INTERNATIONAL STANDARD

ISO/IEC 19823-19

First edition
2018-09

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

Part 19: Crypto suite RAMON

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

Partie 19: Suite cryptographique RAMON

Reference number
ISO/IEC 19823-19:2018(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. 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.

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

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

ISO/IEC 19823 describes the conformance test methods for security service crypto suites. ISO/IEC 19823 is related to ISO/IEC 18047, 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 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 RAMON crypto suite as standardized in ISO/IEC 29167-19.

NOTE 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 19: Crypto suite RAMON

1 Scope

This document describes test methods for determining the conformance of security crypto suites with the specifications given in ISO/IEC 29167-19.

This document contains conformance tests for all mandatory and 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 exclusively applicable in relation to RFID tags and interrogators defined in the ISO/IEC 18000 series using a reference to this document.

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 18000-63:2015, *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 29167-19:2016, *Information technology — Automatic identification and data capture techniques — Part 19: Crypto suite RAMON security services for air interface communications*

3 Terms, definitions, symbols and abbreviated terms

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

Clause 4 describes the general test methods for ISO/IEC 29167-19. As the parts of ISO/IEC 19823 are always tested in relation to ISO/IEC 18047, 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. They may only be defined in ISO/IEC 19823 if ISO/IEC 18047 does not define them, 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

Laboratory testing of one, or (if required for statistical reasons) multiple, products, processes or services to ensure conformance. A laboratory 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 laboratory.

4.3 By design

Design parameters and/or theoretical analysis that ensure conformance. A vendor submitting a component or system for conformance testing shall provide the necessary technical information, in the form of a technical memorandum or similar. A laboratory shall approve the technical analysis as being sufficient to ensure conformance of the component or system.

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

5 Test methods with respect to ISO/IEC 18000 parts

5.1 Test requirements for ISO/IEC 18000-63 interrogators and tags

Interrogators and tags tested according this document shall be based on ISO/IEC 18000-63. Test requirements for ISO/IEC 18000-63 interrogators and tags shall be as specified in ISO/IEC 18047-6:2017, Clauses 4 and 5.

Before a DUT is tested according to this document, it shall meet the requirements of ISO/IEC 18047-6:2017, Clause 8.

5.2 Test requirements for other parts of ISO/IEC 18000

Currently there are no test methods defined for other parts of ISO/IEC 18000.

6 Test methods with respect to ISO/IEC 29167-19 interrogators and tags

6.1 Test map for optional features

Interrogators and tags tested according this document shall be based on ISO/IEC 29167-19. 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 Table 2.

Table 1 — Test map for optional features

#	Feature	Additional requirement	Mark items to be tested for supplied product	Test results
1	Mutual authentication	Shall be tested with the authenticate command of the declared ISO/IEC 18000 part		
2	Secure communication	Shall be tested with the authenticate command of the declared ISO/IEC 18000 part		
3	Key update	Shall be tested with the authenticate command of the declared ISO/IEC 18000 part		
4	Number of keys supported			
5	Key length supported by the tag			

Table 2 lists all crypto suite requirements that shall be tested in dependence of the features of Table 1 as supported by the DUT.

