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

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0110	10.3	If CustomData="1_b" the Tag shall parse the TAM2 Message as described in 10.3.4.	O-1	Tag	By demonstration using Test pattern 4
0120	10.3.2	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 the Key Management Table (see Clause 12). — KeyID: defines the key that shall be used for TAM1.	M	Interrogator Tag	By demonstration using Test pattern 1 twice with different values of KeyID and checking that the response contains the appropriate MAC in both cases.
0130	10.3.2	The Tag shall accept this message in any state. If the parameters of the message are valid, then the Tag shall transition to the **Initial** state; thereby aborting any cryptographic protocol that has not yet been completed.	M	Tag	By demonstration sending two different TAM1 messages, one after each other, without waiting for the response to the first TAM1 message. Check if the response to the second TAM1 message is correct.
0140	10.3.2	If the length of the TAM1 message <> 96 bits then the Tag shall return an "Other Error" error condition and shall transition to the **Initial** state.	M	Tag	By demonstration using a sequence of Test pattern 1, with different values for IChallenge_TAM1. First time IChallenge_TAM1 shall be "D53600FAA9B4C1965CC3$_h$" and the response shall be according to Test pattern 1. Second time IChallenge_TAM1 shall be "D53600FAA9B4C1965C" (88 bits) and the response shall be "Other Error". Third time IChallenge_TAM1 shall be "D53600FAA9B4C1965CCFF$_h$" (104 bits) and the response shall be "Other Error".
0150	10.3.2	If TAM1_RFU <> "00000_b" then the Tag shall return a "Not Supported" error condition and shall transition to the **Initial** state.	M	Tag	By demonstration using a sequence of Test pattern 1, with two different values for TAM1_RFU. First time TAM1_RFU shall be "$0x00000_b$" and the response shall be according to Test pattern 1. Second time TAM1_RFU shall be "$0x00001_b$" and the response shall be "Other Error".

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0160	10.3.2	If the Tag does not support key[KeyID].ENC_key then it shall return a "Not Supported" error condition and shall transition to the **Initial** state.	M	Tag	By demonstration using Test pattern 5
0170	10.3.3	If all verifications are successful, then the Tag shall generate the random data TRnd_TAM1 (32 bits) and encrypt the challenge IChallenge_TAM1 of the Interrogator using Key[KeyID]. ENC_key, after first prefixing the constant C_TAM1 (16 bits) and the random data TRnd_TAM1.	M	Tag	By demonstration using Test pattern 3
0180	10.3.2	After returning the TAM1 Response (TResponse) the Tag shall remain in the **Initial** state.	M	Tag	By demonstration using Test pattern 1 twice and verifying two correct responses.
0190	10.3.4	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. If the values are correct, then the Tag can be considered as authentic.	M	Interrogator	By demonstration using Test pattern 3
0200	10.3.5	TAM2 shall be used for Tag Authentication if the Tag needs to return part of its memory as custom data that may be protected (protection of integrity and authenticity) and/or encrypted (confidentiality protection) with the Tag authentication. The TAM2 message shall also include the reference KeyID to select an encryption key in the Key Management Table (see Clause 12). If protection of integrity and authenticity of the data is requested, the selected key shall also contain a MAC key.	O-1.1	Interrogator Tag	By design
0210	10.3.5	A Tag that supports TAM2 shall define at least one and at most 16 memory profiles. All supported addresses or pointers for the memory profiles shall be specified in Annex E.	O-1.1	Tag	By design

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0220	10.3.5	The memory profiles may also be linked to a key in the Key Management Table that shall be used for the encryption process to protect the data.	O-1.1	Tag	By design
0230	10.3.5	Custom data is specified as a number (1 to 16) of consecutive 64-bit blocks in the Tag's memory. The custom data block shall be defined by the parameters Profile, Offset and BlockCount.	O-1.1	Tag	By design
0240	10.3.5	Profile shall select one of the memory profiles that are supported by the Tag.	O-1.1	Tag	By design
0250	10.3.5	BlockCount specifies the 4-bit number of 64-bit custom data blocks that need to be returned from the offset position onwards. Minimum value is "0000_b", corresponding to one single 64-bit block. Maximum binary value is "1111_b", or decimal 15, corresponds to a maximum number of 16 64-bit blocks of custom data that shall be returned. If the number of returned bits of the custom data 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. The Interrogator shall maintain the value of BlockCount for use as part of the MAC verification process. The Tag manufacturer shall specify the number of custom data blocks that can be returned.	O-1.1	Tag	By design
0260	10.3.5	ProtMode specifies the mode of operation that shall be used for the encipherment and/or protection of the custom data. Table 5 defines the mode of operation for encipherment algorithms and/or message authentication algorithms for the (optional) protection (authentication and/or encipherment) of custom data.	O-1.1	Tag	By design

