

# ISO/IEC 19790:2012-08 (E)

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

---

| <b>Contents</b> |   | <b>Page</b> |
|-----------------|---|-------------|
| <b>1</b>        | <b>Scope .....</b>  | <b>1</b>    |
| <b>2</b>        | <b>Normative references .....</b>   | <b>1</b>    |
| <b>3</b>        | <b>Terms and definitions .....</b>  | <b>1</b>    |
| <b>4</b>        | <b>Abbreviated terms .....</b>  | <b>15</b>   |
| <b>5</b>        | <b>Cryptographic module security levels .....</b>                                       | <b>15</b>   |
| 5.1             | Security Level 1 .....  | 15          |
| 5.2             | Security Level 2 .....  | 16          |
| 5.3             | Security Level 3 .....  | 16          |
| 5.4             | Security Level 4 .....  | 17          |
| <b>6</b>        | <b>Functional security objectives .....</b>   | <b>17</b>   |
| <b>7</b>        | <b>Security requirements .....</b>  | <b>18</b>   |
| 7.1             | General .....   | 18          |
| 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 .....   | 24          |
| 7.3.3           | Definition of interfaces .....  | 24          |
| 7.3.4           | Trusted channel .....   | 25          |
| 7.4             | Roles, services, and authentication .....   | 25          |
| 7.4.1           | Roles, services, and authentication general requirements .....                          | 25          |
| 7.4.2           | Roles .....   | 26          |
| 7.4.3           | Services .....  | 26          |
| 7.4.4           | Authentication .....  | 28          |
| 7.5             | Software/Firmware security .....  | 29          |
| 7.6             | Operational environment .....   | 31          |
| 7.6.1           | Operational environment general requirements .....                                      | 31          |
| 7.6.2           | Operating system requirements for limited or non-modifiable operational environments .. | 33          |
| 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 .....              | 39          |
| 7.7.4           | Environmental failure protection/testing .....  | 42          |
| 7.8             | Non-invasive security .....   | 43          |
| 7.9             | Sensitive security parameter management .....   | 44          |
| 7.9.1           | Sensitive security parameter management general requirements .....                      | 44          |
| 7.9.2           | Random bit generators .....   | 44          |
| 7.9.3           | Sensitive security parameter generation .....   | 44          |
| 7.9.4           | Sensitive security parameter establishment .....  | 45          |
| 7.9.5           | Sensitive security parameter entry and output .....                                     | 45          |
| 7.9.6           | Sensitive security parameter storage .....  | 46          |

|   |   |           |
|---|---|-----------|
| 7.9.7   | Sensitive security parameter zeroisation .....  | 46        |
| 7.10  | Self-tests .....                                | 47        |
| 7.10.1  | Self-test general requirements .....            | 47        |
| 7.10.2  | Pre-operational self-tests .....                | 47        |
| 7.10.3  | Conditional self-tests .....                    | 48        |
| 7.11  | Life-cycle assurance .....                      | 50        |
| 7.11.1  | Life-cycle assurance general requirements ..... | 50        |
| 7.11.2  | Configuration management .....                  | 51        |
| 7.11.3  | Design .....                                    | 51        |
| 7.11.4  | Finite state model .....                        | 51        |
| 7.11.5  | Development .....                               | 52        |
| 7.11.6  | Vendor testing .....                            | 53        |
| 7.11.7  | Delivery and operation .....                    | 54        |
| 7.11.8  | End of life .....                               | 54        |
| 7.11.9  | Guidance documents .....                        | 54        |
| 7.12  | Mitigation of other attacks .....               | 55        |
| <b>Annex A (normative) Documentation requirements .....</b>           |   | <b>56</b> |
| A.1   | Purpose .....                                   | 56        |
| A.2   | Items .....                                     | 56        |
| A.2.1   | General .....                                   | 56        |
| A.2.2   | Cryptographic module specification .....        | 56        |
| A.2.3   | Cryptographic module interfaces .....           | 57        |
| A.2.4   | Roles, services, and authentication .....       | 57        |
| A.2.5   | Software/Firmware security .....                | 57        |
| A.2.6   | Operational environment .....                   | 58        |
| A.2.7   | Physical security .....                         | 58        |
| A.2.8   | Non-invasive security .....                     | 58        |
| A.2.9   | Sensitive security parameter management .....   | 58        |
| A.2.10  | Self-tests .....                                | 59        |
| A.2.11  | Life-cycle assurance .....                      | 60        |
| A.2.12  | Mitigation of other attacks .....               | 61        |
| <b>Annex B (normative) Cryptographic module security policy .....</b> |   | <b>62</b> |
| B.1   | General .....                                   | 62        |
| B.2   | Items .....                                     | 62        |
| B.2.1   | General .....                                   | 62        |
| B.2.2   | Cryptographic module specification .....        | 62        |
| B.2.3   | Cryptographic module interfaces .....           | 63        |
| B.2.4   | Roles, services, and authentication .....       | 63        |
| B.2.5   | Software/Firmware security .....                | 64        |
| B.2.6   | Operational environment .....                   | 64        |
| B.2.7   | Physical security .....                         | 64        |
| B.2.8   | Non-invasive security .....                     | 65        |
| B.2.9   | Sensitive security parameters management .....  | 65        |
| B.2.10  | Self-tests .....                                | 66        |
| B.2.11  | Life-cycle assurance .....                      | 66        |
| B.2.12  | Mitigation of other attacks .....               | 66        |
| <b>Annex C (normative) Approved security functions .....</b>          |   | <b>67</b> |
| C.1   | Purpose .....                                   | 67        |
| C.1.1   | Block ciphers .....                             | 67        |
| C.1.2   | Stream ciphers .....                            | 67        |
| C.1.3   | Asymmetric algorithms and techniques .....      | 67        |
| C.1.4   | Message authentication codes .....              | 67        |
| C.1.5   | Hash functions .....                            | 67        |
| C.1.6   | Entity authentication .....                     | 68        |
| C.1.7   | Key management .....                            | 68        |
| C.1.8   | Random bit generation .....                     | 68        |

|   |           |
|---|-----------|
| <b>Annex D (normative) Approved sensitive security parameter generation and establishment methods</b> | <b>69</b> |
| <b>D.1 Purpose</b>  | <b>69</b> |
| <b>D.1.1 Sensitive security parameter generation</b>  | <b>69</b> |
| <b>D.1.2 Sensitive security parameter establishment methods</b>                                       | <b>69</b> |
| <b>Annex E (normative) Approved authentication mechanisms</b>   | <b>70</b> |
| <b>E.1 Purpose</b>  | <b>70</b> |
| <b>E.1.1 Authentication mechanisms</b>  | <b>70</b> |
| <b>Annex F (normative) Approved non-invasive attack mitigation test metrics</b>                       | <b>71</b> |
| <b>F.1 Purpose</b>  | <b>71</b> |
| <b>F.1.1 Non-invasive attack mitigation test metrics</b>  | <b>71</b> |