DIN EN ISO/IEC 19896-2

DIN

ICS 35.030

Einsprüche bis 2022-11-23

Entwurf

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 und Englische Fassung prEN ISO/IEC 19896-2:2022

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 and English version prEN ISO/IEC 19896-2:2022

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 et anglaise prEN ISO/IEC 19896-2:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-09-23 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

— vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;

— oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;

— oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 86 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

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 prEN ISO/IEC 19896-2:2022 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).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

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: E DIN EN ISO/IEC 19896-2:2022-10

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

– Entwurf –

September 2022

prEN ISO/IEC 19896-2

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 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)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

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: E DIN EN ISO/IEC 19896-2:2022-10

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 Authentifizierung . . . 29
C.4.1 Allgemeines . . . 29
C.4.2 Dienste . . . 29
C.4.3 Authentifizierung . . . 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 Löschen . . . 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 Abwehr 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 Authentifizierung . . . 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: E DIN EN ISO/IEC 19896-2:2022-10

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 prEN ISO/IEC 19896-2:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 19896-2:2018 wurde von CEN als prEN ISO/IEC 19896-2:2022 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

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: E DIN EN ISO/IEC 19896-2:2022-10

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: E DIN EN ISO/IEC 19896-2:2022-10

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 http://www.electropedia.org/

4 Abkürzungen

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

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

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: E DIN EN ISO/IEC 19896-2:2022-10

— 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:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

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: E DIN EN ISO/IEC 19896-2:2022-10

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) Löschen sensibler Sicherheitsparameter;

f) Identifizierungs- und Authentifizierungsmechanismen:

1) identitätsgestützte Authentifizierung;

2) rollenbasierte Authentifizierung;

3) Multifaktor-Authentifizierung;

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: E DIN EN ISO/IEC 19896-2:2022-10

BEISPIEL 1 Vorladelogik, Dual-Rail-Logik, Stromabflachung, Sondenerkennung, Hinzufügen von Rauschen, zufällige Unterbrechungen, gejitterter Takt.

ii) logische Gegenmaßnahmen;

BEISPIEL 2 Maskieren, Verstecken, Dummy-Betrieb, ausgewogenes Timing, Mischen, automatisches Nachschlüsseln.

j) Selbsttestmechanismen:

1) vorbetriebliche Prüfungen;

2) bedingte Prüfungen;

k) Sicherheitsmechanismen:

1) Löschen;

2) vertrauenswürdiger Pfad;

3) manipulationssichere Geräte;

4) Epoxidharze, Vergussmaterialien und Klebstoffe (einschließlich chemischer Eigenschaften);

5) Verkapselungen und Werkstoffe;

6) Manipulationsmechanismen;

7) Gegenmaßnahmen gegen Fehlerinjektionsangriffe;

BEISPIEL 3 Redundanzbasiertes System, Fehlererkennungscode, Fußabdruck.

8) sichere Kommunikationsprotokolle (z. B. Secure Sockets Layer, Transport Layer Security, Internet Key Exchange, Secure Socket Shell, Over-the-Air-Rekeying, usw.);

9) Attribute der Sicherheitsrichtlinien;

10) Verfahren zur Aufteilung des Wissens;

l) Gestaltungsmerkmale:

1) Anschlüsse und Schnittstellen;

2) genehmigte Betriebsmodi;

3) Spezifikation der Dienste;

4) Spezifikation der sensiblen Sicherheitsparameter;

m) Tools und Prüfverfahren:

1) Konstruktion von Prüfvorrichtungen (Software oder Hardware);

2) Umweltprüfverfahren wie die Verwendung von Temperatur (z. B. Wärme und Kälte) und Spannung (z. B. Änderungen der Eingangsleistung);

i) Temperaturkammern (z. B. Heiz- und Kühlmechanismen);

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

ii) regelbare Stromversorgungen;

3) Einsatz von Handwerkzeugen (z. B. Sägen, Bohrer, Stemmwerkzeuge, Schleifwerkzeuge, rotierende Werkzeuge mit variabler Drehzahl, Küretten und Spiegel usw.);

4) Verwendung von chemischen Lösungsmitteln (z. B. Säuren und Laugen);

5) künstliche Lichtquellen;

6) Vergrößerungsinstrumente;

7) Verwendung digitaler Speicheroszilloskope oder Logikanalysatoren;

8) Verwendung eines Volt-Ohm-Meters oder digitalen Multimeters;

9) digitaler Scanner;

10) Digitalkamera (einschließlich Nah- oder MACRO-Fokus-Funktionen);

11) Werkzeuge des Validierungsprogramms.

