INTERNATIONAL STANDARD

ISO/IEC 19823-21

First edition
2019-05

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

Part 21: Crypto suite SIMON

Technologies de l'information — Méthodes d'essai de conformité pour les suites cryptographiques des services de sécurité —

Partie 21: Suite cryptographique SIMON

Reference number
ISO/IEC 19823-21:2019(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

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 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 ISO/IEC 29167 is related to ISO/IEC 18000.

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, 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 SIMON crypto suite as standardized in ISO/IEC 29167-21.

NOTE 2 Test methods for interrogator and tag performance are covered by ISO/IEC 18046 (all parts).

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

Part 21: Crypto suite SIMON

1 Scope

This document describes methods for determining conformance to the security crypto suite defined in ISO/IEC 29167-21.

This document contains conformance tests for all mandatory functions.

The conformance parameters are the following:

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

— protocol including commands and replies,

— nominal values and tolerances.

Unless otherwise specified, the tests in this document are intended to be applied exclusively to RFID tags and interrogators defined in the ISO/IEC 18000 series using ISO/IEC 29167-21.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

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

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

ISO/IEC 29167-21:2018, *Information technology — Automatic identification and data capture techniques — Part 21: Crypto suite SIMON security services for air interface communications*

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 19762 and in ISO/IEC 29167-21 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/

4 Test methods

4.1 General

This document describes test methods for ISO/IEC 29167-21. As parts of ISO/IEC 19823 are always tested in relation to ISO/IEC 18047, duplication of information requirements and specifications is meant to be avoided.

Clause 5 defines elements that are covered in the respective part of ISO/IEC 18047.

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

4.2 By demonstration

If tests are labelled "**by demonstration**" then laboratory testing of one or (if required for statistical reasons) multiple products, processes or services is required to ensure conformance. A test laboratory that meets the requirements of 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 in this document. The detailed test plan is left to the discretion of the test laboratory.

4.3 By design

If tests are labelled "**by design**" then verification of design parameters and/or theoretical analysis is used to ensure conformance. A vendor submitting a component or system for conformance testing shall provide the necessary technical information, in the form of a technical memorandum or similar. A test laboratory shall issue a test report 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 requirements for ISO/IEC 18000-63 interrogators and tags

The mandatory requirements and applicable optional requirements of ISO/IEC 18047-6:2017, Clauses 4 and 5 shall be fulfilled.

Before a DUT is tested according to this document, it shall successfully pass ISO/IEC 18047-6:2017, Clause 7.

6 Test methods with respect to ISO/IEC 29167-21 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 6.2.

Table 1 — Test map for optional features

#	Feature	Additional requirement	To be tested for supplied product?	Test results
1	TA	Shall be tested with the Authenticate command of ISO/IEC 18000-63		
2	IA	Shall be tested with the Authenticate command of ISO/IEC 18000-63		
3	MA	Shall be tested with the Authenticate command of ISO/IEC 18000-63		
4	Secure Communication	Shall be tested with the SecureComm command of ISO/IEC 18000-63		

6.2 Crypto suite requirements

6.2.1 General

This clause refers to the requirements of ISO/IEC 29167-21.

6.2.2 Crypto suite requirements of ISO/IEC 29167-21:2018, Clauses 1 to 8 and Annexes A to C

All the requirements of ISO/IEC 29167-21:2018, Clauses 1 to 8 and Annexes A to C shall be met and conformance shall be verified by design only.

6.2.3 Crypto suite requirements of ISO/IEC 29167-21:2018, Clauses 9 to 12 and Annex E

The requirements of ISO/IEC 29167-21:2018, Clauses 9 to 12 and Annex E listed in Table 2 shall be met. This document shall be read in conjunction with ISO/IEC 29167-21 to provide a full explanation of the terms used.

