INTERNATIONAL STANDARD

ISO/IEC 19823-16

First edition
2020-10

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

Part 16: Crypto suite ECDSA-ECDH security services for air interface communications

Reference number
ISO/IEC 19823-16:2020(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 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*.

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.

This part of ISO/IEC 19823 describes the test methods for the ECDSA-ECDH crypto suite as standardized in ISO/IEC 29167-16.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning radio-frequency identification security technology given in Clause 6.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has 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 statement of the holder of this patent right is registered with ISO and IEC.

Information may be obtained from:

Patent holder: China IWNCOMM Co., Ltd.

Address: A201, QinFeng Ge, Xi'an Software Park, No.68 KeJi 2nd Road, Xi'an Hi-tech Industrial Development Zone, Xi'an, Shaanxi, P.R.China 710075

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

NOTE 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 16: Crypto suite ECDSA-ECDH security services for air interface communications

1 Scope

This document describes test methods for determining the conformance of security crypto suites defined in ISO/IEC 29167-16.

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 to be applied exclusively to RFID tags and interrogators defined in the ISO/IEC 18000 series using ISO/IEC 29167-16.

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 19762 (all parts), *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

ISO/IEC 18000-4:2018, *Information technology — Radio frequency identification for item management — Part 4: Parameters for air interface communications at 2.45 GHz*

ISO/IEC 29167-16:2015, *Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA-ECDH 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 29167-16 and the following 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

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 and the following apply.

ECDH	elliptic curve diffie-hellman
ECDHP	ECDH parameter
ECDSA	ellipticcurvedigital signature algorithm
MAC	message authentication code
MAM	mutual authentication message
MIC	message integrity code
RN	random number
SEK	session encryption key
SIK	session integrity check key
TPK	temporary public key
TRAIS	tag and reader air interface security
TRAIS-P	tag and reader air interface security based on public key cryptography
TTP	trusted third party
TTPID	identifier of TTP

4 Test methods

4.1 General

This document describes the general test methods for ISO/IEC 29167-16. 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 19823 series.

Clause 6 defines elements that are not covered by the ISO/IEC 18047 series and are therefore addressed in this document.

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 analyses that ensure conformance. 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 ISO/IEC 18000-4 Mode 4

5.1 Default items applicable to the test methods

The following requirements and applicable optional requirements shall be fulfilled.

5.1.1 Test environment

Unless otherwise specified, testing shall take place in an environment of temperature 23 °C ± 3 °C (73 °F ± 5 °F) and relative humidity of 40 % to 60 %.

5.1.2 Pre-conditioning

Where pre-conditioning is required by the test method, the tags and interrogators to be tested shall be conditioned to the test environment for an appropriate period of time before testing.

5.1.3 Default tolerance

Unless otherwise specified, a default tolerance of ±5 % shall be applied to the quantity values given to specify the characteristics of the test equipment (e.g. linear dimensions) and the test method procedures (e.g. test equipment adjustments).

5.1.4 Total measurement uncertainty

The total measurement uncertainty for each quantity determined by these test methods shall be stated in the test report.

NOTE1 Basic information is given in “ISO Guide to the Expression of Uncertainty in Measurement”, ISBN 92-67-10188-9, 1993.

NOTE2 The default items applicable to the test methods defined in 5.1 is given in ISO/IEC TR 18047-4.

5.2 Test setup and measurement equipment

This subclause defines the test setup and measurement equipment for verifying the operation of a tag or an interrogator according to ISO/IEC 18000-4 Mode 4.

Test results shall not be influenced by the setup method of the test.

Test setups include:

— test setup for interrogator testing (see 5.2.1),

— test setup for tag testing (see 5.2.2),

— test equipment (see 5.2.3).

These are described in the following subclauses.

5.2.1 Test setup for interrogator testing

An interrogator with integral antenna(e) shall be equipped with temporary antenna connector(s), or else coupling device(s) [i.e. sense antenna(e)] shall be used to connect to the test equipment.

A sense antenna shall not affect test results. Appropriate distances (e.g. 30 cm), antenna sizes and types (e.g. patch antenna) and antenna polarization (i.e. circular polarization) shall be used. The antenna configuration and distance shall be included in the test report.

To set up an interrogator with the appropriate test pattern and operational modes, one of two methods shall be used (combinations shall also be possible):

a) an implemented test mode,

b) a tag for initializing the appropriate operational mode.

The air interface parameter in a test mode shall behave in the same way as the air interface parameter during normal usage.

