International Standard

ISO/IEC 19790

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

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences de sécurité pour les modules cryptographiques

Third edition
2025-02

Reference number
ISO/IEC 19790:2025(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 Abbreviated terms **17**
5 Cryptographic module security levels **18**
5.1 General 18
5.2 Security level 1 18
5.3 Security level 2 19
5.4 Security level 3 19
5.5 Security level 4 20
6 Functional security objectives **21**
7 Security requirements **21**
7.1 General 21
7.2 Cryptographic module specification 24
7.2.1 Cryptographic module specification general requirements 24
7.2.2 Types of cryptographic modules 24
7.2.3 Cryptographic boundary 24
7.2.4 Module operations 25
7.3 Cryptographic module interfaces 27
7.3.1 Cryptographic module interfaces general requirements 27
7.3.2 Types of interfaces 27
7.3.3 Categories of interfaces 27
7.3.4 Plaintext trusted path 28
7.3.5 Protected internal paths 29
7.4 Roles, services, and authentication 29
7.4.1 Roles, services, and authentication general requirements 29
7.4.2 Roles 29
7.4.3 Services 30
7.4.4 Authentication 31
7.5 Software/firmware security 33
7.5.1 Software/firmware security general requirements 33
7.5.2 Security level 1 34
7.5.3 Security level 2 34
7.5.4 Security levels 3 and 4 35
7.6 Operational environment 35
7.6.1 Operational environment general requirements 35
7.6.2 Clause applicability 36
7.6.3 Operating system requirements for modifiable operational environments 37
7.7 Physical security 39
7.7.1 Physical security embodiments 39
7.7.2 Physical security general requirements 40
7.7.3 Physical security requirements for each physical security embodiment 42
7.7.4 Environmental failure protection/testing 43
7.7.5 Environmental failure protection features 43
7.7.6 Environmental failure testing procedures 44
7.8 Non-invasive security 44
7.8.1 Non-invasive security general requirements 44
7.8.2 Security levels 1 and 2 45
7.8.3 Security level 3 45
7.8.4 Security level 4 45

© ISO/IEC 2025 – All rights reserved

7.9 Sensitive security parameter management 45
7.9.1 Sensitive security parameter management general requirements 45
7.9.2 Random bit generators 45
7.9.3 Sensitive security parameter generation 46
7.9.4 Automated sensitive security parameter establishment 46
7.9.5 Sensitive security parameter entry and output 46
7.9.6 Sensitive security parameter storage 47
7.9.7 Sensitive security parameter zeroization 47
7.10 Self-tests 48
7.10.1 Self-test general requirements 48
7.10.2 Security levels 3 and 4 49
7.10.3 Pre-operational self-tests 49
7.10.4 Conditional self-tests 50
7.11 Life-cycle assurance 53
7.11.1 Life-cycle assurance general requirements 53
7.11.2 Configuration management 53
7.11.3 Design 54
7.11.4 Finite state model 54
7.11.5 Development 55
7.11.6 Vendor testing 56
7.11.7 Delivery and operation 56
7.11.8 Guidance documents 58
7.12 Mitigation of other attacks 58
7.12.1 Mitigation of other attacks general requirements 58
7.12.2 Security levels 1, 2 and 3 58
7.12.3 Security level 4 59

Annex A (normative) **Documentation requirements** **60**

Annex B (normative) **Cryptographic module security policy** **66**

Annex C (normative) **Approved security functions** **72**

Annex D (normative) **Approved sensitive security parameter generation and establishment methods** **74**

Annex E (normative) **Approved authentication mechanisms** **75**

Annex F (normative) **Approved non-invasive attack mitigation test metrics** **76**

Annex G (normative) **Module secure development, manufacturing and operation** **77**

Bibliography **78**

© 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 third edition cancels and replaces the second edition (ISO/IEC 19790:2012), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 19790:2012/Cor 1:2015.

The main changes are as follows:

— Clauses 3, 4 and 5 have been refined and updated to reflect changes in requirements in Clause 7;

— the language in Clause 6 has been refined and modernized;

— in Clause 7, the requirements have been reworded and rearranged for clarity. New requirements have been added, and redundant or unnecessary requirements removed;

— Annexes A and B have been updated to reflect changes in requirements in Clause 7;

— Annexes C, D and E have been restructured and updated in line with standards published since the previous edition, as well as with examples of rate limiting methods;

— Annex F has been updated with the inclusion of ISO/IEC 17825; and

— new Annex G on module secure development, manufacturing and operation has been added.

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.

This document 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.

The overall security rating or the security level within each area of a cryptographic module is chosen to provide a level of security which is appropriate for the security requirements of the application and environment in which the module is utilized and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an appropriate level of security for the given application and environment. Since each authority is responsible for selecting which approved security functions are appropriate for a given application, conformity with this document does not imply either full interoperability or mutual acceptance of compliant products. The importance of security awareness and of making information security a management priority should be communicated to all concerned.

Information security requirements vary for different applications; organizations should identify their information resources and determine the sensitivity to and the potential impact of a loss by implementing appropriate controls. Controls include, but are not limited to:

— physical and environmental controls;

— access controls;

— system security maintenance and patch management;

— backup and contingency plans; and

— information and data controls.

These controls are only as effective as the administration of appropriate security policies and procedures within the operational environment.

Conformity with this document is not sufficient to ensure that a module is secure or that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected.

© ISO/IEC 2025 – All rights reserved

Owners of sensitive information are expected to assess the risks to their information and to deploy cryptographic modules as part of their overall risk mitigation plan, in order to mitigate specific identified risks. The security policy of the module, which outlines its strengths and limitations, is expected to be followed for any given deployment.

© ISO/IEC 2025 – All rights reserved

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

1 Scope

This document specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in Information and Communication Technologies (ICT). It defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity and a diversity of application environments. This document specifies up to four security levels for each of the 11 requirement areas with each security level increasing security over the preceding level.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
access control list
ACL
list of permissions to grant access to an object

3.2
administrator guidance
written material that is used by either the *crypto officer* (3.30) or any other administrative *role* (3.119) for the correct configuration, maintenance, and administration of the *cryptographic module* (3.35)

3.3
automated
without *manual* (3.81) intervention or input (e.g. electronic means such as through a computer network)

3.4
approved data authentication technique
approved method providing assurance that the originator of the data is as claimed

Note 1 to entry: Approved data authentication techniques can include the use of an approved *digital signature* (3.43), approved *message authentication code* (3.82) or approved keyed hash. Approved data authentication techniques are specified in Annex C.

3.5
approved integrity technique
approved method of verifying whether or not data has been corrupted or modified

Note 1 to entry: Approved integrity techniques can be keyed, and can include an approved hash, a *message authentication code* (3.82) or a *digital signature* (3.43) algorithm.

© ISO/IEC 2025 – All rights reserved