Table 2 — Crypto suite requirements for ISO/IEC 29167-21

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
1	9.3.2	The Interrogator shall generate a random Interrogator challenge (IChallenge-*b*/*k*) that is carried in the TAM1 message.	M	Interrogator	By design
2	9.3.3	The Tag shall accept the TAM1 message at any time (unless occupied by internal processing and not capable of receiving messages), i.e. upon receipt of the message with valid parameters, the Tag shall abort any cryptographic protocol that has not yet been completed and shall remain in the **Initial** state.	M	Tag	By design
3	9.3.3	The Tag shall check if the Step is "00_2". If the value of Step is different, the Tag shall return a "Not Supported" error.	M	Tag	Test_Pattern 2
4	9.3.3	The Tag shall check if the RFU is "00_2". If the value of RFU is different, the Tag shall return a "Not Supported" error.	M	Tag	Test_Pattern 2

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
5	9.3.3	The Tag shall check whether the values of BlockSize and KeySize are supported by the Tag. If at least one of these checks is failed, the Tag shall return a "Not Supported" error.	M	Tag	By design
6	9.3.3	The Tag shall check whether the values of BlockSize and KeySize are supported by Key.KeyID and that Key.KeyID is authorized for use in Tag authentication. If either or both of these checks is failed, the Tag shall return a "Not Supported" error.	M	Tag	By design
7	9.3.3	The Tag shall check whether the parameter set PS is supported. If the parameter set PS is not supported, the Tag shall return a "Not Supported" error.	M	Tag	Test_Pattern 2
8	9.3.3	Assuming that the TAM1 message is successfully parsed by the Tag, the Tag shall prepare the TAM1 response.	M	Tag	By design
9	9.3.4	The Tag shall generate a random salt TRnd-*b*/*k* of length *r* bits were *r* is given for the parameter set in Table 4.	M	Tag	By design
10	9.3.4	The Tag shall use Key.KeyID and SIMON encryption to form a *b*-bit string TResponse such that TResponse = SIMON-b/k-ENC (Key.KeyID, C_TAM-*b*/*k* || TRnd-*b*/*k* || IChallenge-*b*/*k*)	M	Tag	Test_Pattern 1
11	9.3.4	The Tag shall return TResponse to the Interrogator.	M	Tag	By design
12	9.3.5	After receiving TAM1 response, the Interrogator shall use Key.KeyID to compute the *b*-bit string S where: S = SIMON-*b*/*k*-DEC (Key.KeyID, TResponse). The Interrogator shall check that S[*t*-1:0] = IChallenge-*b*/*k*.	M	Interrogator	By design
13	9.4.2	The Interrogator shall send an initial message IAM1 to the Tag prompting the Tag to start a challenge-response exchange. The Interrogator shall also indicate the variant of SIMON to be used.	O	Interrogator	By design
14	9.4.3	The Tag shall accept this message at any time (unless occupied by internal processing and not capable of receiving messages), i.e. upon receipt of the message with valid parameters, the Tag shall abort any cryptographic protocol that has not yet been completed and shall remain in the **Initial** state.	O	Tag	By design
15	9.4.3	If Interrogator authentication is not supported on the Tag, i.e. if "01_2" is not a valid value for AuthMethod, then the Tag shall return a "Not Supported" error condition.	O	Tag	By design

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
16	9.4.3	The Tag shall check if the Step is "00_2". If the value of Step is different, the Tag shall return a "Not Supported" error.	O	Tag	Test_Pattern 3
17	9.4.3	The Tag shall check if the RFU is "00_2". If the value of RFU is different, the Tag shall return a "Not Supported" error.	O	Tag	Test_Pattern 3
18	9.4.3	The Tag shall check whether the values of BlockSize and KeySize are supported by the Tag. If at least one of these checks is failed, the Tag shall return a "Not Supported" error.	O	Tag	By design
19	9.4.3	The Tag shall check whether the values of BlockSize and KeySize are supported by Key. KeyID and that Key.KeyID is authorized for use in Interrogator authentication. If at least one of these checks is failed, the Tag shall return a "Not Supported" error.	O	Tag	By design
20	9.4.3	The Tag shall check whether the value of parameter set PS is supported by the Tag. If not, the Tag shall return a "Not Supported" error.	O	Tag	Test_Pattern 3
21	9.4.3	If the IAM1 message is successfully parsed by the Tag, the Tag shall calculate the IAM1 response.	O	Tag	By design
22	9.4.4	The Tag shall generate a random challenge TChallenge-*b*/*k* of length *t* bits, where *t* is determined by the parameter set, and shall send this to the Interrogator.	O	Tag	By design
23	9.4.5	The Interrogator shall construct the IAM2 message.	O	Interrogator	By design
24	9.4.6	The Interrogator shall form a *b*-bit string IResponse such that IResponse = SIMON-*b*/*k*-DEC (Key.KeyID, C_IAM-*b*/*k* || IRnd-*b*/*k* || TChallenge-*b*/*k*). The Interrogator shall send IResponse to the Tag as part of the IAM2 message; see Table 10.	O	Interrogator	Test_Pattern 4
25	9.4.7	The Tag shall only accept the IAM2 message when the cryptographic engine is in state **PA1**.	O	Tag	By design
26	9.4.7	If Interrogator authentication is not supported on the Tag, i.e. if "01_2" is not a valid value for AuthMethod, then the Tag shall return a "Not Supported" error condition.	O	Tag	By design
27	9.4.7	The Tag shall check if the Step is "01_2". If the value of Step is different, the Tag shall return a "Not Supported" error.	O	Tag	Test_Pattern 5
28	9.4.7	The Tag shall check if the RFU is "0000_2". If the value of RFU is different, the Tag shall return a "Not Supported" error.	O	Tag	Test_Pattern 5
29	9.4.7	The Tag shall use Key.KeyID to compute the *b*-bit string S where S = SIMON-*b*/*k*-ENC (Key.KeyID, IResponse).	O	Tag	By design

