

DIN EN ISO/IEC 19790:2020-08 (E)

Information technology - Security techniques - Security requirements for cryptographic modules (ISO/IEC 19790:2012, Corrected version 2015-12)

Contents		Page
European foreword		5
Foreword		6
Introduction		8
1 Scope		9
2 Normative references		9
3 Terms and definitions		9
4 Abbreviated terms		23
5 Cryptographic module security levels		23
5.1 Security Level 1		23
5.2 Security Level 2		24
5.3 Security Level 3		24
5.4 Security Level 4		25
6 Functional security objectives		25
7 Security requirements		26
7.1 General		26
7.2 Cryptographic module specification		28
7.2.1 Cryptographic module specification general requirements		28
7.2.2 Types of cryptographic modules		28
7.2.3 Cryptographic boundary		28
7.2.4 Modes of operations		30
7.3 Cryptographic module interfaces		31
7.3.1 Cryptographic module interfaces general requirements		31
7.3.2 Types of interfaces		32
7.3.3 Definition of interfaces		32
7.3.4 Trusted channel		33
7.4 Roles, services, and authentication		33
7.4.1 Roles, services, and authentication general requirements		33
7.4.2 Roles		34
7.4.3 Services		34
7.4.4 Authentication		36
7.5 Software/Firmware security		37
7.6 Operational environment		39
7.6.1 Operational environment general requirements		39
7.6.2 Operating system requirements for limited or non-modifiable operational environments		41
7.6.3 Operating system requirements for modifiable operational environments		41
7.7 Physical security		43
7.7.1 Physical security embodiments		43
7.7.2 Physical security general requirements		45
7.7.3 Physical security requirements for each physical security embodiment		47
7.7.4 Environmental failure protection/testing		50
7.8 Non-invasive security		51
7.9 Sensitive security parameter management		52
7.9.1 Sensitive security parameter management general requirements		52
7.9.2 Random bit generators		52
7.9.3 Sensitive security parameter generation		52
7.9.4 Sensitive security parameter establishment		53
7.9.5 Sensitive security parameter entry and output		53
7.9.6 Sensitive security parameter storage		54

7.9.7	Sensitive security parameter zeroisation.....	54
7.10	Self-tests.....	55
7.10.1	Self-test general requirements.....	55
7.10.2	Pre-operational self-tests.....	55
7.10.3	Conditional self-tests.....	56
7.11	Life-cycle assurance.....	58
7.11.1	Life-cycle assurance general requirements.....	58
7.11.2	Configuration management.....	59
7.11.3	Design.....	59
7.11.4	Finite state model.....	59
7.11.5	Development.....	60
7.11.6	Vendor testing.....	61
7.11.7	Delivery and operation.....	62
7.11.8	End of life.....	62
7.11.9	Guidance documents.....	62
7.12	Mitigation of other attacks.....	63
Annex A	(normative) Documentation requirements.....	64
A.1	Purpose.....	64
A.2	Items.....	64
A.2.1	General.....	64
A.2.2	Cryptographic module specification.....	64
A.2.3	Cryptographic module interfaces.....	65
A.2.4	Roles, services, and authentication.....	65
A.2.5	Software/Firmware security.....	65
A.2.6	Operational environment.....	66
A.2.7	Physical security.....	66
A.2.8	Non-invasive security.....	66
A.2.9	Sensitive security parameter management.....	66
A.2.10	Self-tests.....	67
A.2.11	Life-cycle assurance.....	68
A.2.12	Mitigation of other attacks.....	69
Annex B	(normative) Cryptographic module security policy.....	70
B.1	General.....	70
B.2	Items.....	70
B.2.1	General.....	70
B.2.2	Cryptographic module specification.....	70
B.2.3	Cryptographic module interfaces.....	71
B.2.4	Roles, services, and authentication.....	71
B.2.5	Software/Firmware security.....	72
B.2.6	Operational environment.....	72
B.2.7	Physical security.....	72
B.2.8	Non-invasive security.....	73
B.2.9	Sensitive security parameters management.....	73
B.2.10	Self-tests.....	74
B.2.11	Life-cycle assurance.....	74
B.2.12	Mitigation of other attacks.....	74
Annex C	(normative) Approved security functions.....	75
C.1	Purpose.....	75
C.1.1	Block ciphers.....	75
C.1.2	Stream ciphers.....	75
C.1.3	Asymmetric algorithms and techniques.....	75
C.1.4	Message authentication codes.....	75
C.1.5	Hash functions.....	75
C.1.6	Entity authentication.....	76

C.1.7 Key management76
C.1.8 Random bit generation.....76
Annex D (normative) Approved sensitive security parameter generation and establishment methods77
D.1 Purpose.....77
D.1.1 Sensitive security parameter generation77
D.1.2 Sensitive security parameter establishment methods77
Annex E (normative) Approved authentication mechanisms78
E.1 Purpose.....78
E.1.1 Authentication mechanisms.....78
Annex F (normative) Approved non-invasive attack mitigation test metrics79
F.1 Purpose.....79
F.1.1 Non-invasive attack mitigation test metrics79
Bibliography80