6.2 Crypto suite requirements

Table 2 — Crypto suite requirements

Item	Protocol subclause[a]	Requirement[a,b]	M/O/PRM/CRM[c]	Applies to	How to verify
1	6.2.1	The Interrogator shall compare its generated Interrogator challenge with the challenge it received from the Tag. If the values match, the Tag is identified.	M	Interrogator	By demonstration using Test Pattern 12 and Test Pattern 14
2	6.2.1	If the Tag provides a signature along with the SID, the Interrogator shall validate the signature using the signature verification key. If successful, the Tag is authenticated.	M	Interrogator	By design
3	6.5	The IID shall remain constant during a session.	M	Interrogator	By design
4	6.5	The SID of a Tag shall be set during personalization and shall remain constant throughout the lifetime of the Tag.	M	Tag	By design
5	6.5	The SID and the optional signature are secret information and shall never be readable for an unauthorized reader.	M	Tag	By design
6	6.5	The SID shall never be sent in plaintext.	M	Tag	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
7	6.5	The Tag shall not perform signature generation or verification, nor shall it store the corresponding keys.	M	Tag	By design
8	6.5	The Tag shall store the SID and the public key K_E for Tag authentication in its memory.	M	Tag	By design
9	6.5	The Tag shall store the SID along with its signature in its memory.	O	Tag	By design
10	6.5	The memory locations storing the SID and the secret keys shall not be readable for any Interrogator after having written these values once during production of the Tag.	M	Tag	By design
11	6.5	The Interrogator shall have access to the RAMON decryption key K_D to be able to decrypt the authentication message sent by the Tag.	M	Interrogator	By design
12	6.5	The Interrogator shall have access to a list of valid SIDs; each SID might have a signature attached to it.	M	Interrogator	By design
13	6.6	The length of the keys used for Tag identification shall be as specified in Table 4.	M	Tag, Interrogator	By design
14	6.6	The length of the keys used for mutual authentication and secure communication shall be as specified in Table 5.	M	Tag, Interrogator	By design
15	8.1	A Tag shall support at least one of two authentication protocol modes, the partial result mode or the complete result mode.	M	Tag	By design
16	8.1	Interrogators shall support both protocol modes.	M	Interrogator	By demonstration using Test Pattern 12 and 13
17	8.1	The complete result mode shall require the capability of the interface standard to handle long timeouts or to signalize the interrogator that a tag is still processing a command.	M	Interrogator, Tag	By design
18	8.1	In partial result mode, a sequence of Authenticate commands shall be sent to the Tag in order to complete the full authentication protocol.	M	Interrogator, Tag	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
19	8.1	A Tag receiving a command with incorrect AuthMethod or Step fields shall respond either with an "insufficient privileges" or an "other error" error code. The crypto suite shall transit to the **Init** state.	M	Tag	By demonstration using Test Pattern 3 and Test Pattern 4
20	8.1	An Interrogator receiving a Tag's response with incorrect AuthMethod or Step fields shall reset the Tag and try to restart the communication.	M	Interrogator	By design
21	8.2	All Authenticate commands for Tag identification shall use AuthMethod = 11b in accordance with 10.3.	M	Tag	By demonstration using Test Pattern 1 or Test Pattern 2
22	8.2.1	The crypto suite state transitions for Tag identification in partial result mode shall be as specified in Figure 4.	M	Interrogator, Tag	By design
23	8.2.2	The crypto suite state transitions for Tag identification in complete result mode shall be as specified in Figure 5.	M	Interrogator, Tag	By design
24	8.2.2	In case of failure during one of the steps of the protocol, the crypto suite transits to the **Init** state.	M	Tag	By design
25	10.1	The sequence of messages exchanged for Tag identification in partial result mode shall be as depicted in Figure 8.	M	Interrogator, Tag	By design
26	10.1	The sequence of messages exchanged for Tag identification in complete result mode shall be as depicted in Figure 9.	M	Interrogator, Tag	By design
27	10.1.1	In Step 1 of the partial result mode, the Interrogator message shall include a random challenge to request the Tag to send its identification data.	M	Interrogator	By design
28	10.1.1	Upon reception of this message, the Tag shall start calculating the response.	PRM	Tag	By design
29	10.1.1	The first response of the Tag shall be the total length of the identification cryptogram.	PRM	Tag	By design
30	10.1.1	In Step 2 of the partial result mode, the Interrogator shall retrieve the fragments of the Tag's identification cryptogram by chaining further Authenticate commands and responses.	M	Interrogator	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
31	10.1.2	In complete result mode, the first and only Interrogator message shall include a random challenge.	M	Interrogator	By design
32	10.1.2	The Tag shall transmit the identification data to the reader and shall set the remaining bytes to zero.	CRM	Tag	By design
33	10.3.1	The coding of the Message field for Tag Identification, AuthMethod 3, Step 1 shall be as specified in Table 7. This message transmits the Interrogator Challenge to the Tag.	M	Interrogator	By design
