DIN EN ISO/IEC 19790

DIN

ICS 35.030

Einsprüche bis 2020-04-21
Ersatz für
E DIN EN ISO/IEC 19790:2019-11

Entwurf

Informationstechnik – Sicherheitstechniken – Sicherheitsanforderungen für kryptografische Module (ISO/IEC 19790:2012); Deutsche und Englische Fassung prEN ISO/IEC 19790:2019

Information technology –
Security techniques –
Security requirements for cryptographic modules (ISO/IEC 19790:2012);
German and English version prEN ISO/IEC 19790:2019

Technologies de l'information –
Techniques de sécurité –
Exigences de sécurité pour les modules cryptographiques (ISO/IEC 19790:2012);
Version anglaise prEN ISO/IEC 19790:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-02-21 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, Saatwinkler Damm 42/43, 13627 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 168 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

Nationales Vorwort

Der Text von ISO/IEC 19790:2012 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 19790:2019 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Gremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Bei diesem Dokument handelt es sich um einen zweiten Entwurf, da der Verzicht auf die deutsche Sprachfassung nicht genehmigt wurde.

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 internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 10007:2003	siehe	DIN ISO 10007:2004-12
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN ISO 10007:2004-12, *Qualitätsmanagement — Leitfaden für Konfigurationsmanagement (ISO 10007:2003)*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-managementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

– Entwurf –

CEN/CLC/J/TC 13

Datum: 2019-11

prEN ISO/IEC 19790:2019

CEN/CLC/J/TC 13

Sekretariat: DIN

Informationstechnik — Sicherheitstechniken — Sicherheitsanforderungen für kryptografische Module (ISO/IEC 19790:2012)

Technologie de l'information — Techniques de sécurité — Exigences de sécurité pour les modules cryptographiques (ISO/IEC 19790:2012)

Information technology — Security techniques — Security requirements for cryptographic modules (ISO/IEC 19790:2012)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.9p

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

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 27

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 34
7.3.4 Vertrauenswürdiger Kanal 35
7.4 Rollen, Dienste und Authentifizierung 36
7.4.1 Allgemeine Anforderungen an Rollen, Dienste und Authentifizierung 36
7.4.2 Rollen 36
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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

7.9.1 Allgemeine Anforderungen an die Verwaltung von sensiblen Sicherheitsparametern 57
7.9.2 Zufallsbitgeneratoren 57
7.9.3 Erzeugung sensibler Sicherheitsparameter 57
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 59
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 64
7.11.1 Allgemeine Anforderungen an die Lebenszyklussicherung 64
7.11.2 Konfigurationsmanagement 65
7.11.3 Auslegung 65
7.11.4 Endlicher Automat 65
7.11.5 Entwicklung 66
7.11.6 Prüfungen des Anbieters 68
7.11.7 Lieferung und Betrieb 68
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 73
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) Sicherheitsleitlinie 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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

C.1.1 Blockziffern 82
C.1.2 Stromchiffren 82
C.1.3 Asymmetrische Algorithmen und Techniken 82
C.1.4 Mitteilungsauthentisierungscodes 82
C.1.5 Hash-Funktionen 82
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 85
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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

Europäisches Vorwort

Der Text von ISO/IEC 19790:2012, einschließlich Technischer Berichtigung 1:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „ISO/IEC Gemeinschaftskomitee für Informationstechnik“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 19790:2019 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 19790:2012, einschließlich Technischer Berichtigung 1:2015 wurde von CEN als prEN ISO/IEC 19790:2019 ohne irgendeine Abänderung genehmigt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

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. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Die zur Erarbeitung und künftigen Revision dieses Dokumentes verwendeten Regeln sind in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Regeln 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. Einzelheiten zu Patentrechten, die während der Erarbeitung des Dokumentes identifiziert werden, werden in der Einleitung und/oder in der ISO-Liste der erhaltenen Patentdeklarationen (siehe www.iso.org/patents) angegeben.

Alle in diesem Dokument verwendeten Markennamen stellen eine Informationen für den Leser dar und stellen keine Anerkennung derselben dar.

Bezüglich einer Erklärung der Bedeutung ISO-spezifischer Ausdrücke im Zusammenhang mit Konformitätsbewertung sowie Informationen über die Einhaltung der Prinzipien der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT) seitens ISO siehe folgende URL: www.iso.org/iso/foreword.html.

Die Technische Berichtigung 1 zu ISO/IEC 19790:2012 wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27 *Security techniques* erarbeitet.

Diese korrigierte Version der Technischen Berichtigung 1 zu ISO/IEC 19790:2012 ersetzt die erste Ausgabe (ISO/IEC 19790:2012/Cor 1:2015). Sie enthält dieselben technischen Überarbeitungen und sonstigen redaktionellen Korrekturen, die mit **roter** Textfarbe anstelle von schwarzem Unterstrich dargestellt sind:

— 3.21: der Begriff „kryptografische Begrenzung“ wurde korrigiert;

— 3.80: der Begriff „nicht sicherheitsrelevant“ wurde korrigiert;

— 3.108: der Begriff „Selbsttest“ wurde korrigiert;

— 7.2.2: die Anforderungen **[02.04]**, **[02.05]** und **[02.06]** wurden korrigiert;

— 7.2.4.3: die Anforderung **[02.31]** wurde korrigiert;

— 7.3.3: die Anforderung **[03.14]** wurde korrigiert;

— 7.5: die Anforderungen **[05.06]** und **[05.07]** wurden hinzugefügt. Die Anforderungen **[05.08]**, **[05.13]** und **[05.17]** bis **[05.23]** wurden korrigiert;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

— 7.6.3: die Anforderung **[06.06]** wurde korrigiert;

— 7.8: die Anforderung **[08.04]** wurde korrigiert;

— 7.9.1: die Anforderung **[09.04]** wurde korrigiert;

— 7.9.7: die Anforderung **[09.37]** wurde korrigiert;

— 7.10.2.2: die Anforderung **[10.17]** wurde korrigiert;

— 7.11.5: die Anforderung **[11.26]** wurde korrigiert;

— 7.11.7: die Anforderung **[11.35]** wurde korrigiert;

— 7.11.9: die Anforderung **[11.38]** wurde korrigiert;

— A.2.5: die Anforderungen in Unterpunkt 1 und 2 wurden korrigiert;

— A.2.7: die Anforderung in Unterpunkt 3 wurde korrigiert;

— A.2.10: die Anforderung in Unterpunkt 4 wurde korrigiert;

— B.2.4: die Anforderung in Unterpunkt 9 wurde korrigiert;

— B.2.5: die Anforderung in Unterpunkt 1 wurde korrigiert;

— B.2.7: die Anforderung in Unterpunkt 6 der zweiten Gliederungsebene wurde korrigiert;

— D.1: doppelter Text wurde entfernt;

— D.1.2: die Verweisung auf ISO/IEC 15946-3 wurde entfernt;

— E.1: doppelter Text wurde entfernt; und

— F.1: doppelter Text wurde entfernt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

Einleitung

In der Informationstechnologie wächst ständig die Notwendigkeit, kryptografische Mechanismen, wie den Schutz von Daten vor unbefugter Weitergabe oder Manipulation, der Authentifizierung der Entität und der Nichtabstreitbarkeit, einzusetzen. Die Sicherheit und Zuverlässigkeit solcher Mechanismen hängt direkt von den Krypto-Modulen ab, in die sie implementiert sind.

Diese Internationale Norm sieht vier qualitativ ansteigende Stufen an Sicherheitsanforderungen vor, mit der Absicht, ein breites Spektrum möglicher Anwendungen und Umgebungen abzudecken. Die kryptografischen Techniken sind über die vier Sicherheitsstufen hinweg identisch. Die Sicherheitsanforderungen decken Bereiche ab, die sich auf die Auslegung und Implementierung eines Krypto-Moduls beziehen. Diese Bereiche umfassen die Spezifikation und Schnittstellen des Krypto-Moduls, die Rollen, Dienste und Authentifizierung, die Software-/Firmware-Sicherheit, die Betriebsumgebung, die physische Sicherheit, die Sicherheit bei nicht-invasiven Angriffen, die Verwaltung von sensiblen Sicherheitsparametern, Selbsttests, die Lebenszyklus-sicherung und die Schadensminderung bei anderen Angriffen.

