

---

---

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

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



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2012

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 .....	v
Introduction.....	vi
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	1
4 Abbreviated terms .....	14
5 Cryptographic module security levels .....	15
5.1 Security Level 1 .....	15
5.2 Security Level 2 .....	15
5.3 Security Level 3 .....	15
5.4 Security Level 4 .....	16
6 Functional security objectives .....	17
7 Security requirements.....	17
7.1 General .....	17
7.2 Cryptographic module specification .....	20
7.2.1 Cryptographic module specification general requirements .....	20
7.2.2 Types of cryptographic modules .....	20
7.2.3 Cryptographic boundary .....	21
7.2.4 Modes of operations .....	22
7.3 Cryptographic module interfaces .....	23
7.3.1 Cryptographic module interfaces general requirements .....	23
7.3.2 Types of interfaces .....	23
7.3.3 Definition of interfaces.....	23
7.3.4 Trusted channel.....	24
7.4 Roles, services, and authentication .....	25
7.4.1 Roles, services, and authentication general requirements .....	25
7.4.2 Roles .....	25
7.4.3 Services .....	26
7.4.4 Authentication .....	27
7.5 Software/Firmware security .....	29
7.6 Operational environment.....	30
7.6.1 Operational environment general requirements .....	30
7.6.2 Operating system requirements for limited or non-modifiable operational environments.....	32
7.6.3 Operating system requirements for modifiable operational environments .....	33
7.7 Physical security .....	35
7.7.1 Physical security embodiments.....	35
7.7.2 Physical security general requirements .....	37
7.7.3 Physical security requirements for each physical security embodiment .....	38
7.7.4 Environmental failure protection/testing .....	41
7.8 Non-invasive security .....	42
7.9 Sensitive security parameter management .....	43
7.9.1 Sensitive security parameter management general requirements .....	43
7.9.2 Random bit generators .....	43
7.9.3 Sensitive security parameter generation .....	43
7.9.4 Sensitive security parameter establishment .....	43
7.9.5 Sensitive security parameter entry and output.....	44
7.9.6 Sensitive security parameter storage .....	44
7.9.7 Sensitive security parameter zeroisation .....	45

<b>7.10</b>	<b>Self-tests</b> .....	<b>45</b>
<b>7.10.1</b>	<b>Self-test general requirements</b> .....	<b>45</b>
<b>7.10.2</b>	<b>Pre-operational self-tests</b> .....	<b>46</b>
<b>7.10.3</b>	<b>Conditional self-tests</b> .....	<b>47</b>
<b>7.11</b>	<b>Life-cycle assurance</b> .....	<b>49</b>
<b>7.11.1</b>	<b>Life-cycle assurance general requirements</b> .....	<b>49</b>
<b>7.11.2</b>	<b>Configuration management</b> .....	<b>49</b>
<b>7.11.3</b>	<b>Design</b> .....	<b>50</b>
<b>7.11.4</b>	<b>Finite state model</b> .....	<b>50</b>
<b>7.11.5</b>	<b>Development</b> .....	<b>51</b>
<b>7.11.6</b>	<b>Vendor testing</b> .....	<b>52</b>
<b>7.11.7</b>	<b>Delivery and operation</b> .....	<b>52</b>
<b>7.11.8</b>	<b>End of life</b> .....	<b>53</b>
<b>7.11.9</b>	<b>Guidance documents</b> .....	<b>53</b>
<b>7.12</b>	<b>Mitigation of other attacks</b> .....	<b>54</b>
<b>Annex A</b>	<b>(normative) Documentation requirements</b> .....	<b>55</b>
<b>A.1</b>	<b>Purpose</b> .....	<b>55</b>
<b>A.2</b>	<b>Items</b> .....	<b>55</b>
<b>Annex B</b>	<b>(normative) Cryptographic module security policy</b> .....	<b>61</b>
<b>B.1</b>	<b>General</b> .....	<b>61</b>
<b>B.2</b>	<b>Items</b> .....	<b>61</b>
<b>Annex C</b>	<b>(normative) Approved security functions</b> .....	<b>66</b>
<b>C.1</b>	<b>Purpose</b> .....	<b>66</b>
<b>Annex D</b>	<b>(normative) Approved sensitive security parameter generation and establishment methods</b> .....	<b>68</b>
<b>D.1</b>	<b>Purpose</b> .....	<b>68</b>
<b>Annex E</b>	<b>(normative) Approved authentication mechanisms</b> .....	<b>69</b>
<b>E.1</b>	<b>Purpose</b> .....	<b>69</b>
<b>Annex F</b>	<b>(normative) Approved non-invasive attack mitigation test metrics</b> .....	<b>70</b>
<b>F.1</b>	<b>Purpose</b> .....	<b>70</b>
	<b>Bibliography</b> .....	<b>71</b>

## 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 shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19790 was prepared by Technical Committee ISO/TC 2, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 19790:2006), which has been technically revised. It also revises ISO/IEC 19790:2006/Cor 1:2008.

## Introduction

In Information Technology there is an ever-increasing need to use cryptographic mechanisms such as the protection of data against unauthorised 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 International Standard provides for 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. 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 of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilised 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 utilise cryptographic modules provide an acceptable 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, compliance with this International Standard 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;
- software development;
- 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.

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

## 1 Scope

This International Standard specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems. This International Standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location). This International Standard specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level.

This International Standard specifies security requirements specified intended to maintain the security provided by a cryptographic module and compliance to this International Standard is not sufficient to ensure that a particular 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.

## 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.

The documents listed in Annexes C, D, E and F of this International Standard