Unless otherwise stated, for all tests, the frequency of the reference carrier shall conform to ISO/IEC 18000-4:2018, 9.3.1. The output power shall be set to maximum (both carriers switched on).

5.2.2 Test setup for tag testing

A tag with integral antenna(e) shall be equipped with temporary antenna connector(s),or else suitable coupling device(s) [i.e. antenna(e)] shall be used to connect to the test equipment.

A sense antenna shall not affect test results. Appropriate distances (e.g. 30 cm), antenna sizes and types (e.g. patch antenna), as well as antenna polarization (i.e. circular polarization) shall be used. The antenna configuration and distance shall be included in the test report.

To set up a tag with the appropriate test pattern and operational modes, one of two methods shall be used (combinations shall also be possible):

a) an implemented test mode,

b) an interrogator for initializing the appropriate operational mode.

Unless otherwise stated, for all tests, the frequency of the reference carrier shall conform to ISO/IEC 18000-4:2018, 9.3.1.

5.2.3 Test equipment

All tests shall be performed using commercial test equipment. In addition to the measurement devices described in the following subclauses, appropriate devices such as power supplies, splitters, combiners and cables shall be used.

The reference point for all measurements shall be either (temporary) antenna connector(s), or appropriate coupling device(s). The reference point shall be documented in the test report.

5.2.3.1 Spectrum analyser

A spectrum analyser with the capability of digital demodulating and with vector signal analysis capability shall be used. Appropriate trigger functionality shall be either implemented in the spectrum analyser or generated externally with additional measurement devices.

5.2.3.2 Signal generator

A signal generator for the 2,45 GHz band shall be used to generate an interrogator output signal for testing tags. The signal level for the tests shall be within the operational range of the receiver input of the tag. The input level shall be specified by the tag manufacturer and shall be documented in the test report.

5.2.3.3 Logic analyser

A logic analyser shall be used for verification of the correct data. Therefore, the analyser shall be capable of storage of sequent samples in 0,5 second.

6 Test methods in respect to ISO/IEC 29167-16 interrogators and tags

6.1 Test map for optional features

Table 1 lists all optional features of the crypto suite defined by Tag and Reader Air Interface Security (TRAIS) based on Public key cryptography (TRAIS-P) and shall be used as a template for reporting the test results. Furthermore, Table 1 shall be used in reference to the test requirements in 6.2.

Table 1 — Test map for optional features

#	Feature	Additional requirement	Mark items to be tested for supplied product	Test results
1	Mutual Authentication without TTP involved	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 18000.		
2	Mutual Authentication with TTP involved	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 18000.		
3	Authenticate communication	Shall be tested with the *AuthComm* command of the relevant part of ISO/IEC 18000.		
4	Secure communication	Shall be tested with the *SecureComm* command of the relevant part of ISO/IEC 18000.		

Table 2 to Table 5 lists all crypto suite requirements that shall be tested in depending on the features of Table 1 as supported by the device under test. Items marked with M are mandatory and shall be tested for each device under test.

6.2 Crypto suite requirements

6.2.1 General

This subclause contains all of the requirements of ISO/IEC 29167-16.

6.2.2 Crypto suite requirements of ISO/IEC 29167-16:2015, Clauses 1 - 6

All of the requirements of ISO/IEC 29167-16:2015, Clauses 1-6 are mandatory, inherently by design only.

6.2.3 Crypto suite requirements of ISO/IEC 29167-16:2015, Clauses 7 - 11

Table 2 contains all of the requirements of ISO/IEC 29167-16:2015, Clauses 7 – 11.

The column MO (Mandatory / Optional) contains the following information:

— items marked with "M" are mandatory and shall be tested for all devices;

— items marked with "O" are optional and shall be tested only for devices that support the feature that is indicated by the requirement.