Die Gesamtsicherheitsklassifizierung eines Krypto-Moduls muss so gewählt werden, dass die entsprechende Sicherheitsstufe für die Sicherheitsanforderungen der Anwendung und der Umgebung, in der das Modul verwendet werden soll, sowie für die Sicherheitsdienste, die das Modul erbringen soll, angemessen ist. Die verantwortliche Instanz in jeder Organisation sollte sicherstellen, dass die Computer- und Telekommunikationssysteme, die Krypto-Module nutzen, eine für die jeweilige Anwendung und Umgebung annehmbare Sicherheitsstufe bieten. Da jede Instanz für die Auswahl der für eine bestimmte Anwendung geeigneten genehmigten Sicherheitsfunktionen verantwortlich ist, schließt die Einhaltung dieser Internationalen Norm weder vollkommene Interoperabilität noch die gegenseitige Anerkennung konformer Produkte ein. Alle Beteiligten sollten auf die Wichtigkeit, ein Sicherheitsbewusstsein zu entwickeln und die Informationssicherheit als Priorität im Management anzuerkennen, hingewiesen werden.

Die Anforderungen an die Informationssicherheit sind je nach Anwendung unterschiedlich; Organisationen sollten ihre Informationsressourcen identifizieren und die Empfindlichkeit in Bezug auf Datenverlust sowie dessen mögliche Auswirkungen durch die Implementierung geeigneter Kontrollmechanismen ermitteln. Kontrollen schließen Folgendes ein, sind aber nicht darauf begrenzt:

— physische Kontrollen und Kontrollen der Umgebung;

— Zugriffskontrollen;

— Softwareentwicklung;

— Datensicherungs- und Notfallpläne; und

— Kontrolle der Informationen und Daten.

Diese Kontrollen sind nur so wirksam wie die Verwaltung geeigneter Sicherheitsleitlinien und -verfahren in der Betriebsumgebung.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

1 Anwendungsbereich

Diese Internationale Norm legt die Sicherheitsanforderungen für ein Krypto-Modul fest, das in einem Sicherheitssystem zum Schutz sensibler Informationen in Computer- und Telekommunikationssystemen genutzt wird. Diese Internationale Norm definiert vier Sicherheitsstufen für Krypto-Module, um ein breites Spektrum an Datensensibilität (z. B. Verwaltungsdaten von geringem Wert, Geldtransfers in Millionenhöhe, Lebensschutzdaten, Identitätsdaten von Personen und sensible Informationen, die von Regierungen verwendet werden) und eine Vielzahl von Anwendungsumgebungen (z. B. eine bewachte Einrichtung, ein Büro, Wechselmedien und ein völlig ungeschützter Standort) abzudecken. Diese Internationale Norm legt vier Sicherheitsstufen für jeden der elf Anforderungsbereiche fest, wobei jede Sicherheitsstufe eine höhere Sicherheit als die vorhergehende bietet.

Diese Internationale Norm legt Sicherheitsanforderungen fest, um die Sicherheit eines Krypto-Moduls aufrechtzuerhalten. Die Einhaltung dieser Internationalen Norm reicht nicht aus, um sicherzustellen, dass ein bestimmtes Modul sicher ist oder dass die vom Modul gebotene Sicherheit für den Eigentümer der zu schützenden Informationen ausreichend und annehmbar ist.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. 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).

Die in ISO/IEC 19790 *Informationstechnik — Sicherheitstechniken — Sicherheitsanforderungen für kryptografische Module,* Anhänge C, D, E und F aufgelisteten Dokumente.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1
Zugriffskontrollliste
ACL
(en: access control list)
Liste mit Berechtigungen, die den Zugriff auf ein Objekt erlauben

3.2
Administratorleitlinien
schriftliche Unterlagen, die vom Kryptobeauftragten und/oder anderen administrativen Rollen zur korrekten Konfiguration, Wartung und Administration des Krypto-Moduls herangezogen werden

3.3
automatisiert
ohne manuellen Eingriff oder manuelle Eingabe (z. B. elektronische Mittel, wie ein Computernetzwerk)

3.4
Genehmigungsinstanz
nationale oder internationale Organisation/Instanz, die befugt ist, Sicherheitsfunktionen zu genehmigen und/oder zu evaluieren

ANMERKUNG Eine Genehmigungsinstanz im Kontext dieser Definition evaluiert und genehmigt Sicherheitsfunktionen ausgehend von deren kryptografischen oder mathematischen Eigenschaften, es handelt sich dabei jedoch nicht um die Prüfstelle, die die Übereinstimmung mit dieser Internationalen Norm prüfen würde.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

3.5
genehmigte Datenauthentisierungstechnik
genehmigtes Verfahren, das die Nutzung einer digitalen Signatur, eines Mitteilungsauthentisierungscodes oder eines verschlüsselten Hashs (z. B. HMAC) beinhalten kann

3.6
genehmigte Integritätstechnik
genehmigter Hash, Mitteilungsauthentisierungscode oder Algorithmus für digitale Signaturen

3.7
genehmigter Betriebsmodus
Satz an Diensten, der mindestens einen Dienst beinhaltet, welcher eine genehmigte Sicherheitsfunktion oder einen genehmigten Sicherheitsprozess verwendet, und auch nicht sicherheitsrelevante Dienste enthalten kann

ANMERKUNG 1 Nicht zu verwechseln mit einem konkreten Modus einer genehmigten Sicherheitsfunktion, z. B. CBC-Modus (en: Cipher Block Chaining Mode).

ANMERKUNG 2 Nicht genehmigte Sicherheitsfunktionen oder -prozesse sind nicht eingeschlossen.

3.8
genehmigte Sicherheitsfunktion
Sicherheitsfunktion (z. B. kryptografischer Algorithmus), auf die in Anhang C verwiesen wird

3.9
asymmetrische Kryptografietechnik
kryptografische Technik, die zwei miteinander verbundene Transformationen nutzt: eine öffentliche Transformation (durch den öffentlichen Schlüssel definiert) und eine private Transformation (durch den privaten Schlüssel definiert)

ANMERKUNG Die beiden Transformationen haben die Eigenschaft, dass es aufgrund der öffentlichen Transformation im Hinblick auf Rechenleistung nicht machbar ist, innerhalb einer bestimmten begrenzten Zeit und mit einer bestimmten verfügbaren Rechenleistung daraus die private Transformation abzuleiten.

3.10
biometrisch
messbares körperliches Merkmal oder messbares Handlungsmuster, das zur Erkennung der Identität oder zur Überprüfung der vorgegebenen Identität eines Bedieners verwendet wird

3.11
Fähigkeit zum Umgehen
Vermögen eines Dienstes, die Anwendung einer kryptografischen Funktion auf sich selbst teilweise oder vollständig zu verhindern

3.12
Zertifikat
Daten einer Entität, die mittels des privaten oder geheimen Schlüssels einer Zertifizierungsinstanz fälschungssicher gemacht wurden

ANMERKUNG Nicht zu verwechseln mit einem Modulvalidierungszertifikat, das von einer Validierungsinstanz ausgestellt wird.