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0270	10.3.5	Tags shall implement at least one of the modes of operation as defined by Table 5 for each of the memory profiles that the Tag supports.	O-1.1	Tag	By design
0280	10.3.5	The Interrogator shall generate an 80-bit random TAM2 Interrogator challenge in the following TAM2 message and include several fields indicating additional options for the authentication protocol.	O-1.1	Interrogator Tag	By design
0290	10.3.5	— ProtMode: 4-bit value to select the mode of operation that shall be used to process the custom data	O-1.1	Tag	By design
0300	10.3.5	The Tag shall accept this message in any state. If the parameters of the message are valid, then the Tag shall transition to the **Initial** state; thereby aborting any cryptographic protocol that has not yet been completed.	O-1.1	Tag	By design
0310	10.3.5	If the length of the TAM2 message <> 120 bits, then the Tag shall return an "Other Error" error condition and shall transition to the **Initial** state.	O-1.1	Tag	By demonstration using a sequence of Test pattern 4, with different values for IChallenge_TAM2. First time IChallenge_TAM2 shall be "D53600FAA9B4C1965CC3$_h$" and the response shall be according to Test pattern 4. Second time IChallenge_TAM2 shall be "D53600FAA9B4C1965C$_h$" (88 bits) and the response shall be "Other Error". Third time IChallenge_TAM2 shall be "D53600FAA9B4C1965CCFF$_h$" (104 bits) and the response shall be "Other Error".
0320	10.3.5	If TAM2_RFU <> "00000$_b$" then the Tag shall return a "Not Supported" error condition and shall transition to the **Initial** state.	O-1.1	Tag	By demonstration using a sequence of Test pattern 4, with two different values for TAM2_RFU. First time TAM2_RFU shall be "0x00000$_b$" and the response shall be according to Test pattern 4. Second time TAM2_RFU shall be "0x00001b" and the response shall be "Other Error".

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0330	10.3.5	If the Tag does not support key[KeyID].ENC_key then it shall return a "Not Supported" error condition and shall transition to the **Initial** state.	O-1.1	Tag	By demonstration using a sequence of Test pattern 4, with different values for key[KeyID]. First time with supported key[KeyID] and the response shall be according to Test pattern 4. Second time with key[KeyID] that is not supported and the response shall be "Other Error".

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0340	10.3.5	The Tag shall check if the specified memory profile has the right to use KeyID for further processing: If Profile="0000_b" and key[KeyID].MPI[0:0]="1_b" or If Profile="0001_b" and key[KeyID].MPI[1:1]="1_b" or if Profile="0010_b" and key[KeyID].MPI[2:2]="1_b" or if Profile="0011_b" and key[KeyID].MPI[3:3]="1_b" or if Profile="0100_b" and key[KeyID].MPI[4:4]="1_b"or if Profile="0101_b" and key[KeyID].MPI[5:5]="1_b" or if Profile="0110_b" and key[KeyID].MPI[6:6]="1_b" or if Profile="0111_b" and key[KeyID].MPI[7:7]="1_b" or if Profile="1000_b" and key[KeyID].MPI[8:8]="1_b" or if Profile="1001_b" and key[KeyID].MPI[9:9]="1_b" or if Profile="1010_b" and key[KeyID].MPI[10:10]="1_b" or if Profile="1011_b" and key[KeyID].MPI[11:11]="1_b" or if Profile="1100_b" and key[KeyID].MPI[12:12]="1_b" or if Profile="1101_b" and key[KeyID].MPI[13:13]="1_b" or if Profile="1110_b" and key[KeyID].MPI[14:14]="1_b" or if Profile="1111_b" and key[KeyID].MPI[15:15]="1_b", then key[KeyID] is authorized for this memory profile, else key[KeyID] is not authorized for this memory profile and the Tag shall return a "Not Supported" error condition and shall transition to the **Initial** state.	O-1.1	Tag	By demonstration using Test pattern 6