Table 2 — Crypto suite requirements

Item	Protocol Subclause	Requirement	M/O	Applies To	How Verified
1	7.1	ECDHP: ECDH parameter, consisting of parameter ID, parameter length and parameter content three parts, where the parameter ID shall be 8 bits; parameter shall be 16 bits in length and indicates the number of bytes in the parameter content. The values of ECDH parameter: 1) 01_h: The field value shall be denoted by OIDs. The Length subfield indicates the number of octets of OIDs. The values of Content subfield are the content of OIDs. 2) Other: All other values are RFU.	M	Interrogator/ Tag	By design
2	7.1	MK[127:0] Master key	M	Interrogator/ Tag	By design
3	7.1	MIC_t[255:0] Message integrity code generated by the tag, the length shall be 256 bits.	M	Tag	By design
4	7.1	RN_t[63:0] 64-bit random number generated by the tag	M	Tag	By design
5	7.1	Sig_t[383:0] Digital signature generated by the tag. The length shall be 384 bits.	M	Tag	By design
6	7.1	TPK_t[391:0] Temporary public key generated by tag, the length shall be 392 bits.	M	Tag	By design
7	7.1	X_t[391:0] Temporary private key generated by tag and used for ECDH exchange.	M	Tag	By design
8	7.1	MIC_i[255:0] Message integrity code generated by the interrogator, the length shall be 256 bits.	M	Interrogator	By design
9	7.1	RN_i[63:0] 64-bit random number generated by theinterrogator.	M	Interrogator	By design
10	7.1	Sig_i[383:0] Digital signature generated by the interrogator. The length shall be 384 bits.	M	Interrogator	By design
11	7.1	TPK_i[391:0] Temporary public key generated by interrogator, the length shall be 392 bits.	M	Interrogator	By design

Table 2 *(continued)*

Item	Protocol Subclause	Requirement	M/O	Applies To	How Verified
12	7.1	X_i[391:0] Temporary private key generated by interrogator and used for ECDH exchange.	M	Interrogator	By design
13	7.2	Cert Type shall be 4 bits, Value shall be: a) 0000:Value subfield contains X.509 certificate of Interrogator, $Cert_i$; b) 0001:Value subfield contains X.509 certificate of Tag, $Cert_t$; c) 0010:Value subfield contains X.509 certificate of TTP, $Cert_{ttp}$; d) Other: All other values are RFU.	M	Interrogator/ Tag	By design
14	8	A transition to Ready state shall also cause a reset of all variables used by the crypto suite.	M	Tag	By design
15	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
16	10.2.1	The crypto suite shall parse the Messages and process the data based on the value of CSI, which is the first parameter of all commands.	M	Interrogator	By demonstration using Test patterns 3,4,7 and 8
17	10.2.2	The FN shall be 8 bits.	M	Interrogator	By demonstration using Test patterns 3,4,7 and 8
18	10.2.2	The IID shall be 64 bits.	M	Interrogator	By demonstration using Test patterns 3,4,7 and 8
19	10.2.2	The following sections of this document describe the formatting of Message and Response for authentication. AuthType shall be "00".	M	Interrogator	By demonstration using Test patterns 3,4,7 and 8
20	10.2.2	In MAM1.1 Message, AuthStep shall be "000".	M	Interrogator	By demonstration using Test patterns 3,4,7 and 8
21	10.2.2	If TTP not to be involved, TTPID shall be "0000 0000", or If TTP to be involved, TTPID shall be "0000 0001".	M	Interrogator	By demonstration using Test patterns 3,4,7 and 8
22	10.2.2	ECDH parameter shall be 01_h.	M	Interrogator	By demonstration using Test patterns 3,4,7 and 8
23	10.2.3	The FN shall be 8 bits.	M	Tag	By demonstration using Test patterns 1,2,5 and 6
24	10.2.3	TheTID shall be 64 bits.	M	Tag	By demonstration using Test patterns 1,2,5 and 6

Table 2 *(continued)*

Item	Protocol Subclause	Requirement	M/O	Applies To	How Verified
25	10.2.3	TTPID is the same as the one in the MAM1.1 Message.	M	Tag	By demonstration using Test patterns 1,2,5 and 6
26	10.2.3	ECDH parameter shall be 01_h.	M	Tag	By demonstration using Test patterns 1,2,5 and 6
27	10.2.4	The FN shall be 8 bits.	M	Interrogator	By demonstration using Test patterns 4 and 8
28	10.2.4	The following sections of this document describe the formatting of Message and Response for authentication. AuthType shall be "00".	M	Interrogator	By demonstration using Test patterns 4 and 8
29	10.2.4	In MAM1.2 Message, AuthStep shall be "001".	M	Interrogator	By demonstration using Test patterns 4 and 8
30	10.2.4	AuthRes: This field shall be present if TTPID = "0000 0001" in MAM1.1 Message; otherwise, this field is not present.	O	Interrogator	By demonstration using Test patterns 4 and 8
31	10.2.5	The FN shall be 8 bits.	M	Tag	By demonstration using Test patterns 2 and 6
32	10.3.1	The tag should have ECC-based private key S_t and the related certificate $Cert_t$. The interrogator shall have ECC-based private key S_i and the related certificate $Cert_i$.	M	Interrogator/ Tag	By design
33	10.3.1	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. Authenticate(MAM1.1 Message) and MAM 1.1 Response, Authenticate(MAM1.2 Message) and MAM 1.2 Response shall be implemented(See ISO/IEC 29167-16:2015, Figure 3).	M	Interrogator/ Tag	By design
34	10.3.2	Transmits command *Authenticate*(MAM1.1 Message) to the tag (See ISO/IEC 29167-16:2015, Table 4).	M	Interrogator	By demonstration using Test patterns 3,4,7 and 8
35	10.3.2	If TTPID in *Authenticate* (MAM1.1 Message) is not "0000 0000" or "0000 0001", the authentication failed. The tag shall remain in the Ready state.	O	Tag	By design
36	10.3.2	Transmits MAM1.1Response to the interrogator(See ISO/IEC 29167-16:2015, Table 5).	M	Tag	By design
37	10.3.2	Sig_t = ECDSA (S_t,TID||IID||$Cert_t$||TTPID||RN_t||TPK_t||ECDHP).	M	Tag	By design