3.13
kompromittieren
kritische Sicherheitsparameter unautorisiert offenlegen, modifizieren, ersetzen oder verwenden oder öffentliche Sicherheitsparameter unautorisiert modifizieren oder ersetzen

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

3.14
bedingter Selbsttest
von einem Krypto-Modul durchgeführte Überprüfung, wenn die für die Überprüfung festgelegten Bedingungen auftreten

3.15
Vertraulichkeit
Eigenschaft, Informationen nicht für Entitäten verfügbar zu machen oder offenzulegen, die nicht dafür autorisiert sind

3.16
Konfigurationsmanagementsystem
CMS
(en: configuration management system)
Management der Sicherheitsmerkmale und Vertrauenswürdigkeiten eines Krypto-Moduls durch gesteuerte Änderungen an dessen Hardware, Software und Dokumentation

3.17
Steuerinformation
Information, die zum Zweck der Steuerung des Betriebs des Krypto-Moduls in dieses Modul eingegeben wird

3.18
kritischer Sicherheitsparameter
CSP
(en: critical security parameter)
sicherheitsbezogene Information, deren Offenlegung oder Modifizierung die Sicherheit eines Krypto-Moduls kompromittieren kann

BEISPIEL Geheime und private kryptografische Schlüssel, Authentisierungsdaten wie Passwörter, PINs, Zertifikate oder andere Vertrauensanker

ANMERKUNG Ein CSP kann in Klartext gehalten oder verschlüsselt sein.

3.19
Kryptobeauftragter
Rolle, die eine Person oder ein Prozess (d. h. ein Subjekt), der für eine Person agiert, inne hat, und die/der auf ein Krypto-Modul zugreift, um eine kryptografische Initialisierung oder Managementfunktionen für das Krypto-Modul durchzuführen

3.20
kryptografischer Algorithmus
klar definierte Computerprozedur, die anhand von variablen Eingaben, wozu auch kryptografische Schlüssel gehören können, eine Ausgabe erzeugt

3.21
kryptografische Begrenzung
explizit definierter Bereich, innerhalb von dessen Grenzen sich alle Komponenten (d. h., Satz an Hardware-, Software- oder Firmware-Komponenten) des Krypto-Moduls befinden

3.22
kryptografische Hashfunktion
recheneffiziente Funktion, die binäre Zeichenfolgen einer beliebigen Länge so zu binären Zeichenfolgen mit fester Länge zuordnet, dass es rechnerisch gesehen nicht machbar ist, dass dabei zwei unterschiedlichen Werten dieselbe feste Zeichenfolge zugeordnet wird

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

3.23
kryptografischer Schlüssel
Schlüssel
Abfolge von Symbolen, die den Ablauf einer kryptografischen Transformation steuert

BEISPIEL Zu kryptografischen Transformationen zählen unter anderem Verschlüsselung, Entschlüsselung, Berechnung kryptografischer Prüffunktionen sowie Generierung und Verifizierung von Signaturen.

3.24
Komponente des kryptografischen Schlüssels
Schlüsselkomponente
Parameter, der in Verbindung mit anderen Schlüsselkomponenten in einer genehmigten Sicherheitsfunktion zur Erzeugung eines Klartext-CSP oder zur Ausführung einer kryptografischen Funktion genutzt wird

3.25
kryptografisches Modul
Krypto-Modul
Hardware-, Software- und/oder Firmware-Satz, der Sicherheitsfunktionen implementiert und sich innerhalb der kryptografischen Begrenzung befindet

3.26
Sicherheitsleitlinie für kryptografische Module
Sicherheitsleitlinie
präzise Spezifikation der Sicherheitsregeln, nach denen ein Krypto-Modul arbeiten muss, einschließlich der aus den Anforderungen dieser Internationalen Norm abgeleiteten Regeln sowie weiteren Regeln, die von der Modul- oder Validierungsinstanz vorgegeben werden

ANMERKUNG Siehe Anhang B.

3.27
Datenweg
physische oder logische Route, entlang der sich Daten bewegen

ANMERKUNG Auf einem physischen Datenweg können mehrere logische Datenwege verlaufen.

3.28
eingeschränkter Betrieb
Betrieb, bei dem aufgrund der Rekonfiguration nach einem Fehlerzustand lediglich ein Teilsatz des gesamten Satzes an Algorithmen, Sicherheitsfunktionen, Diensten oder Prozessen verfügbar und/oder konfigurierbar ist

3.29
differentielle Stromverbrauchsanalyse
DPA
(en: differential power analysis)
Analyse der Schwankungen des Stromverbrauchs eines Krypto-Moduls mit dem Ziel, Informationen im Zusammenhang mit dem kryptografischen Betrieb zu erhalten

3.30
digitale Signatur
an eine Dateneinheit angefügte Daten oder eine kryptografische Transformation einer Dateneinheit, mit der ein Empfänger der Dateneinheit die Möglichkeit der Überprüfung der Quelle und Integrität der Dateneinheit erhält und die einen Schutz gegen Fälschung, z. B. durch den Empfänger, bietet

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

3.31
Direkteingabe
Eingabe eines SSP oder einer Schlüsselkomponente in ein Krypto-Modul über ein Gerät, wie z. B. eine Tastatur

3.32
Teilsignatur
(en: disjoint signature)
eine oder mehrere Signaturen, die zusammen einen vollständigen Codesatz darstellen

3.33
elektromagnetische Emanationen
EME
Informationen enthaltendes Signal, das, wenn es abgefangen und ausgewertet wird, möglicherweise die von einem beliebigen informationsverarbeitenden Gerät übertragenen, empfangenen, koordinierten oder anderweitig verarbeiteten Informationen preisgibt

3.34
elektronische Eingabe
Eingabe von SSP oder Schlüsselkomponenten in ein Krypto-Modul mit elektronischen Methoden

ANMERKUNG Es kann sein, dass der Bediener des Schlüssels keine Kenntnis über den eingegebenen Schlüsselwert hat.

3.35
Gesamtsignatur
(en: encompassing signature)
Einzelne Signatur für einen vollständigen Codesatz

3.36
verschlüsselter Schlüssel
kryptografischer Schlüssel, dessen Verschlüsselung unter Verwendung einer genehmigten Sicherheitsfunktion mit einem Schlüssel-Verschlüsselungsschlüssel (KEK) durchgeführt wurde. Wird als geschützt angesehen

3.37
Entität
Person, Gruppe, Gerät oder Prozess

3.38
Entropie
Messgröße für die Unordnung, Zufälligkeit oder Variabilität innerhalb eines abgeschlossenen Systems

ANMERKUNG Die Entropie einer Zufallsvariablen X ist eine mathematische Messgröße für die Menge an Informationen, die sich aus der Beobachtung von X ergibt.

3.39
Schutz vor umgebungsbedingtem Ausfall
EFP
(en: environmental failure protection)
Anwendung von Funktionen zum Schutz gegen das Kompromittieren der Sicherheit eines Krypto-Moduls aufgrund von Umgebungsbedingungen, die sich außerhalb des üblichen Betriebsbereichs des Krypto-Moduls befinden

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

3.40
Prüfung auf umgebungsbedingten Ausfall
EFT
(en: environmental failure testing)
Anwendung spezieller Methoden, um in angemessenem Umfang sichergehen zu können, dass die Sicherheit eines Krypto-Moduls nicht aufgrund von Umgebungsbedingungen, die sich außerhalb des üblichen Betriebsbereichs des Krypto-Moduls befinden, kompromittiert wird

3.41
Fehlererkennungscode
EDC
(en: error detection code)
aus Daten berechneter Wert, der aus redundanten Informationsbits besteht und dafür bestimmt ist, unbeabsichtigte Änderungen in den Daten zu erkennen, jedoch nicht zu korrigieren

3.42
ausführbare Form
Form des Codes, mit dem die Software oder Firmware vollständig von der Betriebsumgebung des Krypto-Moduls verwaltet und gesteuert wird und die keine Kompilierung (z. B. keinen Quellcode, Objektcode oder per JIT kompilierten Code) erfordert

3.43
Fehlerinjektion
Technik, bei der mittels Einsatz von Spannungsimpulsen, Strahlung, Laser oder Taktversatz Änderungen des Betriebsverhaltens der Hardware hervorgerufen werden

3.44.
endlicher Automat
EA
mathematisches Modell einer sequenziellen Maschine, die über einen endlichen Satz an Eingabeereignissen, einen endlichen Satz an Ausgabeereignissen, einen endlichen Satz an Zuständen, eine Funktion, die Zustände und Eingaben den Ausgaben zuordnet (Zustandsübergangsfunktion) und eine den ursprünglichen Zustand beschreibende Funktion verfügt

3.45
Firmware
ausführbarer Code eines Krypto-Moduls, der auf innerhalb der kryptografischen Begrenzung befindlichen Hardware gespeichert ist und während seiner Ausführung beim Betrieb in einer nicht modifizierbaren oder begrenzten Betriebsumgebung nicht dynamisch geschrieben oder modifiziert werden kann

BEISPIEL Speicher-Hardware kann u. a. sein: PROM, EEPROM, FLASH, Solid-State-Speicher, Festplatten usw.