34	10.3.1	KeySelect shall allow selecting one key (K_E) out of a number of keys.	M	Interrogator	By design
35	10.3.1	If only one key is supported, KeySelect shall be 00h.	M	Interrogator	By design
36	10.3.1	If the selected key is not available on the Tag, it shall respond with a "Not supported" error code and transit to **Init** state.	M	Tag	By demonstration using Test Pattern 5
37	10.3.1	MRead shall be set to "0000b" for Tag identification.	M	Interrogator, Tag	By design
38	10.3.1	An Interrogator shall set all RFU bits of the message field to "0".	M	Interrogator	By design
39	10.3.1	A Tag receiving a Message field with RFU bits set other than "0" shall respond with a "Not supported" error code and transit to **Init** state.	M	Tag	By design
40	10.3.1	A Tag using partial result mode shall require additional commands to transmit the partial result.	PRM	Tag	By design
41	10.3.1	The coding of the Message field in state **TAM1.1** and **TAM1.2** for AuthMethod 3, Step 2 shall be as specified in Table 8.	M	Interrogator	By design
42	10.3.1	An Interrogator shall set all RFU bits of the message field to "0".	M	Interrogator	By design
43	10.3.1	A Tag receiving a Message field with RFU bits set other than "0" shall respond with a "Not supported" error code and transit to **Init** state.	PRM	Tag	By design
44	10.4	The Tag shall send a response message to each Authenticate command.	M	Tag	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
45	10.4.1.1	In partial result mode, the first Tag response shall indicate the overall length of response data and shall not carry any bytes of the response data itself.	PRM	Tag	By design
46	10.4.1.1	The subsequent response messages shall transmit fragments of the response data in consecutive order.	PRM	Tag	By design
47	10.4.1.1	Each response message shall indicate the remaining number of bytes to be transmitted.	PRM	Tag	By design
48	10.4.1.1	The coding of the Tag response field for Tag Identification, AuthMethod 3 Step 1, shall be as defined in Table 11.	PRM	Tag	By design
49	10.4.1.1	A Tag shall set all RFU bits of the Tag Response field in step 1 to "0".	PRM	Tag	By design
50	10.4.1.1	An Interrogator receiving an Authenticate Response field with RFU bits set other than "0" shall ignore the RFU bits and try to continue communication with the Tag.	M	Interrogator	By design
51	10.4.1.1	An Interrogator receiving a response frame formatted as shown in Table 11 shall continue with Authenticate commands for AuthMethod 3 with payload for Step 2.	M	Interrogator	By design
52	10.4.1.1	The coding of the Tag response field for Tag Identification, AuthMethod 3, Step 2 shall be as specified in Table 12.	PRM	Tag	By design
53	10.4.1.1	If the Tag receives the first Authenticate command for AuthMethod 3 Step 2, it shall process the command, send the response, transit from state **TAM1.1** into state **TAM1.2** and remain in **TAM1.2** as long as there are identification data bytes remaining to be sent and no error occurred.	PRM	Tag	By demonstration using Test Pattern 2
54	10.4.1.1	The response data shall be calculated in consecutive order.	PRM	Tag	By design
55	10.4.1.1	The Tag shall indicate the remaining number of bytes to be fetched in the Remaining Length field.	PRM	Tag	By design
56	10.4.1.1	The Remaining Length encoded to 000h shall indicate that this is the last fragment.	PRM	Tag	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
57	10.4.1.1	A Tag shall set all RFU bits of the Tag Response field in step 2 to "0".	PRM	Tag	By design
58	10.4.1.1	An Interrogator receiving an Authenticate Response field with RFU bits set other than "0" shall ignore the RFU bits and try to continue communication with the Tag.	M	Interrogator	By design
59	10.4.1.2	In complete result mode, the Tag shall transmit the whole response data in a single response after it has finished the calculation and transit to state **TAM1.3**.	CRM	Tag	By demonstration using Test Pattern 1
60	10.4.1.2	The format of the response field for the complete result mode shall be as specified in Table 12.	CRM	Tag	By design
61	10.4.1.2	In complete result mode, a Tag shall set the *Remaining Length* field to "000h" to indicate that this is the only and complete response.	CRM	Tag	By design
62	10.4.1.2	The response data fragment shall contain the complete RAMON cryptogram, consisting of 128 Byte.	M	Tag	By design
63	10.4.3	A Tag that encounters an error during the execution of a cryptographic suite operation shall send an error reply to the Interrogator.	M	Tag	By design
64	10.5	An Interrogator shall check the Step and the Remaining Length field in the Tags response to determine between complete- and partial response mode.	M	Interrogator	By design
65	A	Any combination of Start States and Transitions for Tag identification in partial result mode not listed in Table A.1 shall result in an error and consequently a transition to the **Init** state.	PRM	Tag	By design
66	A	Any combination of Start States and Transitions for Tag identification in complete result mode not listed in Table A.2 shall result in an error and consequently a transition to the **Init** state.	CRM	Tag	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
67	B	A Tag that encounters an error during the execution of a cryptographic suite operation shall send an error reply to the Interrogator.	M	Tag	By design