ANMERKUNG Eine Kalibrierung der Werkzeuge ist nur in Abhängigkeit vom Prüfverfahren erforderlich.

Zusätzliche Informationen über spezifisches Wissen im Zusammenhang mit der Sicherheit von kryptographischen Modulen sind in Anhang C aufgeführt.

6.3 Wissen über die Normen

6.3.1 Allgemeines

Der Tester muss Wissen über die in Abschnitt 2 genannten normativen Verweisungen besitzen. Der Tester muss in der Lage sein, Verständnis oder Vertrautheit mit einem oder mehreren der folgenden Themen nachzuweisen.

6.3.2 ISO/IEC 19790-Konzepte

Der Tester muss Wissen über die Konzepte in ISO/IEC 19790 besitzen. ISO/IEC 19790 legt die Sicherheitsanforderungen für ein kryptographisches Modul fest, das innerhalb eines Sicherheitssystems zum Schutz sensibler Informationen in Computer- und Telekommunikationssystemen verwendet wird. ISO/IEC 19790 definiert vier Sicherheitsstufen für jeden der 11 Anforderungsbereiche, wobei jede Sicherheitsstufe die Sicherheit der vorangegangenen Stufe für kryptographische Module erhöht.

6.3.3 ISO/IEC 24759

6.3.3.1 Allgemeines

ISO/IEC 24759 legt die Prüfanforderungen für kryptographische Module fest, die von Anbietern und Prüflaboren zu verwenden sind. ISO/IEC 24759:2017 enthält 11 Unterabschnitte, die den 11 Bereichen der Sicherheitsanforderungen entsprechen, und sechs Unterabschnitte, die ISO/IEC 19790:2012, Anhang A bis Anhang F, entsprechen. Diese entsprechenden Sicherheitsanforderungen sind in ISO/IEC 19790:2012, 5.2.2.5 bzw. 5.2.2.6, aufgeführt.

6.3.3.2 Anforderungen an den Anbieter

ISO/IEC 24759 legt alle Anforderungen an den Anbieternachweis (VE, en: vendor evidence) fest, den die Anbieter den Prüflaboren für das zu prüfende Modul zur Verfügung stellen, um die Konformität ihres kryptographischen Moduls mit den in ISO/IEC 19790:2012 festgelegten Sicherheitsanforderungen nachzuweisen.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

Der Anbieter muss auch alle Änderungen, Ergänzungen oder Streichungen des VE-Nachweises erfüllen, die die Validierungsinstanz an ISO/IEC 24759 vorgenommen hat.

Der Tester muss mit allen Anforderungen des Anbieters vertraut sein.

6.3.3.3 Prüfanforderungen

ISO/IEC 24759 legt die Anforderungen an den Testernachweis (TE, en: tester evidence) fest, die für das zu prüfende Modul gelten und von Prüflaboren zu verwenden sind, um zu prüfen, ob das kryptographische Modul mit den in ISO/IEC 19790 festgelegten Anforderungen übereinstimmt. Die Verfahren wurden entwickelt, um ein hohes Maß an Objektivität während des Prüfverfahrens bereitzustellen und die Konsistenz zwischen den Prüflaboren sicherzustellen.

Der Tester muss auch alle Änderungen, Ergänzungen oder Streichungen des TE-Nachweises erfüllen, die die Validierungsinstanz an ISO/IEC 24759 vorgenommen hat.

Der Anbieter muss mit allen Prüfanforderungen vertraut sein.

6.3.4 Zusätzliche ISO/IEC-Normen

Der Tester muss mit Folgendem vertraut sein.

— ISO/IEC 17825 legt die Prüfverfahren für die Abschwächung nicht-invasiver Angriffsklassen gegen kryptographische Module fest.