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
30	9.4.7	The Tag shall check that S[t-1:0] = TChallenge-*b*/*k*.	O	Tag	By design
31	9.4.7	The Tag shall prepare IAM2 response.	O	Tag	By design
32	9.4.8	The Tag shall return the value of TStatus to the Interrogator.	O	Tag	Test_Pattern 6
33	9.4.9	If, under conditions laid out in the over-the-air protocol, there is no response from the Tag or if the returned value of TStatus is 0_2, then the Interrogator shall abandon the cryptographic protocol.	O	Interrogator	By design
34	9.5.2	The Interrogator shall generate a random Interrogator challenge (IChallenge-*b*/*k*) that is carried in the MAM1 message.	O	Interrogator	By design
35	9.5.2	The Interrogator shall indicate the variant of SIMON to be used.	O	Interrogator	By design
36	9.5.3	The Tag shall accept MAM1 message at any time (unless occupied by internal processing and not capable of receiving messages), i.e. upon receipt of the message with valid parameters, the Tag shall abort any cryptographic protocol that has not yet been completed and shall remain in the **Initial** state.	O	Tag	By design
37	9.5.3	If Mutual authentication is not supported on the Tag, i.e. if "10_2" is not a valid value for AuthMethod, then the Tag shall return a "Not Supported" error condition.	O	Tag	By design
38	9.5.3	The Tag shall check if the Step is "00_2". If the value of Step is different, the Tag shall return a "Not Supported" error.	O	Tag	Test_Pattern 7
39	9.5.3	The Tag shall check if the RFU is "00_2". If the value of RFU is different, the Tag shall return a "Not Supported" error.	O	Tag	Test_Pattern 7
40	9.5.3	The Tag shall check whether the values of BlockSize and KeySize are supported by the Tag. If at least one of these checks is failed, the Tag shall return a "Not Supported" error.	O	Tag	By design
41	9.5.3	The Tag shall check whether the values of BlockSize and KeySize are supported by Key.KeyID and that Key.KeyID is authorized for use in Interrogator-Tag mutual authentication. If at least one of these checks is failed, the Tag shall return a "Not Supported" error.	O	Tag	By design
42	9.5.3	The Tag shall check whether the value of parameter set PS is supported by the Tag. If not, the Tag shall return a "Not Supported" error.	O	Tag	By design
43	9.5.3	The Tag shall generate a random challenge TChallenge-b/k.	O	Tag	By design