68	B	The details of these error replies shall be as defined in the respective air interface standards.	M	Tag	By design
69	C.1	The RAMON authentication cryptogram shall be composed from the components specified in Table C.1.	M	Tag	By design
70	C.1	The SID, the signature and the random filling bytes shall be encoded as TLV structure to facilitate the decomposition by the interrogator.	M	Tag	By design
71	C.1	The coding of TLV-fields in the authentication message shall be as specified in Table C.2.	M	Tag	By design
72	C.1	If the optional signature is not present, its TLV structure shall be omitted completely.	M	Tag	By design
73	C.1	A Random filling and a final zero-byte shall be appended to the authentication message to yield a total size of 128 bytes.	M	Tag	By design
74	C.1	If only two bytes are left for the TLV coded random filling, the coding shall be C8h 00h.	M	Tag	By design
75	C.1	If only one byte is left for the TLV coded random filling, the coding shall be 00h.	M	Tag	By design
76	C.1.2	The Tag shall insert additional TLV-fields into the authentication message if the RAMON encryption is used to read out sensor data and/or other dynamic information.	O	Tag	By design
77	C.1.2	The coding of additional TLV-fields shall be as specified in Table C.5.	O	Tag	By design
78	E.1	For the implementation of the RAMON crypto suite, an air interface protocol shall support the required security commands that this crypto suite has implemented.	M	Interrogator, Tag	By design
79	E.1	Security commands shall contain a message field with parameters for the crypto suite.	M	Interrogator	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
80	E.1	A reply of a Tag contains a response field with the data returned by the crypto suite.	M	Tag	By design
81	E.1	The Crypto Suite Identifier (CSI) for this crypto suite shall be defined as the 6-bit value 001001_2 and it is expanded to the 8-bit value 09_h.	M	Interrogator, Tag	By design
82	E.1	This crypto suite shall support the security services which are defined in Table E.1.	M	Interrogator, Tag	By design
83	E.5	A Crypto Suite supporting ISO/IEC 18000-63 shall fulfil the protocol security command requirements as defined in E.5.	M	Interrogator, Tag	By design
84	E.5	For Tag Authentication, the Authenticate command shall be supported.	M	Interrogator, Tag	By demonstration using Test Pattern 1 or Test Pattern 2
85	E.5	For Tag Authentication, the Challenge command may be supported.	O	Interrogator, Tag	By demonstration using Test Pattern 7
86	E.5	The execution time for an authentication shall be below 1 minute.	M	Tag	By demonstration using Test Pattern 1 or Test Pattern 2
87	E.5	The Tag shall ignore commands from an Interrogator during execution of a cryptographic operation.	M	Tag	By design
88	E.5	The Tag shall support sending the contents of the response buffer in the reply to an ACK command.	M	Tag	By demonstration using Test Pattern 8
89	E.5	The Tag shall support sending the contents of the response buffer in the reply to a READ_BUFFER command.	M	Tag	By demonstration using Test Pattern 6
90	E.5	The tag may support a security timeout following a crypto error. The length of the timeout shall be defined by the tag manufacturer, depending on the application profile.	O	Tag	By design
91	E.5	A Tag in any cryptographic state other than **Initial** shall reset its cryptographic engine and transition to the **Open** state upon receiving an invalid command (Invalid command means crypto commands with incorrect handle or CRC error).	M	Tag	By design
92	E.5	For each Error Condition defined in the Cryptographic Suite, the Tag shall remain in its current state.	M	Tag	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
93	E.5	The Tag shall remain in its current state after a Tag Authentication.	M	Tag	By design
94	E.5	The KeyUpdate command may be supported.	O	Interrogator, Tag	By design
95	E.5	The KeyUpdate command shall be encapsulated.	O	Interrogator, Tag	By design
96	E.6.2	In complete result mode, a Tag supporting ISO/IEC 18000-63 shall send an In-Process reply, using Barkers to indicate to the Interrogator that the Tag is still working (see Figure E.2).	M	Tag	By design
97	E.7	The error conditions of the crypto suite shall be returned to the Interrogator as error codes for the air interface.	M	Tag	By design
98	E.7.4	The conversion of error conditions in the crypto suite to ISO/IEC 18000-63 error codes shall be as specified in Table E.2.	M	Tag	By design
99	F.1	To provide non traceability, a Tag may provide an Untraceable command as defined in ISO/IEC 18000-63:2015, 6.3.2.12.3.16.	O	Tag	By demonstration using Test Pattern 9
100	F.1	A session access password, provided within the TLV structure received at Tag Authentication (see C.1.2), shall be used to transit the Tag into the Secured State.	O	Tag	By design
101	F.1	The session password shall be valid only one time to avoid replay attacks.	O	Tag	By design
102	F.1	To provide non traceability, a Tag may use a partly hidden EPC/TID or a randomized EPC/TID as described in F.1.1 and F.1.2.	O	Tag	By design
103	F.1.1	Instead of the EPC, the SID shall be used by the Interrogator to uniquely identify the Tag.	O	Interrogator	By design
104	F.1.1	A portion of the Tag's EPC shall be set to a random value that is updated at each power-on.	O	Tag	By demonstration using Test Pattern 10

