

DIN EN ISO/IEC 19896-2:2024-03 (D)

IT-Sicherheitstechniken - Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit - Teil 2: Anforderungen an Wissen, Fähigkeiten und Effektivität für ISO/IEC 19790-Tester (ISO/IEC 19896-2:2018); Deutsche Fassung EN ISO/IEC 19896-2:2023

Inhalt	Seite
Europäisches Vorwort.....	8
Vorwort.....	9
Einleitung.....	10
1 Anwendungsbereich.....	11
2 Normative Verweisungen.....	11
3 Begriffe.....	11
4 Abkürzungen.....	12
5 Aufbau dieses Dokuments.....	12
6 Wissen.....	12
6.1 Allgemeines.....	12
6.2 Tertiäre Ausbildung.....	12
6.2.1 Allgemeines.....	12
6.2.2 Technische Fachrichtungen.....	12
6.2.3 Fachbezogene Themen.....	13
6.3 Wissen über die Normen.....	17
6.3.1 Allgemeines.....	17
6.3.2 ISO/IEC 19790-Konzepte.....	18
6.3.3 ISO/IEC 24759.....	18
6.3.4 Zusätzliche ISO/IEC-Normen.....	18
6.4 Wissen über das Validierungsprogramm.....	19
6.4.1 Validierungsprogramm.....	19
6.5 Wissen über die Anforderungen der ISO/IEC 17025.....	21
7 Fertigkeiten.....	21
7.1 Allgemeines.....	21
7.2 Prüfung von Algorithmen.....	21
7.3 Prüfung der physischen Sicherheit.....	21
7.4 Seitenkanalanalyse.....	21
7.5 Technologietypen.....	21
8 Erfahrung.....	22
8.1 Allgemeines.....	22
8.2 Nachweis der technischen Kompetenz für das Validierungsprogramm.....	22
8.2.1 Erfahrung mit der Durchführung von Prüfungen.....	22
8.2.2 Erfahrung mit bestimmten Technologietypen.....	22
9 Ausbildung.....	22
10 Effektivität.....	22
Anhang A (informativ) Beispiel für ein ISO/IEC 24759-Testerprotokoll.....	23
Anhang B (informativ) Ontologie der Technologietypen und der zugehörigen Wissensbestände.....	24
B.1 Allgemeines.....	24

B.2	Technologietypen.....	24
B.2.1	Allgemeines.....	24
B.2.2	Software/Firmware.....	24
Anhang C (informativ) Spezifisches Wissen im Zusammenhang mit der Sicherheit von		
	kryptographischen Modulen	28
C.1	Allgemeines.....	28
C.2	Spezifikation des kryptographischen Moduls	28
C.2.1	Allgemeines.....	28
C.2.2	Puffer.....	28
C.2.3	Sicherheitsrelevante Komponenten	29
C.2.4	Identifizierung von programmierbaren Schnittstellen, Debugging-Schnittstellen und verdeckten Kanälen.....	29
C.2.5	Identifizierung von genehmigten und nicht genehmigten Sicherheitsfunktionen.....	29
C.2.6	Ausschluss von Komponenten	30
C.2.7	Eingeschränkter Betrieb.....	30
C.3	Schnittstellen des kryptographischen Moduls	31
C.3.1	Überblick.....	31
C.3.2	Abstand der Eingabedaten von den Ausgabedaten.....	32
C.3.3	Wissen über kritische Sicherheitsfunktionen, Dienste oder sicherheitsrelevante Dienste	32
C.3.4	Vertrauenswürdiger Kanal	32
C.4	Rollen, Dienste und Authentisierung.....	33
C.4.1	Allgemeines.....	33
C.4.2	Dienste.....	33
C.4.3	Authentisierung.....	34
C.5	Sicherheit der Software/Firmware	35
C.6	Betriebsumgebung.....	35
C.6.1	Prozessspeicherverwaltung	35
C.6.2	Laden	35
C.6.3	Verknüpfen.....	35
C.6.4	Virtueller Speicher.....	35
C.7	Physische Sicherheit	35
C.8	Nicht-invasive Sicherheit.....	36
C.9	Handhabung sensibler Sicherheitsparameter.....	36
C.9.1	Allgemeines.....	36
C.9.2	Kennwort gegenüber kryptographischem Schlüssel.....	36
C.9.3	Entropie gegenüber dem Wissen der Angreifer	37
C.9.4	SSP-Hierarchie	37
C.9.5	Autorisierte Rollen für das SSP-Management.....	37
C.9.6	Nullsetzung.....	38
C.10	Selbsttests.....	38
C.10.1	Allgemeines.....	38
C.10.2	Kritische Funktionen	39
C.10.3	Vorbetriebliche Integritätsprüfung der Software/Firmware.....	40
C.10.4	Bedingte Selbsttests des kryptographischen Algorithmus.....	41
C.10.5	Paarweise Konsistenzprüfung	41
C.11	Vertrauenswürdiger Lebenszyklus.....	41
C.11.1	Allgemeines.....	41
C.11.2	Konfigurationsmanagement.....	42
C.11.3	Endlicher Automat.....	42
C.11.4	Entwicklung	43
C.11.5	Prüfung von Anbietern	44
C.11.6	Auslieferung und Betrieb	46
C.11.7	Ende der Nutzungsdauer	46
C.11.8	Leitfäden	46
C.12	Abschwächung anderer Angriffe.....	46
Anhang D (informativ) Kompetenzanforderungen an ISO/IEC 19790-Validierer		
		47

Literaturhinweise	48
--------------------------------	-----------

Bilder

Bild C.1 — Überblick über die Spezifikation des kryptographischen Moduls.....	28
Bild C.2 — Beispiel für Zustandsübergänge, die eine eingeschränkte Funktionalität unterstützen	31
Bild C.3 — Überblick über die Schnittstellen des kryptographischen Moduls	32
Bild C.4 — Überblick über Rollen, Dienste und Authentisierung.....	33
Bild C.5 — Überblick über die Zugangssteuerungsrichtlinie.....	34
Bild C.6 — Überblick über das SSP-Management.....	36
Bild C.7 — Überblick über die Selbsttests	39