— ISO/IEC 18367 legt die Konformitätsprüfung von kryptographischen Algorithmen und Sicherheitsmechanismen fest.

— ISO/IEC 20085-1 legt die Anforderungen an das Prüfwerkzeug für das Prüfen nicht-invasiver Angriffsabwehrtechniken in kryptographischen Modulen fest.

— ISO/IEC 20085-2 legt die Anforderungen an Prüfwerkzeuge für die Prüfung nicht-invasiver Angriffsabwehrtechniken in kryptographischen Modulen fest.

— ISO/IEC 20543 legt Prüf- und Analyseverfahren für Zufallsbitgeneratoren innerhalb von ISO/IEC 19790 und ISO/IEC 15408 fest.

6.4 Wissen über das Validierungsprogramm

6.4.1 Validierungsprogramm

6.4.1.1 Allgemeines

Validierungsprogramme, die in der Regel unter der Schirmherrschaft einer Akkreditierungsbehörde durchgeführt werden, legen häufig programmspezifische Aspekte für ihren Betrieb fest. Dies geschieht in der Regel auf der Grundlage geltender Rechtsvorschriften und Richtlinien, wie z. B. der nationalen Politik, die für ihren Betrieb maßgeblich sind. Die Tester müssen über Wissen hinsichtlich des Validierungsprogramms und aller spezifischen Aspekte verfügen, wie sie in 6.4.1.2 bis 6.4.1.7 aufgeführt sind.

6.4.1.2 Organisation

Dieser Aspekt betrifft die Organisation des Programms und die Stellen, die an der Durchführung des Programms beteiligt sind.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

6.4.1.3 Kommunikation

Dieser Aspekt betrifft die Art und Weise, wie das Programm relevante Informationen an die interessierten Parteien weitergibt, insbesondere an die Prüfeinrichtungen und die zugehörigen Tester. Dies sollte auch beinhalten, wie Kommunikation und Informationen geschützt werden.

6.4.1.4 Rechtliche und behördliche Mandate

Dieser Aspekt betrifft den rechtlichen und/oder regulatorischen Rahmen, in dem das Validierungsprogramm arbeitet.

6.4.1.5 Richtlinien

Dieser Aspekt betrifft konkrete Richtlinien, die auf das Validierungsprogramm anwendbar sind. Diese können prozess- und anforderungsbezogene Richtlinien in Verbindung mit der Annahme von Projekten zur Validierung kryptographischer Module umfassen. Nachfolgend sind einige Beispiele aufgeführt.

a) Ausreichende Prüfung: Der Tester sollte wissen, was erforderlich ist, um sicherzustellen, dass ein kryptographisches Zielmodul ausreichend geprüft wird.

b) Entsorgung von Nachweisen: das Verfahren zur ordnungsgemäßen Entsorgung von Nachweisen nach Abschluss eines Projekts.

c) Vertraulichkeit: etwaige Anforderungen an die Vertraulichkeit (seitens des Testers und die Geheimhaltung der im Rahmen von Prüfprojekten gewonnenen Informationen).

d) Problemlösung: die Vorgehensweise, wenn während des Projekts ein Problem auftritt (ob die Arbeit fortgesetzt wird, sobald das Problem behoben ist, oder ob das Projekt sofort beendet wird und das behobene Produkt erneut eingereicht werden muss).

e) Sprache: jede spezifische (natürliche) Sprache, in der die Dokumentation erstellt werden muss.

f) Anforderungen an aufgezeichnete Nachweise: alle aufgezeichneten Nachweise, die vom Tester dokumentiert werden und die dem Validierungsprogramm vorgelegt werden müssen.

g) Zusätzliche Richtlinien für die Berichterstattung: alle spezifischen Berichte, die vom Tester verlangt werden, wie z. B. Prüfberichte.

h) Anleitung zur Implementierung: Eine Validierungsbehörde kann programmatische oder klärende Anleitungen geben, die vom Tester berücksichtigt werden sollten.

i) Wiederverwendung: Dokumentation und Begründung, die das Validierungsprogramm zur Unterstützung der Wiederverwendung von Prüfnachweisen benötigt.