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
105	F.1.1	The StoredCRC shall be updated at each power-on.	O	Tag	By demonstration using Test Pattern 10
106	F.1.2	A portion of the Tag's MCS serial number shall be set to a random value that is updated at each power-on.	O	Tag	By demonstration using Test Pattern 11

[a] Unless otherwise specified, any reference made in these columns is to ISO/IEC 29167-19:2016.

[b] Any reference made to states of the cryto engine are in bold letters.

[c] M: mandatory; O: optional; PRM: mandatory for partial result mode; CRM: mandatory for complete result mode. Items marked with M are mandatory and shall be tested for each DUT.

6.3 Test patterns

Test_Pattern 1 (Tag)

```
Query (Tari = 12,5µs; BLF=320; Miller4, S0)
ACK
Req_RN
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b11,Step=
0b01,MRead=0x0,RFU=0x00,KeySelect=0x00,InterrogatorChallenge=0x31297EF
6E1EEE0F742C65DA9BFE015F5)
```

The Tag shall operate in the complete result mode. The RAMON decryption key used by the test system shall match with the selected decryption key of the Tag. The test pattern passed if the decrypted response field of the Tag reply to Authenticate is as follows:

```
AuthMeth=0b11;Step=0b10;RFU=0x00;Response Data=(InterrogatorChallenge0
x31297EF6E1EEE0F742C65DA9BFE015F5;TagRandomNumber;TLV_record,
ZeroPadding=0x00);RFU=0x00;Remaining Length=0x000
```

If the processing time of the Authenticate command exceeds 20 ms, the Tag shall backscatter a processing notification, at least every 20 ms. The execution time of the complete sequence shall be below 1 min.