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
44	9.5.3	The Tag shall construct a *b*-bit string by concatenating C_MAM-*b*/*k* with the (*b*-*t*-*c*) most significant bits of TChallenge-*b*/*k* and the entirety of IChallenge-*b*/*k*.	O	Tag	By design
45	9.5.3	The Tag shall use Key.KeyID to compute the b-bit string S where S = SIMON-*b*/*k*-ENC (Key.KeyID, C_MAM-*b*/*k* || TChallenge-*b*/*k* [*t-1*:*2t-b+c*] || IChallenge-*b*/*k*).	O	Tag	Test_Pattern 8
46	9.5.5	After receiving MAM1 Response, the Interrogator shall use Key.KeyID to compute the *b*-bit string T where: T = SIMON-*b*/*k*-DEC (Key.KeyID, TResponse[*b-1*:*0*]). 1. The Interrogator shall check that T[*t*-1:0] = IChallenge-*b*/*k*.	O	Interrogator	By design
47	9.5.6	If the cryptographic protocol has not been abandoned, the Interrogator shall form a *b*-bit string IResponse depending on the parameter set PS as follows: 1. If PS = 00_2 then IResponse is equal to SIMON-b/k-DEC (Key.KeyID, C_MAM-*b*/*k* || T[*b*-*t*-*c*-1:0] || T[*b*-*c*-1:*t*] || TResponse[*2t*+*c*-1:*b*]). 2. If PS = 01_2 then IResponse is equal to T[*b*-*c*:*t*]. The Interrogator shall set SecureComm = 0001_2 if secure communications as described in Section 10 will be used after mutual authentication is completed. Otherwise, the Interrogator shall set SecureComm = 0000_2. The Interrogator shall send IResponse and the value of SecureComm to the Tag as part of the MAM2 message.	O	Interrogator	By design
48	9.5.7	The Tag shall only accept this message when the cryptographic engine is in the state **PA2**.	O	Tag	By design
49	9.5.7	If Mutual authentication is not supported on the Tag, i.e. if "10_2" is not a valid value for AuthMethod, then the Tag shall return a "Not Supported" error condition.	O	Tag	By design
50	9.5.7	The Tag shall check if the Step is "01_2". If the value of Step is different, the Tag shall return a "Not Supported" error.	O	Tag	Test_Pattern 9
51	9.5.7	The Tag shall check if the RFU is "0000_2". If the value of RFU is different, the Tag shall return a "Not Supported" error.	O	Tag	Test_Pattern 9

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
52	9.5.7	If PS = 00_2 then the Tag computes the *b*-bit string S = SIMON-*b*/*k*-ENC (Key.KeyID, IResponse). SIMON-b/k-DEC (Key.KeyID, C_MAM-*b*/*k* $\Vert$ T[*b*-*t*-*c*-1:0] $\Vert$ T[*b*-*c*-1:*t*] $\Vert$ TResponse[2*t*+*c*-*b*-1:0]). The Tag shall check if S[*t*-1:0] = TChallenge-*b*/*k*.	O	Tag	Test_Pattern 10
53	9.5.7	If PS = 01_2, then the Tag shall check whether S = TChallenge-*b*/*k*.	O	Tag	Test_Pattern 10
54	9.5.7	If TStatus = 1_2 and SecureComm = 1_h, the Tag shall generate a random string N_T. The Tag shall further indicate using $KeyID_2$ which key shall be used for the subsequent secure communication session.	O	Tag	Test_Pattern 10
55	9.5.9	If, under conditions laid out in the over-the-air protocol, there is no response from the Tag or if the returned value of TStatus is 0_2 then the Interrogator shall abandon the cryptographic protocol.	O	Interrogator	By design
56	10.1	If the response is encapsulated, then it shall be encapsulated as described in this crypto suite. A Tag shall only encapsulate the response to an encapsulated command.	O	Tag	By design
57	10.2	If a secure communication session is required, the session shall be launched by the Interrogator after a successful mutual authentication.	O	Interrogator	By design
58	10.3.1	SEC shall only be used after mutual authentication has been established and it guarantees the confidentiality and/or authenticity of the payload P being encapsulated.	O	Interrogator Tag	By design
		To send a command as an encapsulated payload P, the Interrogator shall perform the following steps:			

