DIN EN ISO/IEC 19896-2

ICS 35.030

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

IT security techniques –
Competence requirements for information security testers and evaluators –
Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers (ISO/IEC 19896-2:2018);
German version EN ISO/IEC 19896-2:2023

Techniques de sécurité IT –
Exigences de compétence pour l'information testeurs d'assurance et les évaluateurs –
Partie 2: Exigences en matière de connaissances, de compétences et d'efficacité pour ISO/IEC 19790 testeurs (ISO/IEC 19896-2:2018);
Version allemande EN ISO/IEC 19896-2:2023

Gesamtumfang 48 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-2:2024-03

Nationales Vorwort

Der Text von ISO/IEC 19896-2:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 19896-2:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Arbeitskreis NA 043-04-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 17025	siehe	DIN EN ISO/IEC 17025
ISO/IEC 19790	siehe	DIN EN ISO/IEC 19790
ISO/IEC 19896-1	siehe	E DIN EN ISO/IEC 19896-1

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-2:2024-03

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 17025, *Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien*

DIN EN ISO/IEC 19790, *Informationstechnik — Sicherheitstechniken — Sicherheitsanforderungen für kryptografische Module*

E DIN EN ISO/IEC 19896-1, *IT-Sicherheitstechniken — Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit — Teil 1: Einführung, Konzepte und allgemeine Anforderungen*

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-2:2024-03

– Leerseite –

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-2:2024-03

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 19896-2

Januar 2023

ICS 35.030

Deutsche Fassung

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)

IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers (ISO/IEC 19896-2:2018)

Techniques de sécurit IT — Exigences de comp tence pour l'information testeurs d'assurance et les valuateurs — Partie 2: Exigences en matière de connaissances, de comp tences et d'efficacit pour ISO/IEC 19790 testeurs (ISO/IEC 19896-2:2018)

Diese Europäische Norm wurde vom CEN am 9. Januar 2023 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management-Zentrum:
Rue de la Science 23, B-1040 Brüssel

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-2:2024-03

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 6
1 Anwendungsbereich 7
2 Normative Verweisungen 7
3 Begriffe 7
4 Abkürzungen 7
5 Aufbau dieses Dokuments 8
6 Wissen 8
6.1 Allgemeines 8
6.2 Tertiäre Ausbildung 8
6.2.1 Allgemeines 8
6.2.2 Technische Fachrichtungen 8
6.2.3 Fachbezogene Themen 9
6.3 Wissen über die Normen 13
6.3.1 Allgemeines 13
6.3.2 ISO/IEC 19790-Konzepte 13
6.3.3 ISO/IEC 24759 13
6.3.4 Zusätzliche ISO/IEC-Normen 14
6.4 Wissen über das Validierungsprogramm 14
6.4.1 Validierungsprogramm 14
6.5 Wissen über die Anforderungen der ISO/IEC 17025 16
7 Fertigkeiten 16
7.1 Allgemeines 16
7.2 Prüfung von Algorithmen 16
7.3 Prüfung der physischen Sicherheit 17
7.4 Seitenkanalanalyse 17
7.5 Technologietypen 17
8 Erfahrung 17
8.1 Allgemeines 17
8.2 Nachweis der technischen Kompetenz für das Validierungsprogramm 17
8.2.1 Erfahrung mit der Durchführung von Prüfungen 17
8.2.2 Erfahrung mit bestimmten Technologietypen 17
9 Ausbildung 17
10 Effektivität 18
Anhang A (informativ) Beispiel für ein ISO/IEC 24759-Testerprotokoll 19
Anhang B (informativ) Ontologie der Technologietypen und der zugehörigen Wissensbestände . 20
B.1 Allgemeines 20
B.2 Technologietypen 20
B.2.1 Allgemeines 20
B.2.2 Software/Firmware 20
Anhang C (informativ) Spezifisches Wissen im Zusammenhang mit der Sicherheit von kryptographischen Modulen 24
C.1 Allgemeines 24
C.2 Spezifikation des kryptographischen Moduls 24
C.2.1 Allgemeines 24
C.2.2 Puffer 24
C.2.3 Sicherheitsrelevante Komponenten 25
C.2.4 Identifizierung von programmierbaren Schnittstellen, Debugging-Schnittstellen und verdeckten Kanälen 25
C.2.5 Identifizierung von genehmigten und nicht genehmigten Sicherheitsfunktionen 25