j) Jegliche besondere Handhabung der Identifikatoren des Validierungsprogramms, Logos, Markenzeichen usw.

k) Handhabung und Anwendung von Interpretationen des Validierungsprogramms.

l) Eine Liste oder Charakterisierungen geeigneter alternativer Prüfansätze, wenn die vom Validierungsprogramm empfohlene ursprüngliche Prüfung für ein bestimmtes kryptographisches Zielmodul nicht durchführbar ist.

m) Die Richtlinien, anhand derer das Validierungsprogramm feststellt, welche Schritte ein Tester beim Prüfen unternommen hat.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

6.4.1.6 Dokumentation

Dieser Aspekt betrifft die Bereitstellung und Verwendung aller für das Validierungsprogramm spezifischen Dokumente. Dazu können Formulare, Vorlagen, Schulungsunterlagen und Informationsmaterial gehören. Validierungsprogrammspezifische Dokumente können unter anderem folgende Dokumente umfassen:

— Managementhandbücher;

— häufig gestellte Fragen;

— Umsetzung oder programmatische Anleitung;

— Handbücher für die vom Programm gelieferten Tools.

6.4.1.7 Tools

Das Validierungsprogramm kann spezielle Tools für die Prüfung, die Erstellung von Berichten, die Übermittlung oder den Schutz (z. B. Verschlüsselung) bereitstellen. Beispiele hierfür sind:

— algorithmische Testtools;

— Generierung von Prüfvektoren und daraus resultierende erwartete Antworten;

— Dokumentation der Prüftätigkeiten und Berichterstattung;

— Verschlüsselungstool zum Schutz der an das Validierungsprogramm übermittelten Prüfberichte;

— Angabe bestimmter Verschlüsselungsalgorithmen und Signaturverfahren (z. B. 128-Bit-AES für die Verschlüsselung und 2048-Bit-RSA mit SHA-2 für die digitale Signatur).

6.5 Wissen über die Anforderungen der ISO/IEC 17025

Da von Prüfeinrichtungen häufig verlangt wird, dass sie der ISO/IEC 17025 entsprechen, muss der Tester mit den Anforderungen der ISO/IEC 17025 vertraut sein und wissen, wie diese in der/den Validierungseinrichtung(en) umgesetzt werden, mit der/denen der Tester verbunden ist. Wenn es zusätzliche programmatische Akkreditierungsdokumente gibt, die mit der ISO/IEC 17025 verbunden sind und die die Grundlage für die Akkreditierung des Laboratoriums bilden, dann muss der Tester auch mit diesen Dokumenten vertraut sein.

7 Fertigkeiten

7.1 Allgemeines

Schulungen für Tester erfolgen häufig aufgrund von Berufserfahrung in der IT-Branche, während der Zusammenarbeit mit einer Prüfeinrichtung oder aufgrund der Anforderungen von Berufsverbänden.

BEISPIEL Fachliche Zertifizierungen wie die CISSP™-Zertifizierung des ISC2™ sind mit der Anforderung verbunden, sich beruflich weiterzuentwickeln.

7.2 Prüfung von Algorithmen

Der Tester muss in der Lage sein, das Programm zur Validierung des kryptographischen Algorithmus oder die über die Benutzeroberfläche gesteuerten Testtools für Algorithmen zu installieren, zu konfigurieren und auszuführen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

7.3 Prüfung der physischen Sicherheit

Der Tester muss über die Fertigkeiten verfügen, die für die Durchführung der physischen Sicherheitsprüfungen erforderlich sind und für die er entsprechend ausgebildet und qualifiziert ist.

7.4 Seitenkanalanalyse

Der Tester muss über die Fertigkeiten verfügen, die für die Durchführung der Seitenkanalprüfungen erforderlich sind und für die er entsprechend ausgebildet und qualifiziert ist.

7.5 Technologietypen

Die Fertigkeiten und Techniken, die für die Prüfung der kryptographischen Module der verschiedenen Technologietypen erforderlich sind, können sich voneinander unterscheiden. Die Tester müssen in der Lage sein, nachzuweisen, dass sie über das erforderliche Wissen, die erforderlichen Fertigkeiten und Techniken in Bezug auf die Technologietypen der von ihnen geprüften kryptographischen Module verfügen.