3.46
Firmwaremodul
Modul, das ausschließlich aus Firmware besteht

3.47
Funktionsspezifikation
allgemeine Beschreibung der für den Bediener sichtbaren Anschlüsse und Schnittstellen und allgemeine Beschreibung des Verhaltens des Krypto-Moduls

3.48
Funktionsprüfung
Prüfung der in der Funktionsspezifikation definierten Funktionen des Krypto-Moduls

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

3.49
hart/Härte
relative Widerstandsfähigkeit eines Metalls oder anderen Werkstoffs gegenüber Einkerbungen, Kratzern oder Verbiegen; physisch gehärtet; robust und widerstandsfähig

ANMERKUNG Die relative Widerstandsfähigkeit des Werkstoffs gegenüber dem Eindringen eines anderen Objekts.

3.50
Hardware
physische Einrichtungen/Komponenten innerhalb der kryptografischen Begrenzung, mit denen Programme und Daten verarbeitet werden

3.51
Hardwaremodul
Modul, das hauptsächlich aus Hardware besteht und auch Firmware enthalten kann

3.52
Hardwaremodul-Schnittstelle
HMI
(en: hardware module interface)
gesamter Befehlssatz zur Anforderung der Dienste des Hardwaremoduls, einschließlich Parametern, die im Rahmen des angeforderten Dienstes die kryptografische Begrenzung des Moduls in beliebiger Richtung passieren

3.53
Hash-Wert
Ausgabe einer kryptografischen Hashfunktion

3.54
Hybridmodul
Modul, dessen kryptografische Begrenzung den Verbund einer Software- oder Firmwarekomponente und einer separaten Hardwarekomponente abgrenzt

3.55
Hybridfirmwaremodul-Schnittstelle
HFMI
(en: hybrid firmware module interface)
gesamter Befehlssatz zur Anforderung der Dienste des Hybridfirmwaremoduls, einschließlich Parametern, die im Rahmen des angeforderten Dienstes die kryptografische Begrenzung des Moduls in beliebiger Richtung passieren

3.56
Hybridsoftwaremodul-Schnittstelle
HSMI
(en: hybrid software module interface)
gesamter Befehlssatz zur Anforderung der Dienste des Hybridsoftwaremoduls, einschließlich Parametern, die im Rahmen des angeforderten Dienstes die kryptografische Begrenzung des Moduls in beliebiger Richtung passieren

3.57
Eingabedaten
Information, die in ein Krypto-Modul eingegeben wird und unter Verwendung einer genehmigten Sicherheitsfunktion zum Zweck der Transformation oder Berechnung eingesetzt werden kann

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

3.58
Integrität
Eigenschaft, dass Daten nicht auf unautorisierte und unbemerkte Weise modifiziert oder gelöscht worden sind

3.59
Schnittstelle
logischer Eingangs- oder Ausgangspunkt eines Krypto-Moduls, der logischen Informationsströmen den Zugang zum Modul ermöglicht

3.60
von ISO/IEC übernommen
Sicherheitsfunktion, die entweder

— in einer ISO/IEC-Norm festgelegt ist, oder

— in eine ISO/IEC-Norm übernommen wurde oder darin empfohlen wird und entweder in einem Anhang der ISO/IEC-Norm oder in einem Dokument, auf das die ISO/IEC-Norm verweist, festgelegt ist

3.61
Schlüsselübereinstimmung
Verfahren zur SSP-Bereitstellung, bei dem der entstehende Schlüssel aus Informationen von zwei oder mehr Teilnehmern abgeleitet wird, so dass keine Partei vorab mithilfe von automatisierten Methoden den Wert des Schlüssels ohne Kenntnis des Beitrags der anderen Partei(en) bestimmen kann

3.62
Schlüssel-Verschlüsselungsschlüssel
KEK
(en: key encryption key)
kryptografischer Schlüssel, der für die Ver- oder Entschlüsselung anderer Schlüssel genutzt wird

3.63
Schlüsseleingabegerät
(en: key loader)
eigenständiges Gerät, das in der Lage ist, mindestens einen in Klartext gehaltenen oder verschlüsselten SSP oder eine solche Schlüsselkomponente zu speichern, die auf Anforderung in ein Krypto-Modul übertragen werden kann

ANMERKUNG Der Einsatz eines Schlüsseleingabegeräts erfordert das Eingreifen durch eine Person.

3.64
Schlüsselverwaltung
Administration und Anwendung von Erzeugung, Registrierung, Zertifizierung, Deregistrierung, Verteilung, Installierung, Speicherung, Archivierung, Zurückziehen, Ableiten und Vernichtung von Schlüsselmaterial in Übereinstimmung mit einer Sicherheitsleitlinie

3.65
Schlüsseltransport
Prozess der Übertragung eines Schlüssels von einer Entität zu einer anderen Entität mithilfe automatischer Methoden

3.66
begrenzte Betriebsumgebung
Betriebsumgebung, die so ausgelegt ist, dass sie nur kontrollierte Firmwareänderungen akzeptiert und nur dann, wenn diese die Prüfung zum Laden von Software/Firmware erfolgreich bestanden haben

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

3.67
detaillierte Prüfung
Prüfung der einzelnen Komponenten oder Komponentengruppen des Krypto-Moduls und ihrer physischen Anschlüsse und logischen Schnittstellen

3.68
Wartungsrolle
Rolle, die eingenommen wird, um physische und/oder logische Wartungsmaßnahmen durchzuführen

BEISPIEL Zu Wartungsmaßnahmen zählt u. a. die Hardware- und/oder Softwarediagnostik

3.69
manuell
Eingreifen einer bedienenden Person erfordernd

3.70
Mitteilungsauthentisierungscode
MAC
(en: message authentication code)
kryptografische Prüfsumme für Daten, die mithilfe eines symmetrischen Schlüssels sowohl versehentliche als auch vorsätzliche Modifikationen dieser Daten aufdeckt

BEISPIEL Ein Hash-basierter Mitteilungsauthentisierungscode

3.71
Mikrocode
Prozessoranweisungen, die einer ausführbaren Programmanweisung entsprechen

BEISPIEL Assembler-Code

3.72
minimale Entropie
untere Entropiegrenze, die bei der Bestimmung der ungünstigsten Schätzung einer Beispielentropie noch hilfreich ist

3.73
modifizierbare Betriebsumgebung
Betriebsumgebung, die so ausgelegt ist, dass sie funktionale Änderungen akzeptiert, die möglicherweise nicht kontrollierte Software (z. B. nicht vertrauenswürdig) enthalten

3.74
Mehrfaktor-Authentifizierung
Authentifizierung durch mindestens zwei voneinander unabhängige Authentifizierungsfaktoren

ANMERKUNG 1 Ein Authentifizierungsfaktor ist eine Information und ein Prozess, mit denen die Identität einer Entität authentifiziert oder verifiziert wird.

ANMERKUNG 2 Kategorien für unabhängige Authentifizierungsfaktoren sind: die Kenntnis der Entität von etwas, etwas, das im Besitz der Entität ist und eine Eigenschaft der Entität.