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 19896-2:2024-03

C.2.6 Ausschluss von Komponenten . . . 25
C.2.7 Eingeschränkter Betrieb . . . 26
C.3 Schnittstellen des kryptographischen Moduls . . . 27
C.3.1 Überblick . . . 27
C.3.2 Abstand der Eingabedaten von den Ausgabedaten . . . 28
C.3.3 Wissen über kritische Sicherheitsfunktionen, Dienste oder sicherheitsrelevante Dienste 28
C.3.4 Vertrauenswürdiger Kanal . . . 28
C.4 Rollen, Dienste und AuthentisierungAuthentisierung . . . 29
C.4.1 Allgemeines . . . 29
C.4.2 Dienste . . . 29
C.4.3 Authentisierung . . . 30
C.5 Sicherheit der Software/Firmware . . . 31
C.6 Betriebsumgebung . . . 31
C.6.1 Prozessspeicherverwaltung . . . 31
C.6.2 Laden . . . 31
C.6.3 Verknüpfen . . . 31
C.6.4 Virtueller Speicher . . . 31
C.7 Physische Sicherheit . . . 31
C.8 Nicht-invasive Sicherheit . . . 31
C.9 Handhabung sensibler Sicherheitsparameter . . . 32
C.9.1 Allgemeines . . . 32
C.9.2 Kennwort gegenüber kryptographischem Schlüssel . . . 32
C.9.3 Entropie gegenüber dem Wissen der Angreifer . . . 32
C.9.4 SSP-Hierarchie . . . 33
C.9.5 Autorisierte Rollen für das SSP-Management . . . 33
C.9.6 Nullsetzung . . . 34
C.10 Selbsttests . . . 34
C.10.1 Allgemeines . . . 34
C.10.2 Kritische Funktionen . . . 35
C.10.3 Vorbetriebliche Integritätsprüfung der Software/Firmware . . . 36
C.10.4 Bedingte Selbsttests des kryptographischen Algorithmus . . . 37
C.10.5 Paarweise Konsistenzprüfung . . . 37
C.11 Vertrauenswürdiger Lebenszyklus . . . 37
C.11.1 Allgemeines . . . 37
C.11.2 Konfigurationsmanagement . . . 37
C.11.3 Endlicher Automat . . . 38
C.11.4 Entwicklung . . . 38
C.11.5 Prüfung von Anbietern . . . 40
C.11.6 Auslieferung und Betrieb . . . 41
C.11.7 Ende der Nutzungsdauer . . . 42
C.11.8 Leitfäden . . . 42
C.12 Abschwächung anderer Angriffe . . . 42
Anhang D (informativ) **Kompetenzanforderungen an ISO/IEC 19790-Validierer** . . . 43
Literaturhinweise . . . 44

Bilder

Bild C.1 — Überblick über die Spezifikation des kryptographischen Moduls . . . 24
Bild C.2 — Beispiel für Zustandsübergänge, die eine eingeschränkte Funktionalität unterstützen 27
Bild C.3 — Überblick über die Schnittstellen des kryptographischen Moduls . . . 28
Bild C.4 — Überblick über Rollen, Dienste und Authentisierung . . . 29
Bild C.5 — Überblick über die Zugangssteuerungsrichtlinie . . . 30
Bild C.6 — Überblick über das SSP-Management . . . 32
Bild C.7 — Überblick über die Selbsttests . . . 35

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-2:2024-03

Europäisches Vorwort

Der Text von ISO/IEC 19896-2:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 19896-2:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juli 2023 und etwaige entgegenstehende nationale Normen müssen bis Juli 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Entsprechend der CEN CENELEC Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 19896-2:2018 wurde von CEN als EN ISO/IEC 19896-2:2023 ohne irgendeine Abänderung genehmigt.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-2:2024-03

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques,* erarbeitet.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 19896 kann auf der ISO-Internetseite abgerufen werden.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 19896-2:2024-03

Einleitung

Dieses Dokument enthält die speziellen Anforderungen zum Nachweis von Wissen, Fertigkeiten und Anforderungen an die Effektivität von Personen bei der Durchführung von Sicherheitsprüfungsprojekten in Übereinstimmung mit ISO/IEC 19790 und ISO/IEC 24759. ISO/IEC 19790 enthält die Spezifikation der Sicherheitsanforderungen für kryptographische Module. Zahlreiche Zertifizierungs-, Validierungs- und Anerkennungsmaßnahmen wurden auf dieser Grundlage entwickelt. ISO/IEC 19790 ermöglicht die Vergleichbarkeit der Ergebnisse unabhängiger Sicherheitsprüfungsprojekte. ISO/IEC 24759 unterstützt dies, indem es eine Reihe gemeinsamer Prüfungsanforderungen für die Prüfung eines kryptographischen Moduls auf Konformität mit ISO/IEC 19790 festlegt.