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
59	10.3.2	1. The Interrogator shall verify that TStatus is 1_2. If not, the Interrogator shall abandon the encapsulation process. 2. The Interrogator shall identify the key Key. KeyID$_2$ to be used. 3. The Interrogator shall construct the initial value of the (b-16)-bit string N as N = N_T || TChallenge. 4. The Interrogator shall choose the length T_Length for the authentication token T. 5. The Interrogator shall specify if the payload is authenticated or both encrypted and authenticated. If authentication without encryption is required, then the Interrogator shall set Enc = 0. If both encryption and authentication are required, then the Interrogator shall set Enc = 1. 6. The Interrogator shall specify if the payload parameters should be protected. If parameter protection is required, then the Interrogator shall set Protect = 1. If parameter protection is not required, then the Interrogator shall set Protect = 0. 7. The Interrogator shall specify whether the Tag response is to be in the clear, authenticated, or encrypted and authenticated. 8. The Interrogator shall construct a string X where |X| = 0 or |X| = 8. If Protect = 0 then X = Ø. If Protect = 1 then X = Response || Enc || Protect || 00_2. 9. The Interrogator shall compute SEC (Key. KeyID$_2$, N, param, Enc, X || P). The output will be denoted Q || T. Depending on the value of Enc, Q will either be equal to X || P or equal to the encryption of X || P. In both cases, an authentication tag T will be included. 10. The Interrogator shall encapsulate the payload defined in Table 17 and send this to the Tag using an encapsulating over-the-air command. 11. After a successful invocation of SEC, the value of N shall be incremented by 1 using integer addition.	O	Interrogator	By design

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
60	10.3.3	To protect the reply to an encapsulated command, the Tag shall perform the following steps: 1. If the Tag is not in the state IA, then the Tag shall return a "Cryptographic Suite Error" and abandon the communication session. 2. The Tag shall process the encapsulating command as described in 10.4.1. Unless an error has been encountered, this will reveal the encapsulated command and, optionally, the values of Response, Enc, and Protect. 3. If Protect = 1_2, the Interrogator has used parameter protection. Provided the encapsulated command was processed without error (10.4.1), the values of Response, Enc, and Protect in Table 17 shall be recovered from the output of CES in 10.4.1. If Protect = 0_2, the Interrogator has not used parameter protection. The values of Response, Enc, and Protect shall be recovered from the payload in Table 17. 4. If Response = 0000_2, the Tag shall respond without encapsulation. 5. Otherwise, the Tag shall execute the encapsulated command and construct the reply R. 6. If Response = 1_x or 2_x, the Tag shall compute SEC (Key.KeyID$_2$, N, param, Enc, R) with the reply R. The value of Enc will be 0 if Response = 1_x and Enc = 1 if Response = 2_x. The output will be denoted Q || T. 7. The Tag shall return Q || T to the Interrogator instead of the unprotected reply R. 8. After a successful invocation of SEC, the value of N shall be incremented by 1 using integer addition.	O	Tag	By design

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
61	10.4.2	On receiving an encapsulating command with payload Q || T, the Tag shall perform the following steps to process the payload Q || T. 1. If the Tag is not in the state IA, then the encapsulating command shall be ignored and the Tag shall return a “Cryptographic Suite Error” and abandon the communication session. 2. The Tag shall check whether Key. KeyID$_2$ is authorized for use with secure communication. If not, the Tag shall return a "Not Supported" error. 3. The Tag shall check if param is supported by the Tag. If not, the Tag shall return a "Not Supported" error condition. 4. The Tag shall check if the value of Enc is supported by the Tag. If not, the Tag shall return a "Not Supported" error condition. 5. The Tag shall check if the RFU is "00_2". If the value of RFU is different, the Tag shall return a "Not Supported" error. 6. The Tag shall construct the initial value of N as N = N_T || TChallenge. 7. Assuming that the encapsulating command is successfully parsed by the Tag, the Tag shall recover Q || T from the encapsulating command and compute CES (Key.KeyID$_2$, N, param, Enc, Q || T). 8. If the output from CES (Key.KeyID$_2$, N, T_Length, Enc, Q || T) is AUTH_ERROR, the Tag shall return a “Cryptographic Suite Error” and abandon the communication session. 9. If the output from CES (Key.KeyID$_2$, N, T_Length, Enc, Q || T) is not AUTH_ERROR, the Tag shall consider the output to be the intended encapsulated command. 10. After a successful invocation of CES, the value of N shall be incremented by 1 using integer addition.	O	Tag	By design