Table 2 *(continued)*

Item	Protocol Subclause	Requirement	M/O	Applies To	How Verified
38	10.3.2	After returning the MAM1.1 Response, the tag shall remain in the *Authenticate* state.	M	Tag	By design
39	10.3.2	Check whether the values of TTPID and ECDHP in MAM1.1 Response are equal to the values of TTPID and ECDHP in *Authenticate* (MAM1.1 Message). If not, the authentication failed.	M	Interrogator	By design
40	10.3.2	Use Q_t extracted from certificate $Cert_t$ to verify Sig_t. If failed, the authentication failed.	M	Interrogator	By design
41	10.3.2	Generates X_i and TPK_i, uses X_i and TPK_t to perform the ECDH computation, gets $(X_i \bullet TPK_t)_{abscissa}$, computes KD-HMAC-SHA256($(X_i \bullet TPK_t)_{abscissa}$, $RN_t \| RN_i$) to generate a 128 bits MK.	M	Interrogator	By design
42	10.3.2	Computes KD-HMAC-SHA256 (MK, $TID \| IID \| RN_t \| RN_i$) to generate 128 bits IAK, 128 bits SIK and 128 bits SEK.	M	Interrogator	By design
43	10.3.2	Transmits *Authenticate* (MAM1.2 Message) to tag(See ISO/IEC 29167-16:2015, Table 6).	M	Interrogator	By demonstration using Test patterns 4 and 8
44	10.3.2	Sig_i=ECDSA(S_i, $TID \| IID \| TTPID \| RN_t \| RN_i \| TPK_i$).	M	Interrogator	By design
45	10.3.2	MIC_i=HMAC-SHA256(IAK, $TID \| IID \| TTPID \| RN_t \| RN_i \| TPK_i \| Sig_i$).	M	Interrogator	By design
46	10.3.2	Confirm whether RN_t in *Authenticate* (MAM1.2 Message) is equal to the RN_t in MAM1.1 Response, if not, the authentication failed.	M	Interrogator	By demonstration using Test patterns 4 and 8
47	10.3.2	Use Q_i extracted from the certificate $Cert_i$ to verify Sig_i. If failed, authentication failed.	M	Tag	By design
48	10.3.2	Uses X_t and TPK_i to perform the ECDH computation, gets $(X_t \bullet TPK_i)_{abscissa}$, computes KD-HMAC-SHA256($(X_t \bullet TPK_i)_{abscissa}$, $RN_t \| RN_i$) to generate a 128 bits MK.	M	Tag	By design
49	10.3.2	Computes KD-HMAC-SHA256 (MK, $TID \| IID \| RN_t \| RN_i$) to generate 128 bits IAK, 128 bits SIK and 128 bits SEK.	M	Tag	By design
50	10.3.2	MIC_i=HMAC-SHA256(IAK, $TID \| IID \| TTPID \| RN_t \| RN_i \| TPK_i \| Sig_i$).	M	Tag	By design
51	10.3.2	If MIC_i is not equal to MIC_i received from *Authenticate* (MAM1.2 Message), the authentication failed.	M	Tag	By design
52	10.3.2	TransmitsMAM1.2 Response to the interrogator(See ISO/IEC 29167-16:2015, Table 7).	M	Tag	By demonstration using Test patterns2 and 6
53	10.3.2	MIC_t=HMAC-SHA256(IAK,$TID \| IID \| RN_i$)	M	Tag	By design

