
**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



This document is a preview generated by EMS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	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 with respect to 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 with respect to the 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 29167-10:2017, Clauses 1 to 6	5
6.3.3 Crypto suite requirements of ISO/IEC 29167-10:2017, Clauses 7 to 12	5
6.3.4 Crypto suite requirements of ISO/IEC 29167-10:2017, Annex A	21
6.3.5 Crypto suite requirements of ISO/IEC 29167-10:2017, Annex E	21
7 Test patterns	26
7.1 General	26
7.2 Test pattern information	26
7.2.1 General	26
7.2.2 Information related to ISO/IEC 18000-3 MODE 1	26
7.2.3 Information related to ISO/IEC 18000-63	27
7.3 Test pattern descriptions	27
7.3.1 General	27
7.3.2 Test pattern 01 (TAM reject message when "AuthMethod" is '11')	27
7.3.3 Test pattern 02 (TAM1 execution and error handling)	28
7.3.4 Test pattern 03 (TAM1 execution for all keys)	29
7.3.5 Test pattern 04 (TAM1 store Tag reply in the response buffer)	30
7.3.6 Test pattern 05 (TAM1 with Challenge, read Tag reply from the response buffer)	31
7.3.7 Test pattern 06 (TAM2 execution and error handling)	32
7.3.8 Test pattern 07 (TAM2 unauthorized use of KeyID for profile)	36
7.3.9 Test pattern 08 (TAM2 execution for all keys)	37
7.3.10 Test pattern 09 (MAM1 execution and error handling)	37
7.3.11 Test pattern 10 (MAM2 execution and error handling)	39
7.3.12 Test pattern 11 (MAM1 and MAM2 execution for all keys)	43
Bibliography	45

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*.

This second edition cancels and replaces the first edition (ISO/IEC 19823-10:2017), which has been technically revised.

The main changes compared to the previous edition are as follows:

- In addition to Tag Authentication, this edition also defines support for Interrogator authentication and Mutual Authentication. This version describes the test methods for the additional functionality.

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

These relations mean that for a product that is claimed to conform to a pair of ISO/IEC 18000 and ISO/IEC 29167 documents, then the test methods of the ISO/IEC 18047 and ISO/IEC 19823 documents 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 AES-128 crypto suite as standardized in ISO/IEC 29167-10.

NOTE 2 Test methods for interrogator and tag performance are covered by 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 test methods for determining the conformance of security crypto suites defined in ISO/IEC 29167-10.

This document contains conformance tests for all mandatory and applicable 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 intended to be applied exclusively to 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/TR 18047-3:2011, *Information technology — Radio frequency identification device conformance test methods — Part 3: Test methods for air interface communications at 13,56 MHz*

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 29167-10:2017, *Information technology — Automatic identification and data capture techniques — Part 10: Crypto suite AES-128 security services for air interface communications*

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 and ISO/IEC 29167-10 apply.