Test_Pattern 2 (Tag)

```
Query (Tari = 12,5µs; BLF=320; Miller4, S0)
ACK
Req_RN
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b11,Step=
0b01,MRead=0x0,RFU=0x00,KeySelect=0x00,InterrogatorChallenge=0x31297EF
6E1EEE0F742C65DA9BFE015F5)
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b11,Step=
0b10,RFU=0x00)
```

The Tag shall operate in the partial result mode. The RAMON decryption key used by the test system shall match with the selected decryption key of the Tag. The last Authenticate command has to be repeated until the entire identification data is fetched. The response field of the Tag reply to the first Authenticate shall be as follows:

```
AuthMeth=0b11;Step=0b01;RFU=0x00;Remaining Length
```

The Remaining Length parameter shall provide the total length of response data. For each further Authenticate command, the response field shall be as follows:

```
AuthMeth=0b11;Step=0b10;RFU=0x00;Fragment_of_Response_Data;RFU=0x00;
Remaining Length
```

The Remaining Length parameter shall provide the remaining length of response data. The decrypted response data shall be as follows:

```
Response_Data=(InterrogatorChallenge0x31297EF6E1EEE0F742C65DA9BFE015F5;
TagRandomNumber;TLV_record,ZeroPadding=0x00)
```

The execution time of the complete sequence shall be below 1 min.

Test_Pattern 3 (Tag)

```
Query (Tari = 6,25µs; BLF=640; FM0, S0)
ACK
Req_RN
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b00,Step=
0b01,MRead=0x0,RFU=0x00,KeySelect=0x00,InterrogatorChallenge=0x31297EF
6E1EEE0F742C65DA9BFE015F5)
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b01,Step=
0b01,MRead=0x0,RFU=0x00,KeySelect=0x00,InterrogatorChallenge=0x31297EF
6E1EEE0F742C65DA9BFE015F5)
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b10,Step=
0b01,MRead=0x0,RFU=0x00,KeySelect=0x00,InterrogatorChallenge=0x31297EF
6E1EEE0F742C65DA9BFE015F5)
```

The test pattern passed if the Tag returns an error message to all Authenticate commands using either an “insufficient privileges” or an “other error” error condition.

Test_Pattern 4 (Tag)

```
Query (Tari = 12,5µs; BLF=320; Miller4, S0)
ACK
Req_RN
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b11,Step=
0b00,MRead=0x0,RFU=0x00,KeySelect=0x00,InterrogatorChallenge=0x31297EF
6E1EEE0F742C65DA9BFE015F5)
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b11,Step=
0b10,MRead=0x0,RFU=0x00,KeySelect=0x00,InterrogatorChallenge=0x31297EF
6E1EEE0F742C65DA9BFE015F5)
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b11,Step=
0b11,MRead=0x0,RFU=0x00,KeySelect=0x00,InterrogatorChallenge=0x31297EF
6E1EEE0F742C65DA9BFE015F5)
```

The test pattern passed if the Tag returns an error message to all Authenticate commands using either an “insufficient privileges” or an “other error” error condition.

Test_Pattern 5 (Tag)

```
Query (Tari = 12,5µs; BLF=320; Miller4, S0)
ACK
Req_RN
Authenticate
(SenRep=0b1;IncRepLen=0b0;CSI=0x09;Length;Message=(AuthMeth=0b11,Step=
0b01,MRead=0x0,RFU=0x00,KeySelect,InterrogatorChallenge=0x31297EF6E1EE
E0F742C65DA9BFE015F5)
```

The selected key shall not be available on the Tag. The test pattern passed when the Tag returns an error message using a “Not supported” error condition.

Test_Pattern 6 (Tag)

```
Query (Tari = 12,5µs; BLF=320; Miller2, S0)
ACK
Req_RN
```