Table 2 *(continued)*

Item	Protocol Subclause	Requirement	M/O	Applies To	How Verified
54	10.3.2	Confirms whether RN_i in the response is equal to RN_i in *Authenticate* (MAM1.2 Message). If not, the authentication failed.	M	Interrogator	By demonstration using Test patterns 2 and 6
55	10.3.2	MIC_t=HMAC-SHA256(IAK,TID||IID||RN_i)	M	Interrogator	By design
56	10.3.2	If MIC_t is not equal to MIC_t received from *Authenticate* (MAM1.2 Message), the authentication failed.	M	Interrogator	By design
57	10.3.2	The certificate status verification shall be performed by both the tag and interrogator after they receive the certificate from each other and includes verification of the certificate's authenticity and expiration status.	M	Interrogator/ Tag	By demonstration using Test patterns1 to 8
58	10.3.2	The FN, AuthType, AuthStep, IID and TID in the received messages shall also be checked by both the tag and the interrogator.	M	Interrogator/ Tag	By demonstration using Test patterns 1 to 8
59	11.1	*AuthComm* command and Response shall be implemented (see ISO/IEC 29167-16:2015, Figure 5).	M	Interrogator/ Tag	By demonstration using Test pattern 9
60	11.1	The format of message in *AuthComm* command shall be in conformance with ISO/IEC 29167-16:2015, Table 8.	M	Interrogator	By demonstration using Test pattern 9
61	11.1	The format of Response to *AuthComm* command shall be in conformance with ISO/IEC 29167-16:2015, Table 9.	M	Tag	By demonstration using Test pattern 9
62	11.2	*SecureComm* command and Response shall be implemented (see ISO/IEC 29167-16:2015, Figure 6).	M	Interrogator/ Tag	By demonstration using Test pattern 10
63	11.2	The format of message in *SecureComm* command shall be in conformance with ISO/IEC 29167-16:2015, Table 10.	M	Interrogator	By demonstration using Test pattern 10
64	11.2	The format of Response to *SecureComm* command shall be in conformance with ISO/IEC 29167-16:2015, Table 11.	M	Tag	By demonstration using Test pattern 10

NOTE 1 The Authenticate state in ISO/IEC 29167-16 is a subtype of Session state in ISO/IEC 18000-4:2018, 9.6.

NOTE 2 The AuthComm and SecureComm state in ISO/IEC 29167-16 is the subtype of Secure Session state in ISO/IEC 18000-4:2018, 9.6.

6.2.4 Crypto suite requirements of ISO/IEC 29167-16:2015, Annex A

Table 3 contains all requirements related to the Crypto Suite state transitions.

Table 3 — Crypto suite requirements of ISO/IEC 29167-16:2015, Annex A

Item	Protocol Subclause	Requirement	M/O[a]	Applies To	How Verified
1	Annex A	Any combination of Ready states and transitions not listed in ISO/IEC 29167-16:2015, Table A.1 shall result in an error and consequently a transition to the Ready state.	M	Tag	By Design
2	Annex A	All other errors resulting from the execution of commands shall result in an error and consequently a transition to the **Ready** state.	M	Tag	By Design

[a] 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.

6.2.5 Crypto suite requirements of ISO/IEC 29167-16: 2015 in Annex E

This clause contains all requirements for the Protocol specific information.

6.2.5.1 Command definitions for ISO/IEC 29167-16:2015 in Annex E1

Table 4 contains all requirements related to the concept of exchanging Messages and Responses.

Table 4 — Crypto suite requirements of ISO/IEC 29167-16, Annex E.1

Item	Protocol Subclause	Requirement	M/O[a]	Applies To	How Verified
1	E.1	The crypto suites that are defined by ISO/IEC 29167 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 000110_2. For use by the air interface protocols in this Annex the value is expanded to the 8-bit value 06_h.	M	Interrogator Tag	By Design
2	E.1.2	A crypto suite shall identify for each security service above and method if it is mandatory, optional, or prohibited	M	Interrogator Tag	By design

[a] 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.

6.2.5.2 Command definitions for ISO/IEC 29167-16:2015, Annex E.2

Table 5 contains all requirements of ISO/IEC 18000-4:2018, Mode 4.