3.75
eingebettetes Multichip-Krypto-Modul
physische Ausführung, bei der zwei oder mehr integrierte Schaltkreise miteinander verbunden und in ein Gehäuse oder ein Produkt eingebettet sind, das möglicherweise nicht über einen physischen Schutz verfügt

BEISPIEL Adapter und Erweiterungskarten (Expansion Boards)

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

3.76
eigenständiges Multichip-Krypto-Modul
physische Ausführung, bei der zwei oder mehr integrierte Schaltkreise miteinander verbunden sind und das gesamte Gehäuse physisch geschützt ist

BEISPIEL Router mit verschlüsselter Übertragung oder gesicherte Funkanlagen

3.77
Anwenderleitlinien
schriftliche Unterlagen, die vom Anwender und/oder anderen nicht administrativen Rollen für das Betreiben des Krypto-Moduls in einem genehmigten Betriebsmodus herangezogen werden

ANMERKUNG Die Anwenderleitlinien beschreiben die Sicherheitsfunktionen des Krypto-Moduls und enthalten Informationen und Verfahren hinsichtlich der sicheren Nutzung des Krypto-Moduls, darunter Anweisungen, Leitlinien und Warnhinweise.

3.78
nicht-invasiver Angriff
Angriff auf ein Krypto-Modul ohne direkten physischen Kontakt mit den Komponenten innerhalb der kryptografischen Begrenzung des Moduls

ANMERKUNG Ein Angriff, der den Zustand des Krypto-Moduls nicht abwandelt oder ändert.

3.79
nicht modifizierbare Betriebsumgebung
Betriebsumgebung, die so ausgelegt ist, dass sie keine Veränderungen an der Firmware akzeptiert

3.80
nicht sicherheitsrelevant
so implementiert, dass der genehmigte sichere Betrieb des Krypto-Moduls nicht gestört oder kompromittiert wird

3.81
Normalbetrieb
Betrieb, bei dem der gesamte Satz an Algorithmen, Sicherheitsfunktionen, Diensten oder Prozessen verfügbar und/oder konfigurierbar ist

3.82
opak
lichtundurchlässig (d. h. für Licht innerhalb des sichtbaren Spektrums mit Wellenlängen von 400 nm bis 750 nm); im sichtbaren Spektrum weder transparent noch durchscheinend

3.83
Betriebsumgebung
Satz der gesamten Software und Hardware, bestehend aus einem Betriebssystem und einer Hardware-Plattform, die für den sicheren Betrieb des Krypto-Moduls erforderlich ist

3.84
Betriebszustand
Zustand, in dem von einem Bediener Dienste oder Funktionen angefordert und die Ergebnisdaten auf der Datenausgabeschnittstelle des Krypto-Moduls ausgegeben werden können

3.85
Bediener
Einzelperson oder im Auftrag einer Einzelperson handelnder Prozess (Subjekt), die/der für die Annahme einer oder mehrerer Rollen autorisiert ist

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

3.86
Ausgabedaten
Informationen oder berechnete Ergebnisse, die von einem Krypto-Modul erzeugt werden

3.87
Passivierung
Effekt eines reaktiven Prozesses an Verbindungspunkten, Oberflächen oder Komponenten von Halbleitern sowie integrierten Schaltkreisen, die so ausgelegt sind, dass sie Erkennungs- und Schutzmaßnahmen beinhalten

BEISPIEL Quarzglas oder Phosphorglas

ANMERKUNG Eine Passivierung kann das Verhalten des Schaltkreises beeinflussen. Der für die Passivierung verwendete Werkstoff ist von der genutzten Technologie abhängig.

3.88
Passwort
Zeichenfolge, die für die Authentifizierung einer Identität oder für die Verifizierung einer Zugriffsautorisierung genutzt wird

BEISPIEL Buchstaben, Zahlen und andere Symbole

3.89
persönliche Identifikationsnummer
PIN
numerischer Code, der für die Authentifizierung einer Identität genutzt wird

3.90
physischer Schutz
Sicherung eines Krypto-Moduls, von CSP und von PSP mithilfe physischer Mittel

3.91
Klartext-Schlüssel
unverschlüsselter kryptografischer Schlüssel oder kryptografischer Schlüssel, der als ungeschützt angesehen wird, da er mit nicht genehmigten Methoden unkenntlich gemacht wurde

3.92
Anschluss
physischer/logischer Eingangs- oder Ausgangspunkt eines Krypto-Moduls, der den Zugang zum Modul ermöglicht

3.93
vorbetrieblicher Selbsttest
Überprüfung, die von einem Krypto-Modul zwischen dem Zeitpunkt des Einschaltens oder Instantiierens (nach dem Ausschalten, Zurücksetzen, einem Reboot, Kaltstart, Stromausfall usw.) des Moduls und dem Übergang in den Betriebszustand ausgeführt wird

3.94
privater Schlüssel
Schlüssel des asymmetrischen Schlüsselpaars einer Entität, der ausschließlich von dieser Entität verwendet werden sollte

ANMERKUNG Im Fall eines asymmetrischen Signatursystems definiert der private Schlüssel die Signaturtransformation. Bei einem asymmetrischen Verschlüsselungssystem definiert der private Schlüssel die Entschlüsselungstransformation.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

3.95
Produktionsqualität
Produkt, Komponente oder Software, das/die eine Prüfung auf Übereinstimmung mit den Betriebsspezifikationen bestanden hat

3.96
öffentlicher Schlüssel
Schlüssel des asymmetrischen Schlüsselpaars einer Entität, der öffentlich gemacht werden kann

ANMERKUNG 1 Im Fall eines asymmetrischen Signatursystems definiert der öffentliche Schlüssel die Verifizierungstransformation. Bei einem asymmetrischen Verschlüsselungssystem definiert der öffentliche Schlüssel die Verschlüsselungstransformation. Ein „öffentlich bekannter" Schlüssel ist nicht notwendigerweise auch überall verfügbar. Es kann sein, dass der Schlüssel ausschließlich allen Mitgliedern einer vordefinierten Gruppe zur Verfügung steht.

ANMERKUNG 2 Für die Anwendung dieser Internationalen Norm werden öffentliche Schlüssel nicht als CSP betrachtet.

3.97
Zertifikat eines öffentlichen Schlüssels
Informationen eines öffentlichen Schlüssels einer Entität, die von einer entsprechenden Zertifizierungsinstanz signiert und auf diese Weise fälschungssicher gemacht wurden

3.98
kryptografischer Algorithmus mit öffentlichem Schlüssel (asymmetrischer Algorithmus)
kryptografischer Algorithmus, der zwei zusammenhängende Schlüssel, einen öffentlichen und einen privaten, nutzt

ANMERKUNG Die beiden Schlüssel haben die Eigenschaft, dass es hinsichtlich Rechenleistung nicht machbar ist, den privaten Schlüssel aus dem öffentlichen Schlüssel abzuleiten.

3.99
öffentlicher Sicherheitsparameter
PSP
(en: public security parameter)
sicherheitsbezogene öffentliche Information, deren Modifizierung die Sicherheit eines Krypto-Moduls kompromittieren kann

BEISPIEL Öffentliche kryptografische Schlüssel, Zertifikate von öffentlichen Schlüsseln, selbstsignierte Zertifikate, Vertrauensanker, Einmal-Passwörter mit zugeordnetem Zähler sowie intern vorgehaltene Datums- und Uhrzeitangaben

ANMERKUNG Ein PSP gilt als geschützt, wenn er nicht modifiziert werden kann oder eine solche Modifizierung vom Modul bestimmbar ist.

3.100
Zufallsbitgenerator
RGB
(en: random bit generator)
Gerät oder Algorithmus, das/der eine anscheinend statistisch unabhängige und von systematischen Fehlern freie Bitfolge ausgibt

3.101
entfernbare Abdeckung
physisches Mittel, das gezielt so gestaltet ist, dass es einen nicht beschädigenden Zugang zu den physischen Komponenten eines Krypto-Moduls erlaubt

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

3.102
Rolle
Sicherheitsattribut, das einem Anwender zugeordnet ist und das die Zugriffsrechte bzw. -beschränkungen hinsichtlich der Dienste eines Krypto-Moduls für Anwender definiert

ANMERKUNG Einer Rolle können einer oder mehrere Dienste zugeordnet sein. Eine Rolle kann einem oder mehreren Anwendern zugeordnet sein und ein Anwender kann eine oder mehrere Rollen haben.