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
62	10.4.3	To recover the original response from a cryptographically-protected Tag response, the Interrogator shall perform the following steps: 1. The Interrogator shall verify that the Tag response was received in response to an encapsulated command issued by the Interrogator. If not, the Interrogator shall abandon the secure communication process. 2. The Interrogator shall recover the cryptographically-protected reply Q || T from the over-the-air Tag response. 3. The Interrogator shall compute CES (Key. KeyID$_2$, N, param, Enc, Q || T). If the output is AUTH_ERROR, the Interrogator shall abandon the communication session. Otherwise, the output is the originally constructed Tag reply R. 4. After a successful invocation of CES, the value of N shall be incremented by 1 using integer addition.	O	Interrogator	By design
63	11	However, Key.j shall not be specified when there remain unspecified Key.i with i<j.	O	Tag	By design
64	11	If a Tag is unable to act on the key update command, the Tag shall return a "Not Supported" error.	O	Tag	By design
65	E.4.2	1) The *Authenticate* command shall be supported.	M	Tag	Test_Pattern 1
66	E.4.2	2) The *Challenge* command shall not be supported.	M	Tag	By design
67	E.4.2	3) The maximum execution time for an *Authenticate* Command containing a TAM1 payload shall be below 20 ms.	M	Tag	Test_Pattern 1
68	E.4.2	4) The Tag shall ignore commands from an Interrogator during execution of a cryptographic operation.	M	Tag	By design
69	E.4.2	5) The Tag shall not support sending the contents of the ResponseBuffer in the reply to an *ACK* command.	M	Tag	By design
70	E.4.2	6) The Tag shall support sending the contents of the ResponseBuffer in the reply to a *ReadBuffer* command.	M	Tag	Test_Pattern 11
71	E.4.2	8) A Tag in any cryptographic state other than Initial (*i.e.* the state after power-up) shall reset its cryptographic engine and remain in the current state upon receiving an invalid command or a command with an incorrect handle.	M	Tag	By design

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a]	MO[b]	Applies to	How verified
72	E.4.2	9) For each error condition (Annex B) defined in this crypto suite, the Tag shall do the following. — An “Unsupported Error” shall be treated as an “unsupported parameters” error in the air interface standard and shall follow the mandated actions. The Tag shall remain in its current state. — A “Cryptographic Suite Error” results in a reset of the cryptographic engine. The Tag shall remain in its current state. — Where mandated by the air interface standard, the Tag shall backscatter an error code. Otherwise, the Tag may backscatter an error code.	M	Tag	By design
73	E.4.2	10) The Tag shall remain in its current state after a Tag Authentication. The Tag shall transition to the **secured** state after successfully processing an interrogator or mutual authentication.	M	Tag	By design
74	E.4.3	In ISO/IEC 18000-63, the message to execute Tag authentication shall be transmitted to the Tag with the *Authenticate* command. The air interface shall return the response; either it shall be backscattered immediately or it shall be stored in the ResponseBuffer. It can be returned to the Interrogator from the ResponseBuffer with the *ReadBuffer* command.	M	Tag	Test_Pattern 1 and Test_Pattern 11
75	E.4.3	ISO/IEC 18000-63 specifies an 8-bit CSI. For implementation of ISO/IEC 29167-21 in ISO/IEC 18000-63, the CSI shall be expanded to the 8-bit value $0B_h$.	M	Tag	By design
76	E.4.4	ISO/IEC 29167-21 specifies several error conditions. 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 if the Tag supports specific error codes.”	M	Tag	By design
77	E.4.5	ISO/IEC 18000-63 requires the definition of key properties. If an implementation does provide key properties for a key belonging to this crypto suite, it shall set the key properties to 0000_2.	M	Tag	By design

[a] All clause, subclause and table references are to ISO/IEC 29167-21.

[b] 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

6.3.1 General

This subclause provides the test patterns for this document.

6.3.2 Test_Pattern 1

This test pattern shall be applied to all keys Key.i specified in the Tag for use with each BlockSize *b* and KeySize *k* supported by the Tag.

NOTE 1 The size of IChallenge-*b*/*k* depends on *b* and *k* and the value in Test_Pattern 1 is fixed to all ones. Mathematically, this is the |IChallenge-b/k|-bit binary representation of the integer value $2^{|\text{IChallenge-b/k}|}$-1.

NOTE 2 All fields with a variable value for different *b* and *k* are identified solely by name. The appropriate values are given in ISO/IEC 29167-21. Fields that take a value that is common to all variants of *b* and *k* are identified by value.

```
Query (Tari=6,25µs; BLF=640; FM0, S0)
ACK
Req_RN
Authenticate {
SenRep=0b1; IncRepLen=0b0; CSI=0x0B; Length; Message=(AuthMeth=0b00; Step=0b00; RFU=0b00;
BlockSize; KeySize; KeyID=i; PS=0b00; IChallenge-b/k=2^|IChallenge-b/k|-1)
}
```

The test pattern is passed when the decrypted response field to the Authenticate command is as follows:

(C_TAM=b/k; TRnd-b/k=any value; I) with I=$2^{|\text{IChallenge-b/k}|}$-1.