Table 5 — Crypto suite requirements of ISO/IEC 18000-4 Mode 4

Item	Protocol Subclause	Requirement	M/O[a]	Applies To	How Verified
1	E.2.1	A Crypto Suite supporting ISO/ IEC 18000-4 Mode4 shall fulfill the protocol security command requirements as defined in this section.	M	Interrogator/ Tag	By Design
2	E.2.1	NOTE Optional choices shall be accepted for 1-to-1 communication. Reason: Since the Tag is singulated and the TID is known supported options can be derived from it.	M	Tag	By Design
3	E.2.2	The *Authenticate* command shall be supported.	M	Interrogator/ Tag	By Design
4	E.2.2	The maximum execution time for an *Authenticate* Command containing a MAM1.1 or MAM1.2, payload shall be below 500ms.	M	Tag	By demonstration using Test pattern 1 or Test pattern 2
5	E.2.2	The Tag shall ignore commands from an Interrogator during execution of a cryptographic operation.	M	Tag	By Design
6	E.2.3	The *AuthComm* command shall be supported.	M	Interrogator Tag	By Design
7	E.2.3	The maximum execution time for an *AuthComm* Command, payload shall be below 500ms.	M	Tag	By demonstration using Test pattern 3
8	E.2.3	The Tag shall ignore commands from an Interrogator during execution of a cryptographic operation.	M	Tag	By Design
9	E.2.4	The *SecureComm* command shall be supported.	M	Interrogator Tag	By Design
10	E.2.4	The maximum execution time for an *SecureComm* Command, payload shall be below 500ms.	M	Tag	By demonstration using Test pattern 4
11	E.2.4	The Tag shall ignore commands from an Interrogator during execution of a cryptographic operation.	M	Tag	By Design

[a] 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.

6.3 Test patterns for ISO/IEC 18000-4:2018, Mode 4

This clause contains the Test patterns for ISO/IEC 18000-4:2018, Mode 4. Annex A provides parameters and examples for Test patterns 1 through 8. Test pattern 9 and Test pattern 10 do not require additional information.

6.3.1 Test pattern 1 utilizing ISO/IEC 18000-4:2018, 9.3.3

This pattern shall not be TTP involved. It shall be applied for two modulations, O-QPSK and DBPSK.

```
Ready(Command code=01h; Channel number=0; Ready password=00000000h)
Authenticate(MAM1.1 Message) (CSI=06h;Length;Message=(FN=00,IID[63:0],AuthType=00,AuthStep
=000,TTPID=0000 0000,Certi=___,ECDHP[255:0]))
```

The Test pattern is passed when the response field of the tag reply to the *Authenticate* is as follows:

MAM1.1 Response
(Length;Response=(FN=00,TID[63:0],TTPID=00000000,Certt=___,RN_t[63:0],TPK_t[391:0],ECDHP[255:0],Sigt[383:0])

For example:

Based on the example parameters provided in Annex A, Test pattern 1 can be operated as follows. Test patterns 1 to 8 can all be operated based on the example in Annex A.

```
Ready(Command code=01h; Channel number=0; Ready password=00000000h)

    Authenticate(MAM1.1 Message) (

    CSI=06h;

    Length;

    Message=(

          FN=00,

          IID[63:0],

          AuthType=00,

          AuthStep=000,

          TTPID=0000 0000,

          Certi=1099308201953082014 9A003020102020463 90D2F5300C06082A811CD763010101050030513
          1143012060A0992268993F22C6401191604574150 49310B3009060355040 61302434E310D300B0603
          55040A130430303033310B3009060355040B1302534E3110300E0603550403140761733140415355 3
          01E170D313431303031313633333325A170D313531303134313633334335A305931143012060A09
          92268993F22C6401191604574150 49310B3009060355040 61302434E310D300B060355040A1304303
          03033310B3009060355040B1302534E3118301606035504031 40F696E746572726F6761746F724041
          45304A301406072A8648CE3D020106092A811CD763010102010332000 4BBA79921268948117DA7345
          B44479A3EBDF7FE54EE26EBF1A360 1B8E9FF1B7E4EDDBA574BB34C795B0599CFF7A41429CA3143012
          3010060960864801 86F842010D0403160178300C06082A811CD763010101050003380030350219008
          FAB674B943BF646D6D27A70D3DDE435B3C46F6530D8839F021831B27EA8752C2F2DC5CB22951ECEDE
          8C0FEAD4A02B96BCEA,

          ECDHP=01000B06092a811cd763010102010000000000000000000000000000000000000000]

    )

)
```

