

---

---

**Information technology — Security  
techniques — Test requirements  
for cryptographic modules**

*Technologies de l'information — Techniques de sécurité — Exigences  
d'essai pour modules cryptographiques*

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword.....	iv
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions.....</b>	<b>1</b>
<b>4 Abbreviated terms .....</b>	<b>4</b>
<b>5 Document Organization .....</b>	<b>5</b>
5.1 General.....	5
5.2 Assertions and security requirements .....	5
5.3 Assertions with cross references .....	6
<b>6 Security requirements .....</b>	<b>6</b>
6.1 General test requirements .....	6
6.2 Cryptographic module specification .....	6
6.3 Cryptographic module ports and interfaces.....	14
6.4 Roles, services, and authentication.....	27
6.4.1 Roles .....	27
6.4.2 Services .....	28
6.4.3 Operator authentication .....	30
6.5 Finite state model .....	35
6.6 Physical security.....	39
6.6.1 General physical security requirements .....	39
6.6.2 Environmental failure protection/testing .....	55
6.7 Operational environment .....	57
6.8 Cryptographic key management.....	66
6.8.1 Random bit generators (RBGs) .....	67
6.8.2 Key generation .....	68
6.8.3 Key establishment .....	70
6.8.4 Key entry and output.....	71
6.8.5 Key storage .....	75
6.8.6 Key zeroisation .....	75
6.9 Self-tests.....	76
6.9.1 Power-up tests .....	79
6.9.2 Conditional tests.....	85
6.10 Design assurance .....	91
6.10.1 Configuration management .....	91
6.10.2 Delivery and operation .....	94
6.10.3 Development .....	95
6.10.4 Guidance documents .....	100
6.11 Mitigation of other attacks .....	101
6.12 Documentation requirements.....	102
6.13 Cryptographic module security policy .....	102
6.14 Approved protection profiles .....	103
6.15 Approved security functions .....	103
6.16 Approved key establishment methods.....	103
6.17 Recommended software development practices .....	103
6.18 Examples of mitigation of other attacks.....	103

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 24759 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

# Information technology — Security techniques — Test requirements for cryptographic modules

## 1 Scope

This International Standard specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2006. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This International Standard also specifies the requirements for information that vendors provide to testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformance to the requirements specified in ISO/IEC 19790:2006.

Vendors can use this International Standard as guidance in trying to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790 before they apply to the testing laboratory for testing.

## 2 Normative references

The following referenced documents are indispensable for the application 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 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 18031:2005, *Information technology — Security techniques — Random bit generation*

ISO/IEC 19790:2006, *Information technology — Security techniques — Security requirements for cryptographic modules*