial** state.	M	Tag	By demonstration using Test pattern 2
0080	10.3	The functionality shall be implemented by means of a challenge-response exchange. Tag authentication only shall be implemented in TAM1 and Tag authentication with the addition of custom data shall be implemented as TAM2 (see Figure 2).	M	Tag	By design
0090	10.3	The crypto suite shall parse the TAM Messages and process the data based on the value of CustomData, which is the second parameter of both TAM Messages. The Messages for Tag Authentication without and with custom data shall be distinguished by CustomData. CustomData shall be "0_b" for Tag Authentication without custom data and "1_b" for Tag Authentication with custom data.	M	Tag	By demonstration using Test pattern 3
0100	10.3	If CustomData="0_b" the Tag shall parse the TAM1 Message as described in 10.3.2.	M	Tag	By demonstration using Test pattern 3