International Standard

ISO/IEC 19823-10

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

Part 10: Crypto suite AES-128

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

Partie 10: Suite cryptographique AES-128

Third edition
2026-03

Reference number
ISO/IEC 19823-10:2026(en)

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms, definitions, symbols and abbreviated terms ... **1**
3.1 Terms and definitions ... 1
3.2 Symbols and abbreviated terms ... 2

4 Test methods ... **2**
4.1 General ... 2
4.2 By demonstration ... 2
4.3 By design ... 2

5 Test methods for the ISO/IEC 18000 series ... **2**
5.1 Test requirements for ISO/IEC 18000-3 Interrogators and Tags ... 2
5.2 Test requirements for ISO/IEC 18000-63 Interrogators and Tags ... 3

6 Test methods related to ISO/IEC 29167-10 Interrogators and Tags ... **3**
6.1 Test map for optional features ... 3
6.2 Additional parameters required as input for the test ... 4
6.3 Crypto suite requirements ... 4
6.3.1 General ... 4
6.3.2 Crypto suite requirements of ISO/IEC 29167-10:2026, Clauses 4 to 6 ... 4
6.3.3 Crypto suite requirements of ISO/IEC 29167-10:2026, Clauses 7 to 12 ... 4
6.3.4 Crypto suite requirements of ISO/IEC 29167-10:2026, Annex A ... 19
6.3.5 Crypto suite requirements of ISO/IEC 29167-10:2026, Annex E ... 19

7 Test patterns ... **23**
7.1 General ... 23
7.2 Test pattern information ... 23
7.2.1 General ... 23
7.2.2 Information related to ISO/IEC 18000-3:2010, MODE 1 ... 24
7.2.3 Information related to ISO/IEC 18000-63 ... 24
7.3 Test pattern descriptions ... 25
7.3.1 General ... 25
7.3.2 Test pattern 01 (TAM reject message when "AuthMethod" is '11') ... 25
7.3.3 Test pattern 02 (TAM1 execution and error handling) ... 25
7.3.4 Test pattern 03 (TAM1 execution for all keys) ... 27
7.3.5 Test pattern 04 (TAM1 store Tag reply in the response buffer) ... 27
7.3.6 Test pattern 05 (TAM1 with Challenge, read Tag reply from the response buffer) ... 29
7.3.7 Test pattern 06 (TAM2 execution and error handling) ... 30
7.3.8 Test pattern 07 (TAM2 unauthorized use of KeyID for profile) ... 33
7.3.9 Test pattern 08 (TAM2 execution for all keys) ... 34
7.3.10 Test pattern 09 (MAM1 execution and error handling) ... 35
7.3.11 Test pattern 10 (MAM2 execution and error handling) ... 36
7.3.12 Test pattern 11 (MAM1 and MAM2 execution for all keys) ... 40

Bibliography ... **42**

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

This third edition cancels and replaces the second edition (ISO/IEC 19823-10:2020), which has been technically revised.

The main change is as follows: test items have been updated to reflect changes to the over-the-air protocol.

A list of all parts in the ISO/IEC 19823 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

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

The ISO/IEC 19823 series describes conformance test methods for security service crypto suites. The ISO/IEC 19823 series is related to the ISO/IEC 18047 series, which describes the radio frequency identification device conformance test methods, in the same way as the ISO/IEC 29167 series is related to the ISO/IEC 18000 series. These relations mean that, for a product that is claimed to be conform 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 the ISO/IEC 18000 series or the ISO/IEC 29167 series, all related parts of ISO/IEC 18047 and ISO/IEC 19823 apply.

The conformance parameters are:

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

— protocol including commands and replies;

— nominal values and tolerances.

NOTE 1 ISO/IEC 18047-6 contains the conformance test requirements of ISO/IEC 18000-6, ISO/IEC 18000-61, ISO/IEC 18000-62, ISO/IEC 18000-63 and ISO/IEC 18000-64.

NOTE 2 Test methods for Interrogator and Tag performance are covered in the ISO/IEC 18046 series.

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

Part 10:
Crypto suite AES-128

1 Scope

This document describes the test methods for determining conformance for the security crypto suite AES-128 defined in ISO/IEC 29167-10.

This document contains conformance tests for all mandatory and applicable optional functions.

Unless otherwise specified, the tests in this document are only applicable to radio frequency identification (RFID) Tags and Interrogators defined in the ISO/IEC 15693 series and in the ISO/IEC 18000 series using ISO/IEC 29167-10.

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 18047-3:2022, *Information technology — Radio frequency identification device conformance test methods — Part 3: Test methods for air interface communications at 13,56 MHz*

ISO/IEC 18000-63:2026, *Information technology — Radio frequency identification device conformance test methods — Part 6: Test methods for air interface communications at 860 MHz to 960 MHz*[1)]

ISO/IEC 18047-6:2025, *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 — Vocabulary*

ISO/IEC 29167-10:2026, *Information technology — Automatic identification and data capture techniques — Part 10: Crypto suite AES-128 security services for air interface communications*

Bibliography

[1] ISO/IEC 15693 (all parts), *Cards and security devices for personal identification — Contactless vicinity objects*

[2] ISO/IEC 18000 (all parts), *Information technology — Radio frequency identification for item management*

[3] ISO/IEC 18046 (all parts), *Information technology — Radio frequency identification device performance test methods*

[4] ISO/IEC 18047 (all parts), *Information technology — Radio frequency identification device conformance test methods*

[5] ISO/IEC 19823 (all parts), *Information technology — Conformance test methods for security service crypto suites*

[6] ISO/IEC 29167 (all parts), *Information technology — Automatic identification and data capture techniques*