The Test pattern is passed when the response field of the tag reply to the *Authenticate* is as follows:

```
MAM1.1 Response(

    Length;
    Response=(

        FN=00,

        TID[63:0],

        TTPID=00000000,

        Cert_t=11913082018D30820142A00302010202044A6C47C3300C06082A811CD7630101010D3051311
        43012060A0992268993F22C64011916045741504931 0B3009060355040613024345310B0603550
        40A130430303033310B3009060355040B1302534E3110300E0603550403140761733140415355301E1
        70D3134313030313136333333325A170D3135313031343136333334335A3052311430120 60A0992268
        993F22C64011916045741504931 0B3009060355040613024345310D300B0603550403 1304303030333
        10B3009060355040B1302534E3111300F0603550403140874616740415355450 4A301406072A8648C
        E3D020106092A811CD7630101020103320004A2FA97A41B88FB9552D5CA8EEA25EE51EB4ADAF88452
        8013CC11046A795F340E38F7EEB4B2BF00AC3195D60C0482878A31430123010060960864801 86F8420
        10D0403160178300C06082A811CD7630101015000337003034021825 C42F134F22B96399F13C7C31
        06A0C103966B0F326384502180EEAC4544727112856A44F7177D6D1E1EB3A9FEFEFB6C00C,

        RN_t=53CC8496DF6878A4],

        TPK_t=048BB733FA69A4EE35D37C9C7205615B0A767BD0B156B6811A8EE73F2EC633F8107245F0096052
        6FEEB10273E5BA5AD290],

        ECDHP=01000B06092a811cd7630101020100000000000000000000000000000000000000],

        Sig_t=B0B294ECC5F1DB9C85B5EBDCF89AA47F359F4526DC33843628786AE35E94DA884C2CF430C2C8D8
        13CE5FF40E949241FA]

    )

)
```

6.3.2 Test pattern 2 utilizing ISO/IEC 18000-4:2018, 9.3.3

This pattern shall not be TTP involved. It shall be applied for two modulations, O-QPSK and DBPSK.

```
Ready(Command code=01h; Channel number=0; Ready password=00000000h)
Authenticate(MAM1.1 Message) (CSI=06h;Length;Message=(FN=00,IID[63:0],AuthType=00,AuthStep
=000,TTPID=0000 0000,Certi=___,ECDHP[255:0]))
MAM1.1 Response
(Length;Response=(FN=00,TID[63:0],TTPID=00000000,Cert_t=___,RN_t[63:0],TPK_t[391:0],ECDHP[255:
0],Sig_t[383:0])
Authenticate(MAM1.2 Message) (CSI=06h;Length;Message=(FN=00,AuthType=00,AuthStep=001,RN_t[6
3:0],RN_i[63:0],TPK_i[391:0],Sig_i[383:0],MIC_i[255:0]))
```

The Test pattern is passed when the response field of the tag reply to the *Authenticate* is as follows:

```
MAM1.2 Response
(Length; Response=(FN=00,RNi[63:0],MICt[255:0]))
```

6.3.3 Test pattern 3 utilizing ISO/IEC 18000-4:2018, 9.3.3

This pattern shall not be TTP involved. It shall be applied for two modulations, O-QPSK and DBPSK.

```
Ready(Command code=01h; Channel number=0; Ready password=00000000h)
Authenticate(MAM1.1 Message) (CSI=06h;Length;Message=(FN=00,IID[63:0],AuthType=00,AuthStep
=000,TTPID=0000 0000,Certi=___,ECDHP[255:0]))
```

The test pattern is passed when TTPID, ECDHP in the Tag MAM1.1 Response equal to TTPID, ECDHP in Authenticate(MAM1.1 Message).

6.3.4 Test pattern 4 utilizing ISO/IEC 18000-4:2018, 9.3.3

This pattern shall be TTP not be involved, it shall be applied for two modulation O-QPSK and DBPSK.

Ready(Command code=01h; Channel number=0; Ready password=00000000h)
Authenticate(MAM1.1 Message) (CSI=06$_h$;Length;Message=(FN=00,IID[63:0],AuthType=00,AuthStep=000,TTPID=0000 0000,Cert$_i$=___,ECDHP[255:0]))
MAM1.1 Response
(Length;Response=(FN=00,TID[63:0],TTPID=00000000,Cert$_t$=___,RN$_t$[63:0],TPK$_t$[391:0],ECDHP[255:0],Sig$_t$[383:0])

The test pattern is passed when RN_t in Authenticate(MAM1.2 Message) equal to RN_t in the Tag MAM1.1 Response.

Authenticate(MAM1.2 Message) (CSI=06h;Length;Message=(FN=00,AuthType=00,AuthStep=001,RN$_t$[63:0],RN$_i$[63:0],TPK$_i$[391:0],Sig$_i$[383:0],MIC$_i$[255:0]))

6.3.5 Test pattern 5 utilizing ISO/IEC 18000-4:2018, 9.3.3

This pattern shall be TTP involved. It shall be applied for two modulations, O-QPSK and DBPSK.