6.3.3 Test_Pattern 2

This test pattern shall be applied to all keys Key.i specified in the Tag for use with each BlockSize *b* and KeySize *k* supported by the Tag. In each case, the five cases shall be tested with parameters taking the values indicated in Table 3.

Table 3 — Parameter values for Test_Pattern 2

AuthMeth	Step	RFU	BlockSize indicator	KeySize indicator	KeyID	PS
0b00	0b01	0b00	As required for *b*	As required for *k*	i	0b00
0b00	0b00	0b01	As required for *b*	As required for *k*	i	0b00
0b00	0b00	0b00	As required for *b*	As required for *k*	i	0b01
0b00	0b00	0b00	As required for *b*	As required for *k*	j (where Key.j is the first unassigned key)	0b00

NOTE 1 The size of IChallenge-*b*/*k* in the test pattern depends on *b* and *k* and the value in Test_Pattern 2 is fixed to all ones. Mathematically, this is the |IChallenge-b/k|-bit binary representation of the integer value $2^{|\text{IChallenge-b/k}|}$-1.

NOTE 2 All fields with a variable value for different *b* and *k* are identified solely by name. The appropriate values are given in ISO/IEC 29167-21 or in Table 3. The value of fields that take a value common to all variants of *b* and *k* are identified by Table 3.

```
Query (Tari=6,25µs; BLF=640; FM0, S0)
ACK
Req_RN
Authenticate {
   SenRep=0b1; IncRepLen=0b0; CSI=0x0B; Length; Message=(AuthMeth; Step; RFU; BlockSize;
KeySize; KeyID; PS; IChallenge-b/k=2^|IChallenge-b/k|-1)
   }
```

The test pattern is passed when the Tag returns a “Not Supported” error in all cases.

6.3.4 Test_Pattern 3

This test pattern shall be applied to all keys Key.i specified in the Tag for use with each BlockSize *b* and KeySize *k* supported by the Tag. Each case shall be tested with parameters taking the values indicated in Table 4.

Table 4 — Parameter values for Test_Pattern 3

AuthMeth	Step	RFU	BlockSize indicator	KeySize indicator	KeyID	PS
0b01	0b01	0b00	As required for *b*	As required for *k*	i	0b00
0b01	0b00	0b01	As required for *b*	As required for *k*	i	0b00
0b01	0b00	0b00	As required for *b*	As required for *k*	i	0b01
0b01	0b00	0b00	As required for *b*	As required for *k*	j (where Key.j is the first unassigned key)	0b00

NOTE 1 The size of IChallenge-*b/k* in the test pattern depends on *b* and *k* and the value in Test_Pattern 3 is fixed to all ones. Mathematically, this is the |IChallenge-b/k|-bit binary representation of the integer value $2^{|\text{IChallenge-b/k}|}$-1.

NOTE 2 All fields with a variable value for different *b* and *k* are identified solely by name. The appropriate values are given in ISO/IEC 29167-21 or in Table 4. The value of fields that take a value common to all variants of *b* and *k* are identified by Table 4.

```
Query (Tari=6,25µs; BLF=640; FM0, S0)
ACK
Req_RN
Authenticate {
   SenRep=0b1; IncRepLen=0b0; CSI=0x0B; Length; Message=(AuthMeth; Step; RFU; BlockSize;
KeySize; KeyID; PS; IChallenge-b/k=2|IChallenge-b/k|-1)
   }
```

The test pattern is passed when the Tag returns a “Not Supported” error in all cases.

6.3.5 Test_Pattern 4

This test pattern shall be applied to all keys Key.i specified in the Tag for use with each BlockSize *b* and KeySize *k* supported by the Tag.

NOTE 1 The sizes of IRnd-*b/k* and TChallenge-*b/k* depend on *b* and *k*. Since TChallenge-*b/k* is generated on the Tag, its value cannot typically be specified. However, TChallenge-*b/k* is transported in the clear over-the-air and can be available for testing. Depending on the Interrogator implementation, it can be possible to specify the value of IRnd-*b/k*. The value of IRnd-*b/k* for this test pattern can be set to all ones. Mathematically, this would be the |IRnd-b/k|-bit binary representation of the integer value $2^{|\text{IRnd-b/k}|}$-1.

