INTERNATIONAL STANDARD

ISO/IEC 19823-13

First edition
2018-04

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

Part 13: Cryptographic Suite Grain-128A

Technologies de l'information — Conformance test methods for security service crypto suites —
Partie 13: Suite cryptographique Grain-128A

Reference number
ISO/IEC 19823-13:2018(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 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.

Introduction

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

The ISO/IEC 19823 series of standards describes the conformance test methods for security service crypto suites. The ISO/IEC 19823 series is related to the ISO/IEC 18047 series of standards, which describes the radio frequency identification device conformance test methods, in the same way as ISO/IEC 29167 series is related to the ISO/IEC 18000 series.

These relations mean that for a product that is claimed to be compliant to a pair of ISO/IEC 18000-n and ISO/IEC 29167-m then the test methods of ISO/IEC 18047-n and ISO/IEC 19823-m apply. If a product supports more than one part of ISO/IEC 18000 or ISO/IEC 29167, all related parts of ISO/IEC 18047 and ISO/IEC 19823 apply.

NOTE 1 The conformance test requirements of ISO/IEC 18000-6, ISO/IEC 18000-61, ISO/IEC 18000-62, ISO/IEC 18000-63, ISO/IEC 18000-64 are currently all in ISO/IEC 18047-6.

This document describes the test methods for the Grain-128A crypto suite as standardized in ISO/IEC 29167-13.

NOTE 2 Test methods for interrogator and tag performance are covered by the multiple parts of ISO/IEC 18046.

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

Part 13: Cryptographic Suite Grain-128A

1 Scope

This document describes test methods for determining the conformance of security crypto suites with the specifications given in ISO/IEC 29167-13.

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; and

— nominal values and tolerances.

Unless otherwise specified, the tests in this document are applied exclusively to RFID tags and interrogators defined in the ISO/IEC 18000 series using ISO/IEC 29167-13.

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 18000-62, *Information technology — Radio frequency identification for item management — Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B*

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 29167-13:2015, *Information technology — Automatic identification and data capture techniques — Part 13: Crypto suite Grain-128A security services for air interface communications*

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

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 (all parts) and ISO/IEC 29167-13 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

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

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

3.2 Symbols and abbreviated terms

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

4 Test methods

4.1 General

This Clause describes the general test methods for ISO/IEC 29167-13. As the parts of ISO/IEC 19823 are always tested in relation with 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 parts and therefore shall not be addressed in an ISO/IEC 19823 part. Only if ISO/IEC 18047 does not define them, then they may be defined in ISO/IEC 19823, although a revision of ISO/IEC 18047 should be the preferred option.

Clause 6 defines elements that are not expected to be covered by ISO/IEC 18047 and these 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 compliance. A test laboratory that meets ISO/IEC 17025 shall perform the indicated testing to ensure conformance of the component or system.

For Protocol requirements that are verified **by demonstration**, the test conditions are specified by this document. The detailed test plan is at the discretion of the test laboratory.

4.3 By design

Design parameters and/or theoretical analysis that ensure compliance. A vendor submitting a component or system for compliance testing shall provide the necessary technical information, in the form of a technical memorandum or similar. A test laboratory shall issue a test certificate indicating whether the technical analysis was sufficient to ensure conformance of the component or system.

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

5 Test methods in respect to the ISO/IEC 18000 parts

5.1 Test requirements for ISO/IEC 18000-62 interrogators and tags

The following mandatory requirements and applicable optional requirements of ISO/IEC 18047-6:2017 shall be fulfilled:

— Clause 4 Default conditions applicable to the test methods;

— Clause 5 Setup of test equipment.

Before a DUT is tested according this document it shall successfully pass the following of ISO/IEC 18047-6:2017:

— Clause 7 Conformance tests for ISO/IEC 18000-62.

6 Test methods in respect to the ISO/IEC 29167-13 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 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	Mark items to be tested for supplied product	Test results
1	TA	Shall be tested with the authenticate command of the declared ISO/IEC 18000 part		
2	IA	Shall be tested with the authenticate command of the declared ISO/IEC 18000 part		
3	Secure Authenticated Communication	Shall be tested with the SecureComm command of the declared ISO/IEC 18000 part		
4	Key update	Shall be tested with the SecureComm command of the declared ISO/IEC 18000 part		
2	Number of keys supported			

Table 2 lists all crypto suite requirements that shall be tested in dependence of the features of Table 1 as supported by the DUT. Items marked with M are mandatory and shall be tested for each DUT.

6.2 Crypto suite requirements

This clause contains all requirements of ISO/IEC 29167-13.

6.2.1 Crypto suite requirements of ISO/IEC 29167-13:2015 in Clauses 1 to 8 and Annexes A to C

All the requirements of ISO/IEC 29167-13:2015 in Clauses 1 to 8 and Annexes A to C shall apply, inherently by design only.

6.2.2 Crypto suite requirements of ISO/IEC 29167-13:2015 in Clauses 9 to 12 and Annex E

Table 2 contains all requirements of ISO/IEC 29167-13:2015 in Clauses 9 to 12 and Annex E.