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0350	10.3.5	If the memory profile specified in Profile is not supported by the Tag then the Tag shall return a "Not Supported" error condition.	O-1.1	Tag	By demonstration using a sequence of Test pattern 4, with different values for Profile. First time with a supported Profile and the response shall be according to Test pattern 4. Second time with a Profile that is not supported and the response shall be "Other Error".
0360	10.3.5	If the block of custom data specified by Profile, Offset and BlockCount is not supported by the Tag, then the Tag shall return a "Memory Overrun" error condition.	O-1.1	Tag	By demonstration using a sequence of Test pattern 4, with different values for Profile, Offset or BlockCount. First time with supported values for Profile, Offset and BlockCount and the response shall be according to Test pattern 4. Second time with a value for Profile, Offset or BlockCount that is not supported and the response shall be "Other Error".
0370	10.3.5	The Tag shall verify if the value of ProtMode is "0000_b" or "0001_b" or "0010_b" or "0011_b". If ProtMode has any other value, the Tag shall return a "Not Supported" error condition and shall transition to the **Initial** state.	O-1.1	Tag	By demonstration using a sequence of Test pattern 4, with different values for ProtMode. First time with ProtMode="0001b" and the response shall be according to Test pattern 4. Second time with ProtMode="0100b" and the response shall be "Other Error".
0380	10.3.6	If all verifications are successful, then the Tag shall proceed with parsing the TAM2 message.	O-1.1	Tag	By demonstration using Test pattern 4
0390	10.3.6.1	If all verifications are successful, then the Tag shall proceed with parsing the TAM2 message. Custom data is added in plaintext. The initialization vector IV for the encryption shall contain all zeroes.	O-1.1	Tag	By demonstration using Test pattern 4

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0400	10.3.7	If ProtMode=0010_b or ProtMode=0011_b, the Interrogator first checks the supplied MAC for correctness and aborts if MAC verification fails. The Interrogator (or the external application controlling the Interrogator) then decrypts the TAM2 Response (TResponse) and shall verify whether: C_TAM2 and IChallenge_TAM2 have the correct value. If the values are correct, then the Tag can be considered as authentic. (The additional data for Profile[3:0]) can be accepted if C_TAM2 and IChallenge_TAM2 have the correct values.)"	O-1.2 O-1.3	Interrogator	By demonstration using Test pattern 4 and verifying that the interrogator aborts if the local key at the interrogator is changed to a value different from that in the tag
0410	12	A Tag shall store one or more keys in the Key Table. A key is identified by the KeyID, the identification number of the key within the Key Table. KeyID shall start with "00_h" and increment with one for every next key in the Key Table.	M	Tag	By design
0420	12	Each key shall contain an encryption key (ENC_key).	M	Tag	By design
0430	12	Encryption keys shall be exclusively used for Tag authentication and encryption of additional data.	M	Tag	By design
0440	12	Message authentication keys shall be exclusively used for the authentication of additional data. The Tag shall maintain a record in the Key Table for each key.	M	Tag	By design
0450	12	A record of the Key Management Table shall have the following fields for every key:	M	Tag	By design

Table 3 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
0460	12	Each key may be linked to a memory profile that is supported by the Tag. The links are stored in the MPI field. The MPI field contains 16 bits that correspond to a memory profile that is supported on the Tag and defines if a security command of the air interface has the right to use that key to authenticate the Tag, encrypt the custom data and/or authenticate the custom data for the specified memory profile. MPI[0:0] to MPI[15:15] refers to memory profile 0 to 15 respectively, as far as they are supported by the Tag. If the value of an MPI bit is "0_b", this key shall not be used by the related profile. If the value of an MPI bit is "1_b", this key may be used by the related profile.	O-1.1	Tag	By design
0470	12	The MPI bit or bits for non-existing profile on a Tag shall be permalocked to zero (bit "0_b") by the Tag manufacturer.	O-1.1	Tag	By design
0480	12	MPI is an optional field, but is shall be supported if the Tag supports the TAM2 mode (with custom data).	O-1	Tag	By design
0490	12	The size and initial values of the Key Management Table and its mapping to their respective physical memory locations on the Tag shall be defined by the manufacturer.	M	Tag	By design

6.3.3 Crypto suite requirements of ISO/IEC 29167-10:2015, Annex A

Table 4 contains all requirements related to the crypto suite state transitions.

Table 4 — Crypto suite requirements of ISO/IEC 29167-10:2015, Annex A

Item	Protocol subclause	Requirement	MO	Applies to	How verified
1000	Annex A	Any combination of Start States and Transitions not listed in Table A.1 shall result in an error and consequently a transition to the **Initial** state.	M	Tag	By design
1010	Annex A	All other errors resulting from the execution of commands shall result in an error and consequently a transition to the **Initial** state.	M	Tag	By design

6.3.4 Crypto suite requirements of ISO/IEC 29167-10:2015, Annex E

This clause contains all requirements for the Protocol specific information.

6.3.4.1 Command definitions for ISO/IEC 29167-10:2015, E.1

Table 5 contains all requirements related to the concept of exchanging Messages and Responses.