NOTE 2 All fields with a variable value for different *b* and *k* are solely identified by name. The appropriate values are given in ISO/IEC 29167-21. Fields that take a value that is common to all variants of *b* and *k* are identified by value.

```
Query (Tari=6,25µs; BLF=640; FM0, S0)
ACK
Req_RN
Authenticate {
   SenRep=0b1; IncRepLen=0b0; CSI=0x0B; Length; Message=(AuthMeth=0b01; Step=0b00;
RFU=0b00; BlockSize; KeySize; KeyID=i; PS=0b00)
    }
Authenticate {
   SenRep=0b1; IncRepLen=0b0; CSI=0x0B; Length; Message=(AuthMeth=0b01; Step=0b01;
RFU=0b0000; IResponse)
   }
```

The test pattern is passed when the encryption of IResponse is as follows:

(C_IAM=b/k; IRnd-b/k=any value; T) with T = TChallenge-b/k.

6.3.6 Test_Pattern 5

This test pattern shall be applied to all keys Key.i specified in the Tag for use with each BlockSize *b* and KeySize *k* supported by the Tag. Each case shall be tested with parameters taking the values indicated in Table 5.

Table 5 — Parameter values for Test_Pattern 5

AuthMeth	Step	RFU	BlockSize indicator	KeySize indicator	KeyID	PS
0b01	0b00	0b0000	As required for *b*	As required for *k*	I	0b00
0b01	0b01	0b0001	As required for *b*	As required for *k*	I	0b00

NOTE 1 The size of IResponse in the test pattern depends on *b*. The value for Test_Pattern 5 can be fixed to all binary ones. Mathematically, this would be the b-bit binary representation of the integer value 2^b-1.

NOTE 2 All fields with a variable value for different *b* and *k* are identified solely by name. The appropriate values are given in ISO/IEC 29167-21 or in Table 5. Fields that take a value that is common to all variants of *b* and *k* are identified by value.

```
Query (Tari=6,25µs; BLF=640; FM0, S0)
ACK
Req_RN
Authenticate {
   SenRep=0b1; IncRepLen=0b0; CSI=0x0B; Length; Message=(AuthMeth=0b01;  Step=0b00;
RFU=0b00; BlockSize; KeySize; KeyID=i; PS=0b00)
   }
Authenticate {
   SenRep=0b1; IncRepLen=0b0; CSI=0x0B; Length; Message=(AuthMeth=0b01; Step; RFU;
IResponse)
   }
```

The test pattern is passed when the Tag returns a “Not Supported” error in all cases.

6.3.7 Test_Pattern 6

This test pattern shall be applied to all keys Key.i specified in the Tag for use with each BlockSize *b* and KeySize *k* supported by the Tag.

NOTE 1 The sizes of IRnd-*b*/*k* and TChallenge-*b*/*k* depend on *b* and *k*. Since TChallenge-*b*/*k* is generated on the Tag, its value cannot typically be specified. However, TChallenge-*b*/*k* is transported in the clear and can be available for testing. Depending on the Interrogator implementation, it can be possible to specify the value of IRnd-*b*/*k*. The value of IRnd-*b*/*k* for this test pattern can be set to all binary ones. Mathematically, this would be the |IRnd-b/k|-bit binary representation of the integer value $2^{|IRnd\text{-}b/k|}$-1.

NOTE 2 All fields with a variable value for different *b* and *k* are solely identified by name. The appropriate values are given in ISO/IEC 29167-21. Fields that take a value that is common to all variants of *b* and *k* are identified by value.

```
Query (Tari=6,25µs; BLF=640; FM0, S0)
ACK
Req_RN
Authenticate {
   SenRep=0b1; IncRepLen=0b0; CSI=0x0B; Length; Message=(AuthMeth=0b01; Step=0b00;
RFU=0b00; BlockSize; KeySize; KeyID=i; PS=0b00)
   }
Authenticate {
   SenRep=0b1; IncRepLen=0b0; CSI=0x0B; Length; Message=(AuthMeth=0b01; Step=0b01;
```