Ready(Command code=01h; Channel number=0; Ready password=00000000h)
Authenticate(MAM1.1 Message) (CSI=06$_h$;Length;Message=(FN=00,IID[63:0],AuthType=00,AuthStep=000,TTPID=0000 0001,Cert$_i$=___,ECDHP[255:0]))

The Test pattern is passed when the response field of the tag reply to the *Authenticate* is as follows:

MAM1.1 Response
(Length;Response=(FN=00,TID[63:0],TTPID=00000001,Cert$_t$=___,RN$_t$[63:0],TPK$_t$[391:0],ECDHP[255:0],Sig$_t$[383:0])

6.3.6 Test pattern 6 utilizing ISO/IEC 18000-4:2018, 9.3.3

This pattern shall be TTP involved. It shall be applied for two modulations, O-QPSK and DBPSK.

Ready(Command code=01h; Channel number=0; Ready password=00000000h)
Authenticate(MAM1.1 Message) (CSI=06$_h$;Length;Message=(FN=00,IID[63:0],AuthType=00,AuthStep=000,TTPID=0000 0001,Cert$_i$=___,ECDHP[255:0]))
MAM1.1 Response
(Length;Response=(FN=00,TID[63:0],TTPID=00000000,Cert$_t$=___,RN$_t$[63:0],TPK$_t$[391:0],ECDHP[255:0],Sig$_t$[383:0])
Authenticate(MAM1.2 Message) (CSI=06h;Length;Message=(FN=00,AuthType=00,AuthStep=001,RN$_t$[63:0],RN$_i$[63:0],TPK$_i$[391:0],Sig$_i$[383:0],MIC$_i$[255:0],AuthRes=___))

The Test pattern is passed when the response field of the tag reply to the *Authenticate* is as follows:

MAM1.2 Response
(Length; Response=(FN=00,RN$_i$[63:0],MIC$_t$[255:0]))

6.3.7 Test pattern 7 utilizing ISO/IEC 18000-4:2018, 9.3.3

This pattern shall be TTP involved. It shall be applied for two modulations, O-QPSK and DBPSK.

Ready(Command code=01h; Channel number=0; Ready password=00000000h)
Authenticate(MAM1.1 Message) (CSI=06$_h$;Length;Message=(FN=00,IID[63:0],AuthType=00,AuthStep=000,TTPID=0000 0001,Cert$_i$=___,ECDHP[255:0]))

The Test pattern is passed when TTPID, ECDHP in the Tag MAM1.1 Response are equal to TTPID, ECDHP in *Authenticate* (MAM1.1 Message).

6.3.8 Test pattern 8 utilizing ISO/IEC 18000-4:2018, 9.3.3

This pattern shall be TTP involved. It shall be applied for two modulations, O-QPSK and DBPSK.

Ready(Command code=01h; Channel number=0; Ready password=00000000h)
Authenticate(MAM1.1 Message) (CSI=06$_h$;Length;Message=(FN=00,IID[63:0],AuthType=00,AuthStep=000,TTPID=0000 0001,Cert$_i$=___,ECDHP[255:0]))

The Test pattern is passed when RN_t in *Authenticate*(MAM1.2 Message) is equal to RN_t in the tag MAM1.1 Response.

Authenticate(MAM1.2 Message) (CSI=06h;Length;Message=(FN=00,AuthType=00,AuthStep=001,RN_t[63:0],RN_i[63:0],TPK_i[391:0],Sig_i[383:0],MIC_i[255:0],AuthRes=___))

6.3.9 Test pattern 9 utilizing ISO/IEC 18000-4:2018, 9.3.3

This Test pattern shall be executed after being authenticated successfully.

AuthComm
(Command=81h;CSI=06h;Length;Message=___,MAC[127:0],RN[15:0],CRC16[15:0])

The Test pattern is passed when the response field of the tag reply to the AuthCommis as follows:

Reply=(Header=0;Length;Response=___,MAC[127:0],RN[15:0],CRC16[15:0])

6.3.10 Test pattern 10 utilizing ISO/IEC 18000-4:2018, 9.3.3

This Test pattern shall be executed after being authenticated successfully.

SecureComm
(Command=82h;CSI=06h;Length;Message=___,MAC[127:0],RN[15:0],CRC16[15:0])

The Test pattern is passed when the response field of the tag reply to the SecureComm is as follows:

Reply=(Header=0;Length;Response=___,MAC[127:0],RN[15:0],CRC16[15:0])