International Standard

ISO/IEC 24759

# Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules

*Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences d'essai pour modules cryptographiques*

Fourth edition
2025-02

Reference number
ISO/IEC 24759:2025(en)

© ISO/IEC 2025



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2025

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

**Foreword** ..... **v**
**Introduction** ..... **vi**
**1 Scope** ..... **1**
**2 Normative references** ..... **1**
**3 Terms and definitions** ..... **1**
**4 Symbols and abbreviated terms** ..... **2**
**5 Document organization** ..... **2**
5.1 General ..... 2
5.2 Assertions and security requirements ..... 3
5.3 Assertions with cross references ..... 3
**6 Security requirements** ..... **4**
6.1 General ..... 4
6.2 Cryptographic module specification ..... 5
6.2.1 Cryptographic module specification general requirements ..... 5
6.2.2 Types of cryptographic modules ..... 5
6.2.3 Cryptographic boundary ..... 6
6.2.4 Module operations ..... 16
6.3 Cryptographic module interfaces ..... 23
6.3.1 Cryptographic module interfaces general requirements ..... 23
6.3.2 Categories of interfaces ..... 26
6.3.3 Plaintext trusted path ..... 35
6.3.4 Protected internal paths ..... 38
6.4 Roles, services, and authentication ..... 39
6.4.1 Roles, services, and authentication general requirements ..... 39
6.4.2 Roles ..... 40
6.4.3 Services ..... 41
6.4.4 Authentication ..... 49
6.5 Software/firmware security ..... 59
6.5.1 Software/firmware security general requirements ..... 59
6.5.2 Security level 1 ..... 62
6.5.3 Security level 2 ..... 67
6.5.4 Security levels 3 and 4 ..... 68
6.6 Operational environment ..... 69
6.6.1 Operational environment general requirements ..... 69
6.6.2 Clause applicability ..... 70
6.6.3 Operating system requirements for modifiable operational environments ..... 71
6.7 Physical security ..... 83
6.7.1 Physical security embodiments ..... 83
6.7.2 Physical security general requirements ..... 84
6.7.3 Physical security requirements for each physical security embodiment ..... 95
6.7.4 Environmental failure protection/testing ..... 100
6.7.5 Environmental failure protection features ..... 100
6.7.6 Environmental failure testing procedures ..... 101
6.8 Non-invasive security ..... 104
6.8.1 Non-invasive security general requirements ..... 104
6.8.2 Security levels 1 and 2 ..... 104
6.8.3 Security level 3 ..... 105
6.8.4 Security level 4 ..... 105
6.9 Sensitive security parameter management ..... 106
6.9.1 Sensitive security parameter management general requirements ..... 106
6.9.2 Random bit generators ..... 108
6.9.3 Sensitive security parameter generation ..... 110
6.9.4 Automated sensitive security parameter establishment ..... 110

© ISO/IEC 2025 – All rights reserved

6.9.5 Sensitive security parameter entry and output 111
6.9.6 Sensitive security parameter storage 117
6.9.7 Sensitive security parameter zeroization 118
6.10 Self-tests 122
6.10.1 Self-test general requirements 122
6.10.2 Security levels 3 and 4 126
6.10.3 Pre-operational self-tests 127
6.10.4 Conditional self-tests 130
6.11 Life-cycle assurance 143
6.11.1 Life-cycle assurance general requirements 143
6.11.2 Configuration management 143
6.11.3 Design 145
6.11.4 Finite state model 145
6.11.5 Development 149
6.11.6 Vendor testing 155
6.11.7 Delivery and operation 157
6.11.8 Guidance documents 160
6.12 Mitigation of other attacks 161
6.12.1 Mitigation of other attacks general requirements 161
6.12.2 Security levels 1, 2 and 3 161
6.12.3 Security level 4 161

**7 Documentation requirements 162**
7.1 Purpose 162
7.2 Items 163
7.2.1 Cryptographic module specification 163
7.2.2 Cryptographic module interfaces 164
7.2.3 Roles, services, and authentication 164
7.2.4 Software/Firmware security 165
7.2.5 Operational environment 165
7.2.6 Physical security 166
7.2.7 Non-invasive security 167
7.2.8 Sensitive security parameter management 167
7.2.9 Self-tests 169
7.2.10 Life-cycle assurance 169
7.2.11 Mitigation of other attacks 171

**8 Cryptographic module security policy 172**
8.1 General 172
8.2 Items 173
8.2.1 General 173
8.2.2 Cryptographic module specification 174
8.2.3 Cryptographic module interfaces 175
8.2.4 Roles, services, and authentication 175
8.2.5 Software/Firmware security 176
8.2.6 Operational environment 177
8.2.7 Physical security 178
8.2.8 Non-invasive security 179
8.2.9 Sensitive security parameters management 179
8.2.10 Self-tests 180
8.2.11 Life-cycle assurance 180
8.2.12 Mitigation of other attacks 181

**Bibliography 182**

© ISO/IEC 2025 – All rights reserved

# 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 not 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 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 24759:2017), which has been technically revised.

The main changes are as follows:

— new terminology has been added;

— ASs, VEs and TEs have been updated according to ISO/IEC 19790:2025; and

— VEs and TEs have been corrected or updated to improve efficiency.

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.

© ISO/IEC 2025 – All rights reserved

# Introduction

In information technology there is an ever-increasing need to use cryptographic mechanisms, such as for the protection of data against unauthorized disclosure or manipulation, for entity authentication, and for non-repudiation. The security and reliability of such mechanisms are directly dependent on the cryptographic modules in which they are implemented.

ISO/IEC 19790 provides four increasing, qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The cryptographic techniques are identical over the four security levels defined in this document. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include:

— cryptographic module specification;

— cryptographic module interfaces;

— roles, services and authentication;

— software/firmware security;

— operational environment;

— physical security;

— non-invasive security;

— sensitive security parameter management;

— self-tests;

— life-cycle assurance; and

— mitigation of other attacks.

This document specifies the test requirements for cryptographic modules conforming to ISO/IEC 19790:2025.

© ISO/IEC 2025 – All rights reserved

# Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules

## 1 Scope

This document specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2025. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This document also specifies the information that vendors are required to provide testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2025.

Vendors can also use this document to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2025 before applying to a testing laboratory for testing.

## 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 19790:2025, *Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules*

ISO/IEC 20085-1, *IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques*

ISO/IEC 20085-2, *IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus*

ISO/IEC 20543, *Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19790 and the following apply.

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

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

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

**3.1**
**validation certificate**
assertion by a certification body that a cryptographic function has been tested and found to be a correct implementation of the target cryptographic function

© ISO/IEC 2025 – All rights reserved