3.103
rollenbasierte Zugriffskontrolle
RBAC
(en: role-based access control)
Berechtigungen, die einer Rolle zugeordnet sind und dieser den Zugriff auf ein Objekt erlauben

3.104
Laufzeitumgebung
virtueller Gerätezustand, der zur Laufzeit eines Computers Software-Dienste für Prozesse oder Programme bereitstellt

ANMERKUNG Der Begriff kann sich auf das Betriebssystem selbst oder auf die Software beziehen, auf der das Betriebssystem aufgesetzt ist. Hauptziel ist es, eine „plattformunabhängige“ Programmierung zu ermöglichen.

3.105
geheimer Schlüssel
kryptografischer Schlüssel, der mit einem einer oder mehreren Entitäten eindeutig zugeordneten kryptografischen Secret-Key-Algorithmus verwendet wird und nicht öffentlich verbreitet werden sollte

3.106
Sicherheitsfunktion
kryptografische Algorithmen in Kombination mit Betriebsmodi, wie beispielsweise Blockverschlüsselung, Stromverschlüsselung, Algorithmen mit symmetrischen oder asymmetrischen Schlüsseln, Mitteilungs-authentisierungscodes, Hashfunktionen oder andere Sicherheitsfunktionen, Zufallsbitgeneratoren, Authentisierung von Entitäten sowie SSP-Erzeugung und -Bereitstellung, die alle entweder von ISO/IEC oder einer Genehmigungsinstanz genehmigt wurden

ANMERKUNG Siehe Anhang C.

3.107
Startwert
Seed
geheimer Wert, mit dem ein Zufallsbitgenerator initialisiert wird

3.108
Selbsttest
vor dem Betrieb oder unter bestimmten Bedingungen durchgeführte Prüfung, die vom Krypto-Modul ausgeführt wird

3.109
sensible Daten
Daten, die nach Ansicht des Anwenders Schutz erfordern

3.110
sensible Sicherheitsparameter
SSP
(en: sensitive security parameters)
kritische Sicherheitsparameter (CSP) und öffentliche Sicherheitsparameter (PSP)

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

3.111
Dienst
von einem Bediener extern ausgelöste(r) Vorgang oder Funktion, der/die von einem Krypto-Modul ausgeführt werden kann

3.112
Diensteingabe
vom Krypto-Modul verwendete Daten oder Steuerinformationen, die bestimmte Vorgänge oder Funktionen initiieren oder anfordern

3.113
Dienstausgabe
Daten oder Statusinformationen, die das Ergebnis von mittels Diensteingabe initiierten oder angeforderten Vorgängen oder Funktionen sind

3.114
einfache Stromverbrauchsanalyse
SPA
(en: simple power analysis)
direkte (hauptsächlich visuelle) Analyse der Muster von Anweisungsausführungen (oder der Ausführung einzelner Anweisungen) im Zusammenhang mit dem Stromverbrauch eines Krypto-Moduls mit dem Ziel, Informationen im Zusammenhang mit dem kryptografischen Betrieb zu erhalten

3.115
Einzelchip-Krypto-Modul
physische Ausführung, bei der ein einzelner integrierter Schaltkreis als eigenständiges Gerät verwendet oder in ein Gehäuse oder ein Produkt eingebettet sein kann, das möglicherweise nicht über einen physischen Schutz verfügt

BEISPIEL Chips mit integriertem Einzelschaltkreis oder Chipkarten mit integriertem Einzelschaltkreis

3.116
Software
ausführbarer Code eines Krypto-Moduls, der auf löschbaren Medien gespeichert ist und während der Ausführung beim Betrieb in einer modifizierbaren Betriebsumgebung dynamisch geschrieben oder modifiziert werden kann

BEISPIEL Löschbare Medien können u. a. sein: Solid-State-Speicher, Festplatten usw.

3.117
Softwaremodul
Modul, das ausschließlich aus Software besteht

3.118
Prüfung zum Laden von Software/Firmware
Reihe von Prüfungen, die mit Software oder Firmware durchgeführt und erfolgreich bestanden werden muss, bevor diese Soft-/Firmware von einem Krypto-Modul ausgeführt werden kann

ANMERKUNG Nicht anwendbar, wenn die Software oder Firmware ein vollständiges Image darstellt und ausschließlich nach einem Power Cycling des Moduls ausgeführt wird

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

3.119
Software-/Firmwaremodul-Schnittstelle
SFMI
(en: software/firmware module interface)
Befehlssatz zur Anforderung der Dienste des Software- oder Firmwaremoduls, einschließlich Parametern, die im Rahmen des angeforderten Dienstes die kryptografische Begrenzung des Moduls in beliebiger Richtung passieren

3.120
Secret-Sharing
Geheimnisteilung
Technik, bei der ein kryptografischer Schlüssel in mehrere Schlüsselkomponenten aufgeteilt wird, die jeweils keine Auskunft über die anderen Komponenten geben und die anschließend von separaten Entitäten in ein Krypto-Modul eingegeben oder von diesem ausgegeben werden können und in Kombination wieder den ursprünglichen kryptografischen Schlüssel bilden

ANMERKUNG Zur Ausführung dieser Kombination können alle oder nur eine Teilmenge der Komponenten erforderlich sein.

3.121
SSP-Bereitstellung
Vorgang, bei dem ein gemeinsamer SSP für eine oder mehrere Entitäten verfügbar gemacht wird

ANMERKUNG Die SSP-Bereitstellung umfasst SSP-Übereinstimmung, SSP-Transport und SSP-Eingabe oder -Ausgabe.

3.122
Zustandsinformation
Information, die zum Zweck der Anzeige bestimmter Betriebsmerkmale oder -zustände des Krypto-Moduls von diesem Modul ausgegeben wird

3.123
widerstandsfähig
nicht einfach zu besiegen, über mehr als erwartungsgemäße oder überdurchschnittliche Kraft oder Stärke verfügend, widerstandsfähig gegenüber einem Angriff oder solide gebaut

3.124
symmetrische Kryptografietechnik
Kryptografietechnik, bei der sowohl für die Verschlüsselungs- als auch für die Entschlüsselungs-transformation derselbe geheime Schlüssel verwendet wird

3.125
Manipulationserkennung
automatisches Bestimmen durch ein Krypto-Modul, dass ein Versuch unternommen wurde, die Sicherheit des Moduls zu kompromittieren

3.126
Manipulationsschutz
beobachtbare Anzeige, dass ein Versuch unternommen wurde, die Sicherheit eines Krypto-Moduls zu kompromittieren

3.127
Manipulationsreaktion
automatische Aktion, die ein Krypto-Modul durchführt, wenn eine Manipulationserkennung stattgefunden hat

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

3.128
Vertrauensanker
vertrauenswürdige Information, die einen Algorithmus für einen öffentlichen Schlüssel, den Wert eines öffentlichen Schlüssels, einen Ausstellernamen und optional weitere Parameter umfasst

BEISPIEL Zu weiteren Parametern kann u. a. ein Gültigkeitszeitraum zählen.

ANMERKUNG Ein Vertrauensanker kann in Form eines selbstsignierten Zertifikats bereitgestellt werden.

3.129
vertrauenswürdiger Kanal
vertrauenswürdige und sichere Kommunikationsverbindung, die zwischen dem Krypto-Modul und einem Absender oder Empfänger aufgebaut ist, um auf sichere Weise ungeschützte Klartext-CSP, Schlüsselkomponenten und Authentisierungsdaten zu übertragen

ANMERKUNG Ein vertrauenswürdiger Kanal schützt vor Abfangversuchen und physischer oder logischer Manipulation durch unerwünschte Bediener/Entitäten, Prozesse oder andere Geräte zwischen den definierten Eingabe- oder Ausgabeanschlüssen des Krypto-Moduls und entlang der Kommunikationsverbindung mit dem beabsichtigten Endpunkt.