ANMERKUNG 1 Das Validierungsprogramm befasst sich mit kryptographischen Modulen, die viele für die Prüfung in Frage kommende Technologietypen repräsentieren. Anhang B enthält eine Liste der am häufigsten genannten Technologietypen und Vorschläge für grundlegendes Wissen, Fertigkeiten und Techniken, die Tester benötigen.

ANMERKUNG 2 Viele fachspezifische Zertifizierungen decken den Wissensbestand ab, der für Tester erforderlich ist. Solche Zertifizierungen können auf nationaler, regionaler oder globaler Ebene erfolgen. Es würde den Rahmen dieses Dokuments sprengen, sie alle zu katalogisieren, einige von ihnen sind jedoch in den Literaturhinweisen aufgeführt.

8 Erfahrung

8.1 Allgemeines

Der Tester muss seine Schulungs- und Prüfungsaktivitäten in Übereinstimmung mit den Anforderungen des Validierungsprogramms und/oder der Prüfeinrichtung dokumentieren.

8.2 Nachweis der technischen Kompetenz für das Validierungsprogramm

8.2.1 Erfahrung mit der Durchführung von Prüfungen

Der Tester muss alle Prüftätigkeiten in einem Protokoll festhalten. Die Aufzeichnungen müssen zusammen mit den erworbenen Prüfnachweisen aufbewahrt werden (siehe Anhang A). Der Tester sollte das Testerprotokoll für die operativen Prüfungen erstellen, damit sowohl die erwarteten als auch die tatsächlichen Prüfergebnisse deutlich werden.

BEISPIEL Erwartete Statusanzeige.

8.2.2 Erfahrung mit bestimmten Technologietypen

Der Tester muss in seinem Tätigkeitsprotokoll die geprüften Technologietypen angeben.

9 Ausbildung

Der Tester muss seine Ausbildung in Übereinstimmung mit den Anforderungen des Validierungsprogramms und/oder der Prüfeinrichtung dokumentieren.

Die Anforderungen an die Ausbildung sind in 6.2 aufgeführt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

10 Effektivität

Der Tester muss in der Lage sein, sein Wissen und seine Fertigkeiten produktiv einzusetzen, was durch Verhaltensmerkmale wie Eignung, Initiative, Begeisterung, Bereitschaft, Kommunikationsstärke, Teamfähigkeit und Führungsqualitäten gekennzeichnet ist.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

Anhang A
(informativ)

Beispiel für ein ISO/IEC 24759-Testerprotokoll

<table>
<tr><td colspan="3">Name</td></tr>
<tr><td colspan="3">Bezeichnung</td></tr>
<tr><td colspan="2">Validierungsprogramm</td><td>Prüfeinrichtung</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">Name des kryptographischen Moduls</td><td>Typ des kryptographischen Moduls</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">Allgemeine Sicherheitsstufe</td><td>Zertifizierungs-ID (falls bekannt)</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">Antragsteller/Entwickler</td><td>Datum der vorgenommenen Prüfung</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="3">Beschreibung der IUT</td></tr>
<tr><td rowspan="3">AS 01.01</td><td colspan="2">Anwendbare Prüfanforderung nach ISO/IEC 24759</td></tr>
<tr><td colspan="2">Beschreibung der Gestaltung des IUT zur Konformität mit der Prüfanforderung</td></tr>
<tr><td colspan="2">Beschreibung des Prüfverfahrens und der Ergebnisse</td></tr>
</table>

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

Anhang B
(informativ)

Ontologie der Technologietypen und der zugehörigen Wissensbestände

B.1 Allgemeines

Das Validierungsprogramm befasst sich mit kryptographischen Modulen, die viele für die Prüfung in Frage kommende Technologietypen repräsentieren. Nachfolgend ist eine Liste der am häufigsten genannten Technologietypen und Vorschläge für grundlegendes Wissen, Fertigkeiten und Techniken aufgeführt, die Tester benötigen.

B.2 Technologietypen

B.2.1 Allgemeines

Kryptographische Module können aus Software, Firmware, Hardware oder einer Mischung aus Software und Firmware mit Hardware bestehen.