Ein wichtiger Faktor für die Vergleichbarkeit der Ergebnisse solcher Validierungen oder Zertifizierungen sind die Anforderungen an Wissen, Fertigkeiten und Effektivität der einzelnen Tester, die für die Durchführung von Prüfprojekten verantwortlich sind.

In der ISO/IEC 17025, die häufig als Norm für Prüfeinrichtungen angegeben wird, heißt es in 5.2.1: „Das Personal, das bestimmte Aufgaben ausführt, muss auf der Grundlage einer angemessenen Ausbildung, Schulung, Erfahrung und/oder nachgewiesener Fertigkeiten qualifiziert sein“.

Zur Zielgruppe dieses Dokuments gehören Validierungs- und Zertifizierungsinstanzen, Akkreditierungsstellen für Laborprüfungen, Prüfprojekte, Prüfeinrichtungen, Tester und Organisationen, die berufliche Qualifikationen und Anerkennungen anbieten.

Dieses Dokument legt eine Grundlage für die Anforderungen an Wissen, Fertigkeiten und Effektivität von ISO/IEC 19790-Testern fest, mit dem Ziel, Konformität in den Anforderungen an die Ausbildung von ISO/IEC 19790-Testern zu schaffen, die mit Konformitätsprüfprogrammen für kryptographische Module verbunden sind.

Anhang D veranschaulicht die Nützlichkeit dieses Dokuments für Validierer innerhalb eines Validierungsprogramms.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 19896-2:2024-03

1 Anwendungsbereich

Dieses Dokument enthält die Mindestanforderungen an Wissen, Fertigkeiten und Anforderungen an die Effektivität von Personen, die Prüftätigkeiten für ein Konformitätsschema im Rahmen von ISO/IEC 19790 und ISO/IEC 24759 durchführen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 17825, *Information technology— Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*

ISO/IEC 18367, *Information technology — Security techniques — Cryptographic algorithms and security mechanisms conformance testing*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 19896-1, *IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements*

ISO/IEC 20085-1, *Information technology — Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques*

ISO/IEC 20085-2, *Information technology — Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part: 2 Test calibration methods and apparatus*

ISO/IEC 20543, *Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408*

ISO/IEC 24759, *Information technology — Security techniques — Test requirements for cryptographic modules*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 19896-1 und ISO/IEC 19790 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

— IEC Electropedia: verfügbar unter https://www.electropedia.org/

4 Abkürzungen

AES	Erweiterte Verschlüsselungsnorm (en: advanced encryption standard)
HDD	Festplattenlaufwerk (en: hard disk drive)

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 19896-2:2024-03

RSA	Rivest-Shamir-Adleman
SHA	Sicherer Hash-Algorithmus
SSD	Festkörperlaufwerk (en: solid state drive)

5 Aufbau dieses Dokuments

Dieses Dokument gliedert sich in die folgenden Abschnitte: Wissen (Abschnitt 5), Fertigkeiten (Abschnitt 6), Erfahrung (Abschnitt 7), Ausbildung (Abschnitt 8) und Effektivität (Abschnitt 9). Jeder Abschnitt entspricht einem Aspekt der Anforderungen an Wissen, Fertigkeiten, Erfahrung, Ausbildung und Effektivität von Personen, die Prüftätigkeiten durchführen, wie sie in ISO/IEC 19896-1 für ein Konformitätsschema im Rahmen von ISO/IEC 19790 und ISO/IEC 24759 eingeführt wurden.

6 Wissen

6.1 Allgemeines

Wissen ist das, was ein Tester weiß und beschreiben kann. Abschnitt 6 bis Abschnitt 9 befassen sich mit Ausbildungsanforderungen und Wissensgebieten, die speziell für Konformitätsprüfungen nach ISO/IEC 19790 und ISO/IEC 24759 erforderlich sind.

6.2 Tertiäre Ausbildung

6.2.1 Allgemeines

Die Tester müssen über einen Bildungsabschluss verfügen, z. B. einen Associate-, Bachelor- oder höheren Abschluss, der für die in ISO/IEC 19790 behandelten Sicherheitsanforderungen und die Prüfanforderungen in ISO/IEC 24759 relevant ist. Die Tester müssen mindestens nachweisen, dass sie entweder:

a) einen angemessenen Hochschulabschluss mit einem mindestens 3-jährigen Studium in Disziplinen im Bereich der IT oder IT-Sicherheit haben; oder

b) über dem Hochschulabschluss gleichwertige Erfahrung in Disziplinen, die mit IT, IT-Sicherheit oder IT-Systemadministration zu tun haben, verfügen.

