

E DIN EN ISO/IEC 19896-2:2025-02 (D/E)

Erscheinungsdatum: 2025-01-10

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Anforderungen an die Kompetenz des Personals von Konformitätsbewertungsstellen für IT-Sicherheit - Teil 2: Anforderungen an die Kenntnisse und Fähigkeiten von Testern und Validierern nach ISO/IEC 19790 (ISO/IEC DIS 19896-2:2024); Deutsche und Englische Fassung prEN ISO/IEC 19896-2:2024

Information security, cybersecurity and privacy protection - Requirements for the competence of IT security conformance assessment body personnel - Part 2: Knowledge and skills requirements for ISO/IEC 19790 testers and validators (ISO/IEC DIS 19896-2:2024); German and English version prEN ISO/IEC 19896-2:2024

Inhalt	Seite
Europäisches Vorwort.....	8
Vorwort.....	9
Einleitung.....	11
1 Anwendungsbereich.....	12
2 Normative Verweisungen.....	12
3 Begriffe.....	12
4 Abkürzungen.....	13
5 Aufbau dieses Dokuments.....	13
6 Wissen.....	13
6.1 Allgemeines.....	13
6.2 Tester.....	13
6.2.1 Tertiäre Ausbildung.....	13
6.2.2 Wissen über Normen.....	19
6.2.3 Wissen über das Validierungsprogramm.....	20
6.2.4 Wissen über die Anforderungen der ISO/IEC 23532-2.....	22
6.3 Validierer.....	22
6.3.1 Tertiäre Ausbildung.....	22
6.3.2 Wissen über die Norm.....	22
6.3.3 Wissen über das Validierungsprogramm.....	22
6.3.4 Wissen über die Anforderungen der ISO/IEC 23532-2 und die Validierungsinstanz.....	24
7 Fertigkeiten.....	24
7.1 Tester.....	24
7.1.1 Allgemeines.....	24
7.1.2 Prüfung von Algorithmen.....	24
7.1.3 Prüfung der physischen Sicherheit.....	24
7.1.4 Seitenkanalanalyse.....	24
7.1.5 Technologietypen.....	24
7.2 Validierer.....	25
Anhang A (informativ) Beispiel für ein ISO/IEC 24759-Tester- und Validiererprotokoll.....	26
Anhang B (informativ) Ontologie der Technologietypen.....	28
B.1 Allgemeines.....	28
B.2 Technologietypen.....	28
B.2.1 Allgemeines.....	28

B.2.2	Software/Firmware.....	28
Anhang C (informativ) Spezifisches Wissen im Zusammenhang mit der Sicherheit von		
kryptographischen Modulen, die auf die Konformität mit ISO/IEC 19790:2012 geprüft		
werden.....		
		32
C.1	Allgemeines.....	32
C.2	Spezifikation des kryptographischen Moduls	32
C.2.1	Allgemeines.....	32
C.2.2	Puffer.....	33
C.2.3	Sicherheitsrelevante Komponenten	33
C.2.4	Identifizierung von programmierbaren Schnittstellen und Debugging-Schnittstellen	33
C.2.5	Identifizierung von genehmigten und nicht genehmigten Sicherheitsfunktionen.....	33
C.2.6	Ausschluss von Komponenten	34
C.2.7	Eingeschränkter Betrieb.....	34
C.3	Schnittstellen des kryptographischen Moduls	35
C.3.1	Überblick.....	35
C.3.2	Trennung der Eingabedaten von den Ausgabedaten.....	36
C.3.3	Wissen über kritische Sicherheitsfunktionen, Dienste oder sicherheitsrelevante Dienste.....	36
C.3.4	Vertrauenswürdiger Kanal	36
C.4	Rollen, Dienste und Authentisierung.....	36
C.4.1	Allgemeines.....	36
C.4.2	Dienste.....	37
C.4.3	Authentisierung.....	38
C.5	Sicherheit der Software/Firmware	38
C.6	Betriebsumgebung.....	39
C.6.1	Prozessspeicherverwaltung	39
C.6.2	Laden	39
C.6.3	Linking.....	39
C.6.4	Virtueller Speicher.....	39
C.7	Physische Sicherheit	39
C.8	Nicht-invasive Sicherheit.....	39
C.9	Handhabung sensibler Sicherheitsparameter.....	40
C.9.1	Allgemeines.....	40
C.9.2	Entropie gegenüber dem Wissen der Angreifer.....	40
C.9.3	SSP-Hierarchie	41
C.9.4	Autorisierte Rollen für das SSP-Management.....	41
C.9.5	Nullsetzung.....	41
C.10	Selbsttests.....	42
C.10.1	Allgemeines.....	42
C.10.2	Kritische Funktionen	43
C.10.3	Vorbetriebliche Integritätsprüfung der Software/Firmware.....	44
C.10.4	Bedingte Selbsttests der kryptographischen Algorithmen	45
C.10.5	Paarweise Konsistenzprüfung	45
C.11	Vertrauenswürdiger Lebenszyklus.....	45
C.11.1	Allgemeines.....	45
C.11.2	Konfigurationsmanagement.....	45
C.11.3	Endlicher Automat.....	46
C.11.4	Entwicklung	46
C.11.5	Prüfung von Anbietern	48
C.11.6	Auslieferung und Betrieb	49
C.11.7	Ende der Nutzungsdauer	50
C.11.8	Leitfäden	50
C.12	Abschwächung sonstiger Angriffe	50
	Literaturhinweise.....	51

Bilder

Bild C.1 — Überblick über die Spezifikation des kryptographischen Moduls.....	32
Bild C.2 — Beispiel für Zustandsübergänge, die eine eingeschränkte Funktionalität unterstützen	35
Bild C.3 — Überblick über die Schnittstellen des kryptographischen Moduls	36
Bild C.4 — Überblick über Rollen, Dienste und Authentisierung.....	37
Bild C.5 — Überblick über die Zugangssteuerungsrichtlinie.....	38
Bild C.6 — Überblick über das SSP-Management.....	40
Bild C.7 — Überblick über die Selbsttests.....	43

Tabellen

Tabelle A.1 — Beispiel für ein ISO/IEC 24759-Testerprotokoll	26
Tabelle A.2 — Beispiel für ein ISO/IEC 24759-Validiererprotokoll	26