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

M mandatory

Items marked with “M” are mandatory and shall be tested for all devices.

O optional

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

Table 2 — Crypto suite requirements

Item	Protocol Sub clause	Requirement	MO	Applies to	How verified
1	9	The Tag's air interface protocol logic shall provide an external reset to the Tag crypto engine which shall set **INIT**=FALSE, **TA**=FALSE, **IA**=FALSE and ERROR=FALSE before transition to the **CS-Reset** state.	M	Tag	By design
2	9	The **CS-Reset** state shall process crypto commands from the Tag's air interface protocol logic only when **ERROR**=FALSE. If an error condition exists then the Tag crypto engine shall set ERROR=TRUE and remain in the **CS-Reset** state.	M	Tag	By design
3	9	If an error condition exists then the Tag crypto engine shall set ERROR=TRUE and remain in the **CS-Reset** state.	M	Tag	By design
4	9	The Tag shall report an error condition if it receives a CryptoCommCmd, CryptoSecCommCmd or CryptoKeyUpdate command in the **CS-Reset** state.	M	Tag	By design
5	9	The Tag shall check a CryptoAuthCmd payload for any error conditions.	M	Tag	By design
6	9	The Tag shall report an error condition if Step ≠ 00_b in the **CS-Reset** state.	M	Tag	By demonstration using Test Pattern 3
7	9	The Tag shall report an error condition if the KeyID value is not supported by the Tag.	M	Tag	By demonstration using Test Pattern 2 (only if TA is supported), Test Pattern 10 (only if IA is supported) and Test Pattern 16
8	9	The Tag shall report an error condition if AuthMethod=00_b and the Tag does not support Tag authentication.	M	Tag	By design
9	9	The Tag shall report an error condition if AuthMethod=00_b and the Options selected are not supported by the Tag CSFeatures.	O	Tag	By design
10	9	The Tag shall report an error condition if AuthMethod=01_b and the Tag does not support Interrogator authentication.	M	Tag	By design
11	9	The Tag shall report an error condition if AuthMethod=01_b and Options ≠ 0000_b.	O	Tag	By demonstration using Test Pattern 9
12	9	The Tag shall report an error condition if AuthMethod=10_b and Options ≠ 0000_b.	M	Tag	By demonstration using Test Pattern 15
13	9	The Tag shall report an error condition if AuthMethod=11_b and the Tag does not support a vendor defined authentication.	M	Tag	By design
14	9	If no error condition exists, the Tag shall transition to the **CS-Init** state.	M	Tag	By design
15	10.1	The authentication method to be performed shall be specified by the 2-bit value AuthMethod which is defined in Table 2.	M	Tag, Interrogator	By design

Table 2 *(continued)*

Item	Protocol Sub clause	Requirement	MO	Applies to	How verified
16	10.1	If AuthMethod="00b" the Tag shall parse the Message for Tag Authentication as described in section 10.2	O	Tag	By demonstration using Test Pattern 1
17	10.1	If AuthMethod="01b" the Tag shall parse the Message Interrogator Authentication as described in section 10.3	O	Tag	By demonstration using Test Pattern 8
18	10.1	If AuthMethod="10b" the Tag shall parse the Message for Mutual Authentication as described in section 10.4	M	Tag	By demonstration using Test Pattern 14
19	10.1	Some of the authentication methods require multiple steps to be performed in a specific sequence. The current step in the sequence shall be specified by the 2-bit value Step as defined in Table 3.	M	Tag, Interrogator	By design
20	10.1	During step 0 of an authentication method, the Tag shall provide an 8-bit value CSFeatures which is used to indicate which of the optional Grain-128A CS features are supported by the Tag.	M	Tag	By design
21	10.1	During step 0 and 1 of an authentication method, the Interrogator shall provide a 4-bit value Options	M	Interrogator	By design
22	10.2.1	The Tag authentication method uses a challenge-response protocol having one pair of message exchange (see Figure 2).	O	Interrogator, Tag	By design
23	10.2.2	For Tag authentication the Interrogator shall generate a 48-bit random number for use as IRandomNumber and issue the challenge to the Tag with the TA.1 Payload as specified in Table 6.	O	Interrogator	By design
24	10.2.3	The Tag shall generate a 48-bit random number for use as TRandomNumber. The Tag crypto engine shall be initialized for Tag authentication using TRandomNumber, IRandomNumber and the crypto key specified by KeyID. The crypto engine then shall generate the Tag keystream.	O	Tag	By design
25	10.2.3	The Tag shall respond to the challenge from the Interrogator with the TA.1 Payload as specified in Table 7.	O	Tag	By design
26	10.2.3	The Tag shall transition to the **TA.1** state after the response to the Interrogator and shall set **TA**=TRUE.	O	Tag	By design
27	10.2.4	The Interrogator shall be initialized for Tag authentication using TRandomNumber, IRandomNumber and the crypto key specified by KeyID. The crypto engine shall then generate the Interrogator keystream.	O	Interrogator	By design
28	10.2.4	The Interrogator shall compare the Tag keystream with the Interrogator keystream to authenticate the Tag and accepts it as valid if they are equal.	O	Interrogator	By design