

ISO/IEC 19790:2025-02 (E)

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

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
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