3.130
Anwender
Rolle, die eine Person oder ein Prozess (d. h. ein Subjekt), der für eine Person agiert, inne hat, die/der auf ein Krypto-Modul zugreift, um Kryptografie-Dienste anzufordern

3.131
validiert
mit Sicherheit von einer Validierungsinstanz auf Konformität geprüft

3.132
Validierungsinstanz
Entität, die die Prüfergebnisse zur Konformität mit dieser Internationalen Norm validiert

3.133
Anbieter
Entität, Gruppe oder Vereinigung, die das Krypto-Modul zur Prüfung und Validierung einreicht

ANMERKUNG Der Anbieter hat Zugriff auf alle relevanten Unterlagen und Entwurfsnachweise, ungeachtet dessen, ob er das Krypto-Modul tatsächlich entworfen oder entwickelt hat oder nicht.

3.134
Löschen/Vernichten
Methode des Zerstörens gespeicherter Daten und ungeschützter SSP, um deren Wiederherstellung und Wiederverwendung zu verhindern

4 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

API Programmierschnittstelle (en: application program interface)

CBC Cipher Block Chaining (Betriebsart zur Blockverschlüsselung)

CCM Zähler mit Cipher-Block-Chaining-Nachrichtenauthentisierungscode (en: counter with cipher block chaining-message authentication code)

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

ECB	Electronic Codebook (Betriebsart zur Blockverschlüsselung)
HDL	Hardwarebeschreibungssprache (en: hardware description language)
IC	integrierter Schaltkreis (en: integrated circuit)
PROM	programmierbarer Nur-Lese-Speicher (en: programmable read-only memory)
RAM	Direktzugriffsspeicher (en: random access memory)
URL	Uniform Resource Locator

5 Sicherheitsstufen für Krypto-Module

Die folgenden Unterabschnitte bieten einen Überblick über die vier Sicherheitsstufen. Gängige Beispiele, die veranschaulichen, wie die Anforderungen eingehalten werden könnten, sind nicht als einschränkend oder erschöpfend zu verstehen. In diesem Dokument sind Verweisungen auf ein *Modul* als Verweisungen auf ein *Krypto-Modul* zu interpretieren. Die kryptografischen Techniken sind über die vier Sicherheitsstufen hinweg identisch. Die Sicherheitsanforderungen für den Schutz des Moduls selbst (z. B. Zugriff und Kenntnis der internen Komponenten und des Betriebs) und der Sicherheitsparameter, die im Modul enthaltenen sind und durch es gesteuert werden, steigen von Stufe zu Stufe an. Jede Sicherheitsanforderung ist durch ein **muss [xx.yy]** bzw. **darf nicht [xx.yy]** gekennzeichnet, wobei **xx** den Abschnitt bezeichnet und **yy** eine numerische Kennzahl innerhalb des Abschnitts ist.

5.1 Sicherheitsstufe 1

Sicherheitsstufe 1 ist die Grundsicherheitsstufe. Für ein Krypto-Modul werden grundlegende Sicherheitsanforderungen festgelegt (z. B. es muss mindestens eine genehmigte Sicherheitsfunktion oder ein genehmigtes Verfahren zur Bereitstellung sensibler Sicherheitsparameter angewendet werden). Software- oder Firmwaremodule dürfen in einer nicht modifizierbaren, begrenzten oder modifizierbaren Betriebsumgebung betrieben werden. In einem Hardware-Krypto-Modul der Sicherheitsstufe 1 sind keine speziellen physischen Sicherheitsmechanismen erforderlich, die über die grundlegenden Anforderungen an Komponenten in Produktionsqualität hinausgehen. Die implementierten Verfahren zur Schadensminderung bei nicht-invasiven oder anderen Angriffen werden dokumentiert. Beispiele für ein Krypto-Modul der Sicherheitsstufe 1 sind eine Hardwareverschlüsselungsplatine, die sich in einem Personal Computer (PC) befindet, oder ein kryptografisches Toolkit, das in einem tragbaren Gerät oder Universalcomputer ausgeführt wird.

Solche Implementierungen sind ideal für Sicherheitsanwendungen geeignet, bei denen Kontrollen, wie die der physischen und der Netzwerksicherheit, und Verwaltungsverfahren außerhalb des Moduls, aber in der Umgebung, in der es eingesetzt werden soll, vorgesehen sind. So kann beispielsweise die Implementierung des Krypto-Moduls der Sicherheitsstufe 1 in solchen Umgebungen kostengünstiger sein als entsprechende Module auf höheren Sicherheitsstufen, die eine höhere Sicherheit der SSP des Moduls bieten und es Organisationen ermöglichen, alternative kryptografische Lösungen auszuwählen, um den Sicherheitsanforderungen gerecht zu werden, wenn eine Beachtung der Umgebung, in der das Modul betrieben wird, für die Gesamtsicherheit entscheidend ist.

5.2 Sicherheitsstufe 2

Sicherheitsstufe 2 erweitert die physischen Sicherheitsmechanismen der Sicherheitsstufe 1 um die Anforderung des Manipulationsschutzes, der die Verwendung von Manipulationsschutzbeschichtungen oder -siegeln oder aufbruchssicheren Schlössern an entfernbaren Abdeckungen oder an Türen beinhaltet.

Manipulationsschutzbeschichtungen oder -siegel werden auf ein Modul aufgebracht, so dass die Beschichtung oder das Siegel aufgebrochen werden muss, um einen physischen Zugang zu den SSP innerhalb

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

des Moduls zu erhalten. Zum Schutz vor unbefugtem Zugriff werden auf Abdeckungen oder an Türen Manipulationsschutzsiegel oder aufbruchssichere Schlösser angebracht.

Sicherheitsstufe 2 erfordert eine rollenbasierte Authentifizierung, bei der ein Krypto-Modul die Berechtigung eines Bedieners authentifiziert, eine bestimmte Rolle zu übernehmen und einen entsprechenden Satz von Diensten auszuführen.

Sicherheitsstufe 2 ermöglicht die Ausführung eines Software-Krypto-Moduls in einer modifizierbaren Umgebung, in der rollenbasierte Zugriffskontrollen oder zumindest eine anwenderbestimmte Zugriffskontrolle mit widerstandsfähigen Mechanismen zur Definition neuer Gruppen und zur Zuweisung eingeschränkter Berechtigungen über Zugriffskontrolllisten (z. B. ACL) implementiert sind, und die die Möglichkeit, jeden Anwender mehr als einer Gruppe zuzuweisen, sowie Schutz vor unbefugtem Ausführen, Ändern und Auslesen von kryptografischer Software bietet.

5.3 Sicherheitsstufe 3

Zusätzlich zu den für Sicherheitsstufe 2 geforderten physischen Sicherheitsmechanismen für den Manipulationsschutz sieht Sicherheitsstufe 3 als weitere Anforderung Schadensminderung bei unbefugtem Zugriff auf SSP innerhalb des Krypto-Moduls vor. Die für Sicherheitsstufe 3 erforderlichen physischen Sicherheitsmechanismen sollen mit hoher Wahrscheinlichkeit Versuche des direkten physischen Zugriffs, der Verwendung oder Modifizierung des Krypto-Moduls und das Eindringen mit einer Sonde durch Lüftungslöcher oder -schlitze erkennen und darauf reagieren können. Die physischen Sicherheitsmechanismen dürfen den Einsatz von widerstandsfähigen Gehäusen und einer Manipulationserkennungs- und -reaktionsschaltung beinhalten, die alle CSP beim Öffnen der entfernbaren Abdeckungen/Türen des Krypto-Moduls löscht/vernichtet.

