

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

Informationstechnik - Sicherheitstechniken - Sicherheitsanforderungen für
kryptografische Module (ISO/IEC 19790:2012, korrigierte Fassung 2015-12); Deutsche
Fassung EN ISO/IEC 19790:2020

Inhalt	Seite
Europäisches Vorwort.....	5
Vorwort.....	6
Einleitung.....	8
1 Anwendungsbereich.....	9
2 Normative Verweisungen.....	9
3 Begriffe.....	9
4 Abkürzungen.....	24
5 Sicherheitsstufen für Krypto-Module.....	25
5.1 Sicherheitsstufe 1.....	25
5.2 Sicherheitsstufe 2.....	25
5.3 Sicherheitsstufe 3.....	26
5.4 Sicherheitsstufe 4.....	26
6 Funktionale Sicherheitsziele.....	27
7 Sicherheitsanforderungen.....	28
7.1 Allgemeines.....	28
7.2 Spezifikation des Krypto-Moduls.....	30
7.2.1 Allgemeine Anforderungen an die Spezifikation des Krypto-Moduls.....	30
7.2.2 Arten von Krypto-Modulen.....	31
7.2.3 Kryptografische Begrenzung.....	31
7.2.4 Betriebsarten.....	33
7.3 Schnittstellen des Krypto-Moduls.....	34
7.3.1 Allgemeine Anforderungen an die Schnittstellen des Krypto-Moduls.....	34
7.3.2 Arten von Schnittstellen.....	34
7.3.3 Definition der Schnittstellen.....	35
7.3.4 Vertrauenswürdiger Kanal.....	36
7.4 Rollen, Dienste und Authentifizierung.....	36
7.4.1 Allgemeine Anforderungen an Rollen, Dienste und Authentifizierung.....	36
7.4.2 Rollen.....	37
7.4.3 Dienste.....	37
7.4.4 Authentifizierung.....	39
7.5 Software-/Firmware-Sicherheit.....	41
7.6 Betriebsumgebung.....	43
7.6.1 Allgemeine Anforderungen an die Betriebsumgebung.....	43
7.6.2 Anforderungen an das Betriebssystem in begrenzten oder nicht modifizierbaren Betriebsumgebungen.....	45
7.6.3 Anforderungen an das Betriebssystem in modifizierbaren Betriebsumgebungen.....	45
7.7 Physische Sicherheit.....	48
7.7.1 Ausführungen der physischen Sicherheit.....	48
7.7.2 Allgemeine Anforderungen an die physische Sicherheit.....	50
7.7.3 Physische Sicherheitsanforderungen für die jeweiligen physischen Sicherheitsausführungen.....	52
7.7.4 Prüfung auf umgebungsbedingten Ausfall.....	55

7.8	Sicherheit bei nicht-invasiven Angriffen	56
7.9	Verwaltung von sensiblen Sicherheitsparametern.....	57
7.9.1	Allgemeine Anforderungen an die Verwaltung von sensiblen Sicherheitsparametern.....	57
7.9.2	Zufallsbitgeneratoren	58
7.9.3	Erzeugung sensibler Sicherheitsparameter	58
7.9.4	Bereitstellung sensibler Sicherheitsparameter	58
7.9.5	Eingabe und Ausgabe von sensiblen Sicherheitsparametern.....	58
7.9.6	Speicherung sensibler Sicherheitsparameter	59
7.9.7	Löschen/Vernichten sensibler Sicherheitsparameter	60
7.10	Selbsttests.....	60
7.10.1	Allgemeine Anforderungen an Selbsttests	60
7.10.2	Vorbetriebliche Selbsttests	61
7.10.3	Bedingte Selbsttests	62
7.11	Lebenszyklussicherung.....	65
7.11.1	Allgemeine Anforderungen an die Lebenszyklussicherung.....	65
7.11.2	Konfigurationsmanagement.....	65
7.11.3	Auslegung	66
7.11.4	Endlicher Automat.....	66
7.11.5	Entwicklung	67
7.11.6	Prüfungen des Anbieters	68
7.11.7	Lieferung und Betrieb.....	69
7.11.8	Ende der Lebensdauer	69
7.11.9	Leitliniendokumente	69
7.12	Schadensminderung bei anderen Angriffen.....	70
Anhang A (normativ) Dokumentationsanforderungen.....		71
A.1	Zweck	71
A.2	Einheiten	71
A.2.1	Allgemeines.....	71
A.2.2	Spezifikation des Krypto-Moduls.....	71
A.2.3	Schnittstellen des Krypto-Moduls.....	72
A.2.4	Rollen, Dienste und Authentifizierung.....	72
A.2.5	Software-/Firmware-Sicherheit.....	72
A.2.6	Betriebsumgebung.....	73
A.2.7	Physische Sicherheit	73
A.2.8	Sicherheit bei nicht-invasiven Angriffen	73
A.2.9	Verwaltung von sensiblen Sicherheitsparametern.....	73
A.2.10	Selbsttests.....	74
A.2.11	Lebenszyklussicherung.....	75
A.2.12	Schadensminderung bei anderen Angriffen.....	76
Anhang B (normativ) Sicherheitsrichtlinie für das Krypto-Modul.....		77
B.1	Allgemeines.....	77
B.2	Einheiten	77
B.2.1	Allgemeines.....	77
B.2.2	Spezifikation des Krypto-Moduls.....	77
B.2.3	Schnittstellen des Krypto-Moduls.....	78
B.2.4	Rollen, Dienste und Authentifizierung.....	78
B.2.5	Software-/Firmware-Sicherheit.....	79
B.2.6	Betriebsumgebung.....	79
B.2.7	Physische Sicherheit	79
B.2.8	Sicherheit bei nicht-invasiven Angriffen	80
B.2.9	Verwaltung von sensiblen Sicherheitsparametern.....	80
B.2.10	Selbsttests.....	81
B.2.11	Lebenszyklussicherung.....	81
B.2.12	Schadensminderung bei anderen Angriffen.....	81
Anhang C (normativ) Genehmigte Sicherheitsfunktionen		82
C.1	Zweck	82

C.1.1	Blockziffern	82
C.1.2	Stromchiffren	82
C.1.3	Asymmetrische Algorithmen und Techniken	82
C.1.4	Mitteilungsauthentisierungs-codes	82
C.1.5	Hash-Funktionen	83
C.1.6	Authentifizierung von Entitäten	83
C.1.7	Schlüsselverwaltung	83
C.1.8	Generierung von zufälligen Bit	83
Anhang D (normativ) Genehmigte Verfahren zur Erzeugung und Bereitstellung sensibler		
	Sicherheitsparameter	84
D.1	Zweck	84
D.1.1	Erzeugung sensibler Sicherheitsparameter	84
D.1.2	Bereitstellungsverfahren für sensible Sicherheitsparameter	84
Anhang E (normativ) Genehmigte Authentifizierungsmechanismen		
E.1	Zweck	85
E.1.1	Authentifizierungsmechanismen	85
Anhang F (normativ) Genehmigte Prüfmetriken für die Schadensminderung bei nicht-invasiven		
	Angriffen	86
F.1	Zweck	86
F.1.1	Genehmigte Prüfmetriken für die Schadensminderung bei nicht-invasiven Angriffen	86
Literaturhinweise		87