
**Information technology — Security
techniques — Cryptographic
algorithms and security mechanisms
conformance testing**

*Technologie de l'information — Techniques de sécurité — Essais de
conformité des algorithmes cryptographiques et des mécanismes de
sécurité*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	6
5 Objectives	7
6 Types of cryptographic algorithms and security mechanisms from a conformance testing perspective	8
6.1 General	8
6.2 Asymmetric key algorithms	8
6.3 Digital signature	8
6.4 Digital signature with message recovery	8
6.5 Hashing algorithms	8
6.6 Key establishment mechanisms	8
6.7 Lightweight cryptography	9
6.8 Message authentication algorithms	9
6.9 Random bit generator algorithms	9
6.9.1 Deterministic random bit generator algorithms	9
6.9.2 Non-deterministic random bit generator algorithms	9
6.10 Symmetric key algorithms	10
6.10.1 Block cipher symmetric key algorithms	10
6.10.2 Stream cipher symmetric key algorithms	10
7 Conformance testing methodologies	10
7.1 Overview	10
7.2 Black box testing	11
7.2.1 General	11
7.2.2 Known-answer test vectors	11
7.2.3 Multi-block message testing	11
7.2.4 Monte Carlo or statistical testing	11
7.3 Glass box or white box testing	11
7.3.1 Source code inspection	11
7.3.2 Binary analysis	11
8 Levels of conformance testing	12
8.1 Introduction	12
8.2 Level of basic conformance testing	12
8.3 Level of moderate conformance	12
9 Conformance testing guidelines	12
9.1 General guidelines	12
9.1.1 Identification	12
9.1.2 Guidelines for black box testing	13
9.1.3 Guidelines for white box testing	13
9.2 Guidelines specific to encryption algorithms	16
9.2.1 Identification of encryption algorithms	16
9.2.2 Selecting a set of conformance test items	17
9.2.3 Guidelines for each conformance test item	18
9.3 Guidelines specific to digital signature algorithms	29
9.3.1 Identification of digital signature algorithms	29
9.3.2 Selecting a set of conformance test items	29
9.3.3 Guidelines for each conformance test item	29
9.4 Guidelines specific to hashing algorithms	30

9.4.1	Identification of hashing algorithms	30
9.4.2	Selecting a set of conformance test items	31
9.4.3	Guidelines for each conformance test item	31
9.5	Guidelines specific to MAC algorithms	33
9.5.1	Identification of MAC algorithms	33
9.5.2	Selecting a set of conformance test items	34
9.5.3	Guidelines for each conformance test item	34
9.6	Guidelines specific to RBG algorithms	35
9.6.1	Identification of RBG algorithms	35
9.6.2	Selecting a set of conformance test items	35
9.6.3	Guidelines for each conformance test item	35
9.7	Guidelines specific to key establishment mechanisms	36
9.7.1	Identification of key establishment mechanisms	36
9.7.2	Selecting a set of conformance test items	36
9.7.3	Guidelines for each conformance test item	37
9.8	Guidelines specific to key derivation function	39
9.8.1	Identification of key derivation function	39
9.8.2	Selecting a set of conformance test items	39
9.8.3	Guidelines for each conformance test item	39
9.9	Guidelines specific to prime number generation	40
9.9.1	Identification of prime number generation	40
9.9.2	Selecting a set of conformance test items	40
9.9.3	Guidelines for each conformance test item	41
10	Conformance testing	41
10.1	Level of conformance testing	41
10.2	Symmetric key cryptographic algorithms	42
10.2.1	n-bit block cipher	42
10.3	Asymmetric key cryptographic algorithms	43
10.3.1	Digital Signature Algorithm (DSA)	43
10.3.2	RSA	47
10.3.3	Elliptic Curve Digital Signature Algorithm (ECDSA)	49
10.4	Dedicated hashing algorithms	51
10.4.1	General	51
10.4.2	Black box testing	51
10.4.3	White box testing	51
10.5	Message Authentication Codes (MAC)	51
10.5.1	Black box testing	51
10.5.2	White box testing	52
10.6	Authenticated encryption	53
10.6.1	Black box testing	53
10.6.2	White box testing	54
10.7	Deterministic Random Bit Generation algorithms	54
10.7.1	DRBG based on ISO/IEC 18031	54
10.8	Key agreement	58
10.8.1	Black box testing	58
10.8.2	White box testing	61
10.9	Key Derivation Functions (KDF)	62
10.9.1	Black box testing	62
10.9.2	White box testing	63
	Annex A (informative) Common mistakes in cryptographic algorithm implementations	64
	Annex B (informative) Examples of known-answer test vectors	65
	Bibliography	66

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology, SC 27, IT Security techniques*.

Introduction

This document describes cryptographic algorithms and security mechanisms conformance testing methods.

The purpose of this document is to address conformance testing methods of cryptographic algorithms and security mechanisms implemented in a cryptographic module. This will allow a complete security evaluation of both the cryptographic module and the implemented cryptographic algorithms and security mechanisms.

This document is related to ISO/IEC 19790 and ISO/IEC 24759. ISO/IEC 19790 specifies the security requirements for cryptographic modules. At a minimum, a cryptographic module implements at least one approved security function (i.e., cryptographic algorithm or security mechanism). ISO/IEC 24759 addresses the test requirements for each of the security requirements in ISO/IEC 19790. However, ISO/IEC 24759 does not address test methods for cryptographic algorithms and security mechanisms conformance testing.

Information technology — Security techniques — Cryptographic algorithms and security mechanisms conformance testing

1 Scope

This document gives guidelines for cryptographic algorithms and security mechanisms conformance testing methods.

Conformance testing assures that an implementation of a cryptographic algorithm or security mechanism is correct whether implemented in hardware, software or firmware. It also confirms that it runs correctly in a specific operating environment. Testing can consist of known-answer or Monte Carlo testing, or a combination of test methods. Testing can be performed on the actual implementation or modelled in a simulation environment.

This document does not include the efficiency of the algorithms or security mechanisms nor the intrinsic performance. This document focuses on the correctness of the implementation.

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 14888-3:2016, *Information technology — Security techniques — Digital signatures with appendix*

ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*