Table 5 — Crypto suite requirements of ISO/IEC 29167-10:2015, E.1

Item	Protocol subclause	Requirement	MO	Applies to	How verified
1100	E.1.1	For the implementation of this crypto suite, an air interface protocol shall support security commands that allow the exchange of data between the Interrogator and the Tag that has this crypto suite implemented. The security command contains a message with parameters for the crypto suite. The reply of the Tag contains a response with the data that is returned by the crypto suite. An example of such data exchange for this crypto suite is depicted in Figure E.1.	M	Interrogator Tag	By design
1110	E.1.1	The crypto suites that are defined by ISO/IEC 29167 (all parts) can be defined by their Crypto Suite Identifier (CSI). According to ISO/IEC 29167-1, the CSI for this crypto suite shall be defined as the 6-bit value 000000_2. For use by the air interface protocols in this annex, the value is expanded to the 8-bit value 00_h.	M	Interrogator Tag	By design
1120	E.1.2	A crypto suite shall identify for each security service above and method if it is mandatory, optional, or prohibited	M		By design

6.3.4.2 Command definitions for ISO/IEC 29167-10:2015, E.2

This subclause is reserved to define the requirements for ISO/IEC 18000-3 mode 1.

6.3.4.3 Command definitions for ISO/IEC 29167-10:2015, E.3

This subclause is reserved to define the requirements for ISO/IEC 18000-3 mode 3.

6.3.4.4 Command definitions for ISO/IEC 29167-10:2015, E.4

Table 6 contains all requirements of ISO/IEC 18000-63.

Table 6 — Crypto suite requirements of ISO/IEC 18000-63

Item	Protocol subclause	Requirement	MO	Applies to	How verified
1200	E.4.1	A crypto suite supporting ISO/IEC 18000-63 shall fulfill the protocol security command requirements as defined in this clause.	M		By design
1210	E.4.1	Optional choices shall be accepted for 1-to-1 communication; since the Tag is singulated and the TID is known supported options can be derived from it.	M		By design
1220	E.4.1	a) The *Authenticate* command shall be supported.	M	Tag	By design
1230	E.4.1	b) The *Challenge* command shall not be supported.	M	Tag	By design
1240	E.4.1	c) The maximum execution time for an *Authenticate* Command containing a TAM1 or TAM2, payload shall be below 20 ms.	M	Tag	By demonstration using a high repetition of Test patterns 1 and 4 with appropriate timing measurement
1250	E.4.1	d) The Tag shall ignore commands from an Interrogator during execution of a cryptographic operation.	M	Tag	By design
1260	E.4.1	e) The Tag shall not support sending the contents of the ResponseBuffer in the reply to an ACK command.	M	Tag	By design
1270	E.4.1	f) The Tag shall support sending the contents of the ResponseBuffer in the reply to a *ReadBuffer* command	M	Tag	By design
1280	E.4.1	g) The Tag may support a security timeout following a crypto error.	M	Tag	By design

Table 6 *(continued)*

Item	Protocol subclause	Requirement	MO	Applies to	How verified
1290	E.4.1	h) A Tag in any cryptographic state other than initial (i.e. state after power-up) shall reset its cryptographic engine and transition to the open state upon receiving an invalid command. (Invalid commands mean crypto commands with incorrect handle or CRC error.)	M	Tag	By design
1300	E.4.1	i) For each Error Condition defined in the Crypto Suite: — The Tag shall transition to the **arbitrate** state. — The Tag shall send an Error Code in case of a transition to the **arbitrate** state.	M	Tag	By design
1310	E.4.1	j) The Tag shall remain in its current state after a Tag Authentication.	M	Tag	By design
1320	E.4.2	In ISO/IEC 18000-63, the message to execute Tag authentication shall be transmitted to the Tag with the *Authenticate*. The air interface shall return the response, either it shall be backscattered immediately after the command or it shall be stored in the ResponseBuffer, from where it shall be returned to the Interrogator with the *ReadBuffer* command.	M	Tag	By demonstration using Test patterns 7, 8 and 9
1330	E.4.2	ISO/IEC 18000-63 specifies an 8-bit CSI. For implementation of this part of ISO/IEC 29167 in ISO/IEC 18000-63, the CSI shall be expanded to the 8-bit value 00_h.	M	Tag	By design
1340	E.4.3	This part of ISO/IEC 29167 specifies error conditions when the authentication is not successful. The error conditions of the crypto suite shall be returned to the Interrogator as error codes for the air interface. Table E.2 shows the conversion of Error Conditions in the crypto suite to ISO/IEC 18000-63 error codes.	M	Interrogator Tag	By design