B.2.2 Software/Firmware

Software oder Firmware kann in verschiedenen Programmiersprachen geschrieben und dann in verschiedene Formen von ausführbaren Dateien kompiliert werden. Eine ausführbare Datei kann ein kryptographisches Software- oder Firmware-Modul darstellen. Debugger dürfen verwendet werden, um Fehler in der Implementierung zu finden und zu beheben.

B.2.2.1 Programmiersprachen

Beispiele für verschiedene Software-Programmiersprachen, die verwendet werden dürfen, sind (diese Liste ist weder erschöpfend noch vollständig und dient nur zur Veranschaulichung):

— Ada;

— APL;

— Assembler;

— C++;

— dBase;

— Google Apps Script;

— Java;

— JavaScript;

— Microcode;

— Unix-Shell;

— Visual Basic;

— VHDL.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

B.2.2.2 Compiler

Beispiele für verschiedene Open-Source-Software-Compiler, die verwendet werden können, sind (diese Liste ist weder erschöpfend noch vollständig und dient nur zur Veranschaulichung):

— FreeBASIC;

— Clang C/C++/Objective-C Compiler;

— Free Pascal;

— GCC [C, C++, (G++), Java (GCJ) und Ada (GNAT)];

— Local C Compiler;

— Open Watcom;

— Open64;

— XPL PL/I;

— C zu HDL.

B.2.2.3 Debugger oder Simulatoren

Beispiele für verschiedene Open-Source-Debugger, die verwendet werden können, sind (diese Liste ist weder erschöpfend noch vollständig und dient nur zur Veranschaulichung):

— Firefox JavaScript Debugger;

— GDB – der GNU Debugger;

— Eclipse-Debugger;

— Opera Dragonfly;

— Python-Debugger;

— X64dbg;

— ZeroBUGS;

— VHDL;

— Verilog.

B.2.2.4 Hardware

B.2.2.4.1 Allgemeines Wissen

Die Hardware darf in verschiedenen Ausführungsformen und Technologietypen implementiert werden. Nachfolgend sind Beispiele für Hardware-Varianten und Technologietypen aufgeführt. Die folgenden Listen sind weder erschöpfend noch vollständig und dienen lediglich der Veranschaulichung.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10

B.2.2.4.2 Single-Chip-Module

B.2.2.4.2.1 Allgemeines Wissen über Single-Chip-Module

Ein Single-Chip-Kryptomodul ist eine physische Ausführungsform, bei der ein einzelner integrierter Schaltkreis (IC) als eigenständiges Gerät verwendet oder in ein Gehäuse oder ein Produkt eingebettet werden kann, das möglicherweise nicht physisch geschützt ist.

B.2.2.4.2.2 Single-Chip-Substratmaterialien

Beispiele für Single-Chip-Substratmaterialien

— Galliumarsenid;

— Germanium;

— monokristallines Silizium.

B.2.2.4.2.3 Single-Chip-Gehäusearten

Beispiele für Single-Chip-Gehäusearten:

— Duales Inline-Paket (DIP);

— Pin Grid Array (PGA);

— bleifreier Chipträger (LCC, en: leadless chip carrier);

— Oberflächenmontage;

— Thin Small Outline Package (TSOP);

— Plastic Quad Flat Pack (PQFP);

— Ball Grid Array (BGA);

— Flip-Chip Ball Grid Array (FCBGA).

B.2.2.4.3 Eingebettete Multi-Chip-Module

Ein eingebettetes Multi-Chip-Kryptomodul ist eine physische Ausführungsform, bei der zwei oder mehr integrierte Schaltkreis-Chips miteinander verbunden und in ein Gehäuse oder ein Produkt eingebettet sind, das möglicherweise nicht physisch geschützt ist.

BEISPIEL

— Adapterkarten;

— Erweiterungsplatinen;

— untergeordnete Platinen (daughter cards).

B.2.2.4.4 Eigenständige Multichip-Module

Ein eigenständiges Multichip-Krypto-Modul ist eine physische Ausführungsform, bei der zwei oder mehr integrierte Schaltkreischips miteinander verbunden sind und das gesamte Gehäuse physisch geschützt ist.

BEISPIEL

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-2:2022-10