6.2.2 Technische Fachrichtungen

Zusätzlich zu den in 6.2.1 genannten Mindestanforderungen an die Ausbildung müssen die Tester über einen Hochschulabschluss verfügen, z. B. einen Associate-, Bachelor- oder höheren Abschluss, der die spezifischen technischen Fachrichtungen abdeckt. Beispiele für spezifische technische Fachrichtungen beinhalten:

— kryptographische Konzepte;

— Ingenieurswesen;

— Elektrotechnik;

— Maschinenbau;

— Werkstofftechnik;

— chemische Verfahrenstechnik;

— Datenverarbeitungstechnik;

— Technische Informatik;

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 19896-2:2024-03

— Informatik;

— Rechennetze;

— Cybersicherheit;

— Informationssysteme;

— Labormanagement;

— Softwareentwicklung und -sicherheit; oder

— Software-Engineering.

6.2.3 Fachbezogene Themen

ISO/IEC 19790:2012 und die Prüfanforderungen in ISO/IEC 24759 behandeln die folgenden konkreten Themen zum Fachwissen. Ein Tester muss sein Wissen mindestens in einem konkreten Fachgebiet nachweisen.

Ein Prüflabor muss mit seinem gesamten technischen Personal über Wissen in allen Fachgebieten verfügen.

ISO/IEC 19790:2012 und ISO/IEC 24759 legen fachliche Themen fest:

a) Software- und Firmware-Entwicklung:

    1) Programmiersprachen (z. B. Assembler und höhere Programmiersprachen);

    2) Compiler;

    3) Fehlerbehebungsprogramme;

    4) vom Anbieter durchgeführte Produktprüfungen:

        i) Einheitsprüfung;

        ii) Integrationsprüfung;

        iii) Regressionsprüfung;

b) Betriebssysteme:

    1) Installation;

    2) Konfiguration;

    3) Betrieb;

    4) Architektur;

    5) Systemhärtung;

    6) virtuelle Maschinen;

    7) Java-Laufzeitumgebung;

c) Hardware-Entwicklung:

    1) Hardware-Varianten:

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-2:2024-03

i) Single-Chip;

ii) Embedded-Multichip;

iii) Multi-Chip-Standalone;

2) Technologie:

i) Single-Chip-Fertigung;

ii) elektrische Komponenten und Gestaltung, Schaltpläne und Konzepte einschließlich Logikgestaltung und HDL-Darstellungen;

iii) mechanische Gestaltung und Verpackung;

3) Herstellung:

i) Integrität der Lieferkette;

ii) Fertigungsverfahren;

iii) Initialisierung von Parametern;

iv) Verpackung und Versand;

v) Prüfung und Charakterisierung;

4) Hardware-Sicherheitsmerkmale;

d) Betriebsumgebungen:

1) Bootloader;

2) Laden;

3) Verknüpfung;

4) Speichermanagement und -schutz;

5) Interprozesskommunikation;

6) benutzerbestimmbare Zugriffskontrolle;

7) rollenbasierte Zugriffskontrolle;

8) ausführbare Formen;

9) Prüfmechanismen;

e) kryptographische Algorithmen, Mechanismen und Techniken:

1) kryptographische Algorithmen und Sicherheitsfunktionen:

i) symmetrischer Schlüssel;

ii) asymmetrischer Schlüssel;

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-2:2024-03

iii) Hashing;

iv) Zufallsbitgeneratoren;

v) Nachrichtenauthentisierung;

vi) Entropie;

vii) Betriebsweisen;

2) Handhabung sensibler Sicherheitsparameter:

i) Generierung sensibler Sicherheitsparameter;

ii) Einführung sensibler Sicherheitsparameter;

I) automatisierter SSP-Transport oder SSP-Vereinbarung;

II) manuelle SSP-Eingabe oder Ausgabe über direkte oder elektronische Eingabe;

iii) Eingabe oder Ausgabe sensibler Sicherheitsparameter;

iv) Speicherung sensibler Sicherheitsparameter;

v) Nullsetzung sensibler Sicherheitsparameter;

f) Identifizierungs- und Authentisierungsmechanismen:

1) identitätsgestützte Authentisierung;

2) rollenbasierte Authentisierung;

3) Multifaktor-Authentisierung;

g) bewährte Praktiken in Gestaltung und Entwicklung:

1) Gestaltungszusicherung wie Konfigurationsmanagement, Lieferung, Betrieb und Entwicklung;

2) Vertragsgestaltung;

h) informelle Modellierung;

1) endlicher Automat;

i) nicht-invasive Sicherheit;

2) nicht-invasive Angriffe:

i) DPA/DEMA;

ii) SPA/SEMA;

iii) zeitliche Angriffe;

3) Gegenmaßnahmen:

i) physische Gegenmaßnahmen;

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 19896-2:2024-03