

Second edition  
2012-08-15

Corrected version  
2015-12-15

---

---

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

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

---

---

Reference number  
ISO/IEC 19790:2012(E)





**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2012, 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

| <b>Contents</b> | <b>Page</b>  |
|-----------------|--|
| <b>1</b>        | <b>Scope</b> ..... 1   |
| <b>2</b>        | <b>Normative references</b> ..... 1  |
| <b>3</b>        | <b>Terms and definitions</b> ..... 1   |
| <b>4</b>        | <b>Abbreviated terms</b> ..... 15  |
| <b>5</b>        | <b>Cryptographic module security levels</b> ..... 15   |
| <b>5.1</b>      | <b>Security Level 1</b> ..... 15   |
| <b>5.2</b>      | <b>Security Level 2</b> ..... 16   |
| <b>5.3</b>      | <b>Security Level 3</b> ..... 16   |
| <b>5.4</b>      | <b>Security Level 4</b> ..... 17   |
| <b>6</b>        | <b>Functional security objectives</b> ..... 17   |
| <b>7</b>        | <b>Security requirements</b> ..... 18  |
| <b>7.1</b>      | <b>General</b> ..... 18  |
| <b>7.2</b>      | <b>Cryptographic module specification</b> ..... 20   |
| <b>7.2.1</b>    | <b>Cryptographic module specification general requirements</b> ..... 20                              |
| <b>7.2.2</b>    | <b>Types of cryptographic modules</b> ..... 20   |
| <b>7.2.3</b>    | <b>Cryptographic boundary</b> ..... 21   |
| <b>7.2.4</b>    | <b>Modes of operations</b> ..... 22  |
| <b>7.3</b>      | <b>Cryptographic module interfaces</b> ..... 23  |
| <b>7.3.1</b>    | <b>Cryptographic module interfaces general requirements</b> ..... 23                                 |
| <b>7.3.2</b>    | <b>Types of interfaces</b> ..... 24  |
| <b>7.3.3</b>    | <b>Definition of interfaces</b> ..... 24   |
| <b>7.3.4</b>    | <b>Trusted channel</b> ..... 25  |
| <b>7.4</b>      | <b>Roles, services, and authentication</b> ..... 25  |
| <b>7.4.1</b>    | <b>Roles, services, and authentication general requirements</b> ..... 25                             |
| <b>7.4.2</b>    | <b>Roles</b> ..... 26  |
| <b>7.4.3</b>    | <b>Services</b> ..... 26   |
| <b>7.4.4</b>    | <b>Authentication</b> ..... 28   |
| <b>7.5</b>      | <b>Software/Firmware security</b> ..... 29   |
| <b>7.6</b>      | <b>Operational environment</b> ..... 31  |
| <b>7.6.1</b>    | <b>Operational environment general requirements</b> ..... 31   |
| <b>7.6.2</b>    | <b>Operating system requirements for limited or non-modifiable operational environments</b> ..... 33 |
| <b>7.6.3</b>    | <b>Operating system requirements for modifiable operational environments</b> ..... 33                |
| <b>7.7</b>      | <b>Physical security</b> ..... 35  |
| <b>7.7.1</b>    | <b>Physical security embodiments</b> ..... 35  |
| <b>7.7.2</b>    | <b>Physical security general requirements</b> ..... 37   |
| <b>7.7.3</b>    | <b>Physical security requirements for each physical security embodiment</b> ..... 39                 |
| <b>7.7.4</b>    | <b>Environmental failure protection/testing</b> ..... 42   |
| <b>7.8</b>      | <b>Non-invasive security</b> ..... 43  |
| <b>7.9</b>      | <b>Sensitive security parameter management</b> ..... 44  |
| <b>7.9.1</b>    | <b>Sensitive security parameter management general requirements</b> ..... 44                         |
| <b>7.9.2</b>    | <b>Random bit generators</b> ..... 44  |
| <b>7.9.3</b>    | <b>Sensitive security parameter generation</b> ..... 44  |
| <b>7.9.4</b>    | <b>Sensitive security parameter establishment</b> ..... 45   |
| <b>7.9.5</b>    | <b>Sensitive security parameter entry and output</b> ..... 45  |
| <b>7.9.6</b>    | <b>Sensitive security parameter storage</b> ..... 46   |