INTERNATIONAL STANDARD

ISO/IEC 19823-11

First edition
2022-10

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

Part 11: Crypto suite PRESENT-80

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

Partie 11: Suite cryptographique PRESENT-80

Reference number
ISO/IEC 19823-11:2022(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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Test methods **2**
4.1 General 2
4.2 By demonstration 2
4.3 By design 2
5 Test requirements for ISO/IEC 18000-63 interrogators and tags **2**
6 Test methods with respect to ISO/IEC 29167-11 interrogators and tags **2**
6.1 Test map for optional features 2
6.2 Crypto suite requirements 3
6.2.1 General 3
6.2.2 Crypto suite requirements of ISO/IEC 29167-11, Clauses 1 to 8 and Annexes A – C 3
6.2.3 Crypto suite requirements of ISO/IEC 29167-11, Clauses 9 to 11 and Annex E 3
6.3 Test patterns 8
6.3.1 General 8
6.3.2 Test Pattern 1 8
6.3.3 Test Pattern 2 9
6.3.4 Test Pattern 3 9
6.3.5 Test Pattern 4 10
Bibliography **11**

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 PRESENT-80 crypto suite as standardized in ISO/IEC 29167-11.

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

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

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

The holder of this patent right has assured ISO and IEC that he/she is 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 the patent database available at www.iso.org/patents or patents.iec.ch.

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

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

Part 11: Crypto suite PRESENT-80

1 Scope

This document specifies methods for determining conformance to the security crypto suite defined in ISO/IEC 29167-11.

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 29167-11.

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

ISO/IEC 29167-11, *Information technology — Automatic identification and data capture techniques — Part 11: Crypto suite PRESENT-80 security services for air interface communications*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and in ISO/IEC 29167-11 apply.

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

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

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

4 Test methods

4.1 General

This document describes test methods for ISO/IEC 29167-11. 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 29167-11 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	Mark items to be tested for supplied product	Test results
1	TA	Shall be tested with the *Authenticate* command of ISO/IEC 18000-63.		

Table 1 *(continued)*

#	Feature	Additional requirement	Mark items to be tested for supplied product	Test results
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.		

6.2 Crypto suite requirements

6.2.1 General

This clause lists all the requirements of ISO/IEC 29167-11 that shall be met.

6.2.2 Crypto suite requirements of ISO/IEC 29167-11, Clauses 1 to 8 and Annexes A – C

All the requirements of ISO/IEC 29167-11, 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 29167-11, Clauses 9 to 11 and Annex E

The requirements of ISO/IEC 29167-11, Clauses 9 to 12 and Annex E listed in Table 2 shall be met. This document shall be read in conjunction with ISO/IEC 29167-11 to provide a full explanation of the terms used.

Table 2 — Crypto suite requirements

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) 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	A Tag conforming to this document shall support the case of AuthMethod=00_2.	M	Tag	By design
4	9.3.3	If the value of the field RFU is not 00_2 then the Tag shall set a "Not Supported" crypto suite error.	M	Tag	By design
5	9.3.3	The Tag shall parse the value of E.	M	Tag	By demonstration using Test Pattern 2
6	9.3.3	An 80-bit key, for which Key.ID=0, shall be used for Tag authentication.	O	Tag	By demonstration using Test Pattern 1

[a] All clause, subclause and table references are to ISO/IEC 29167-11.

[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
7	9.3.3	A Tag shall support at least one of the options $E=0_2$ or $E=1_2$.	M	Tag	By demonstration using Test Pattern 1
8	9.3.3	The Tag shall set a "Not Supported" crypto suite error for a value of E that is not supported by the Tag.	M	Tag	By design
9	9.3.3	The Tag shall parse the value of T.	M	Tag	By demonstration using Test Pattern 1
10	9.3.3	If the Tag does not support $T=1_2$ then the Tag shall set a "Not Supported" crypto suite error.	M	Tag	By design
11	9.3.3	A Tag shall support the option $T=0_2$ and may support the option $T=1_2$.	M	Tag	By demonstration using Test Pattern 1
12	9.3.3	The Tag shall use Key.KeyID to compute TAM1 response.	O	Tag	By demonstration using Test Pattern 2
13	9.3.3	If the Tag does not support Key.KeyID then the Tag shall set a "Not Supported" crypto suite error.	M	Tag	By design
14	9.3.3	If present, the Tag shall parse L, the value of KeyLength.	O	Tag	By design
15	9.3.3	If $L=0_2$ then PRESENT-80 shall be used in the computation of TAM1 response. If Key.KeyID does not have length 80 bits then the Tag shall set a "Not Supported" crypto suite error.	O	Tag	By demonstration using Test Pattern 2
16	9.3.3	If $L=1_2$ then PRESENT-128 shall be used in the computation of TAM1 response. If Key.KeyID does not have length 128 bits then the Tag shall set a "Not Supported" crypto suite error.	O	Tag	By demonstration using Test Pattern 2
17	9.3.3	If present, the Tag shall check that the value of the field $E\text{-}RFU=000_2$. If not, the Tag shall set a "Not Supported" crypto suite error.	O	Tag	By design
18	9.3.4	The Tag shall generate a random salt TRnd of length 20 bits.	M	Tag	By design
19	9.3.4	The Tag shall use Key.KeyID of length *k* and PRESENT-*k* encryption to form a 64-bit string TResponse: TResponse = PRESENT-*k*-ENC (Key.KeyID, CTAM || TRnd || IChallenge).	M	Tag	By demonstration using Test Pattern 2
20	9.3.5	After receiving TAM1 response, the Interrogator shall use Key.KeyID to compute the 64-bit string R: R = PRESENT-*k*-DEC (Key.KeyID, TResponse).	M	Interrogator	By design
21	9.3.5	The Interrogator shall check that R[41:0] = IChallenge.	M	Interrogator	By design

[a] All clause, subclause and table references are to ISO/IEC 29167-11.

[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.