Sicherheitsstufe 3 erfordert identitätsbasierte Authentifizierungsmechanismen, die die Sicherheit der Stufe 2 durch rollenbasierte Authentifizierungsmechanismen erweitern. Ein Krypto-Modul authentifiziert die Identität eines Bedieners und überprüft, ob der identifizierte Bedienter berechtigt ist, eine bestimmte Rolle zu übernehmen und einen entsprechenden Satz von Diensten auszuführen.

Sicherheitsstufe 3 fordert die Verschlüsselung von manuell erstellten Klartext-CSP, die Nutzung eines vertrauenswürdigen Kanals oder die Verwendung eines Secret-Sharing-Verfahrens für die Eingabe oder Ausgabe.

Sicherheitsstufe 3 schützt ein Krypto-Modul auch vor einer Kompromittierung der Sicherheit durch Umgebungsbedingungen, die außerhalb der normalen Spannungs- und Temperatur-Betriebsbereiche des Moduls liegen. Ein Angreifer kann ein beabsichtigtes Überschreiten der normalen Betriebsbereiche nutzen, um die Verteidigungsmechanismen eines Krypto-Moduls außer Kraft zu setzen. Ein Krypto-Modul muss entweder mit speziellen Schutzfunktionen in Hinblick auf die Umgebungsbedingungen ausgestattet sein, die ein Überschreiten der Spannungs- und Temperaturgrenzen erkennen und die CSP löschen/vernichten, oder strenge Prüfungen in Bezug auf umgebungsbedingte Ausfälle durchlaufen, um auf angemessene Weise sicherzustellen, dass die Auswirkungen eines Überschreitens der normalen Betriebsbereiche die Sicherheit des Moduls nicht kompromittieren.

Schadensminderungsverfahren für nicht-invasive Angriffe nach 7.8, die im Modul implementiert sind, werden mit Metriken der Sicherheitsstufe 3 geprüft.

Nicht alle Abschnitte dieser Internationalen Norm sehen Sicherheitsstufe 3 für Software-Krypto-Module vor, daher ist die höchste Gesamtsicherheitsstufe, die das Software-Krypto-Modul erreichen kann, auf Sicherheitsstufe 2 beschränkt.

Module der Sicherheitsstufe 3 erfordern zusätzliche Lebenszyklussicherungen, wie automatisiertes Konfigurationsmanagement, detaillierte Auslegung, detaillierte Prüfung und eine Bedienerauthentifizierung mit vom Anbieter bereitgestellten Authentifizierungsinformationen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

5.4 Sicherheitsstufe 4

Sicherheitsstufe 4 bietet das höchste Maß an Sicherheit, das in dieser Internationalen Norm definiert ist. Diese Stufe umfasst alle geeigneten Sicherheitsmerkmale der unteren Stufen sowie erweiterte Merkmale.

Bei Sicherheitsstufe 4 bieten die physischen Sicherheitsmechanismen eine vollständige Schutzhülle für das Krypto-Modul, die darauf abzielt, alle Versuche eines unbefugten physischen Zugriffs zu erkennen und darauf zu reagieren, wenn das Modul SSP enthält, unabhängig davon, ob das Module extern mit Strom versorgt wird oder nicht. Ein Eindringen in das Gehäuse des Krypto-Moduls kann unabhängig von der Eindringrichtung mit sehr hoher Wahrscheinlichkeit erkannt werden und führt zum sofortigen Löschen/Vernichten aller ungeschützten SSP. Die Krypto-Module der Sicherheitsstufe 4 sind für den Betrieb in physisch ungeschützten Umgebungen geeignet.

Sicherheitsstufe 4 führt die Mehrfaktor-Authentifizierungsanforderung für die Bedienerauthentifizierung ein. Dafür sind mindestens zwei der folgenden drei Attribute erforderlich:

— etwas, das der Bediener kennt, wie z. B. ein geheimes Passwort;

— etwas, das der Bediener besitzt, wie z. B. ein physischer Schlüssel oder ein Token;

— eine physische Eigenschaft, z. B. ein biometrisches Merkmal.

Auf Sicherheitsstufe 4 muss ein Krypto-Modul mit speziellen Schutzfunktionen in Hinblick auf die Umgebungsbedingungen ausgestattet sein, die Spannungs- und Temperaturgrenzen erkennen und alle ungeschützten SSP löschen/vernichten, um auf angemessene Weise sicherzustellen, dass die Auswirkungen eines Überschreitens der normalen Betriebsbereiche die Sicherheit des Moduls nicht kompromittieren können.

Schadensminderungsverfahren für nicht-invasive Angriffe nach 7.8, die im Modul implementiert sind, werden mit Metriken der Sicherheitsstufe 4 geprüft.

Nicht alle Abschnitte dieser Internationalen Norm sehen Sicherheitsstufe 4 für Software-Krypto-Module vor, daher ist die höchste Gesamtsicherheitsstufe, die durch das Software-Krypto-Modul erreicht werden kann, auf Sicherheitsstufe 2 beschränkt.

Die Auslegung eines Moduls der Sicherheitsstufe 4 wird anhand der Übereinstimmung sowohl der Vor- als auch Nach-Zustandsbedingungen mit der Funktionsspezifikation überprüft.

6 Funktionale Sicherheitsziele

Die Sicherheitsanforderungen in dieser Internationalen Norm beziehen sich auf die sichere Auslegung und Implementierung eines Krypto-Moduls. Die Sicherheitsanforderungen beginnen mit grundlegenden Sicherheitszielen und nehmen mit steigenden Sicherheitsstufen und -zielen zu. Die Anforderungen ergeben sich aus den folgenden anspruchsvollen funktionalen Sicherheitszielen für ein Krypto-Modul wie folgt:

— die genehmigten Sicherheitsfunktionen zum Schutz sensibler Informationen werden angewendet und ordnungsgemäß implementiert;

— ein Krypto-Modul wird gegen unbefugte Bedienung oder Nutzung geschützt;

— die unbefugte Weitergabe der Inhalte des Krypto-Moduls, einschließlich der CSP, wird unterbunden;

— die unbefugte und unentdeckte Modifizierung des Krypto-Moduls und der kryptografischen Algorithmen sowie unbefugtes Modifizieren, Ersetzen, Einfügen und Löschen von SSP wird unterbunden;

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

— Anzeigen für den Betriebszustand des Krypto-Moduls werden vorgesehen;

— die ordnungsgemäße Funktion des Krypto-Moduls bei Betrieb in einer genehmigten Betriebsart wird sichergestellt;

— Fehler beim Betrieb des Moduls werden erkannt und eine Kompromittierung der SSP infolge dieser Fehler wird unterbunden; und

— die ordnungsgemäße Auslegung, Verteilung und Implementierung des Krypto-Moduls werden sichergestellt.

7 Sicherheitsanforderungen

7.1 Allgemeines

Dieser Abschnitt legt die Sicherheitsanforderungen fest, die das Krypto-Modul zur Einhaltung dieser Internationalen Norm erfüllen **muss [01.01]**. Die Sicherheitsanforderungen decken Bereiche ab, die sich auf die Auslegung sowie die Implementierung eines Krypto-Moduls beziehen. Diese Bereiche umfassen die Spezifikation und Schnittstellen des Krypto-Moduls, die Rollen, Dienste und Authentifizierung, die Software-/Firmware-Sicherheit, die Betriebsumgebung, die physische Sicherheit, die Sicherheit bei nicht-invasiven Angriffen, die Verwaltung von sensiblen Sicherheitsparametern, Selbsttests, die Lebenszyklus-sicherung und die Schadensminderung bei anderen Angriffen.

Tabelle 1 fasst die Sicherheitsanforderungen in jedem dieser Bereiche zusammen.

Ein Krypto-Modul **muss [01.02]** in Bezug auf die Anforderungen jedes in diesem Abschnitt behandelten Bereichs geprüft werden. Das Krypto-Modul **muss [01.03]** in jedem Bereich unabhängig bewertet werden. Einige Bereiche sehen eine höhere Sicherheit mit zusätzlichen Sicherheitsanforderungen für jede Sicherheitsstufe vor. In diesen Bereichen erhält das Krypto-Modul eine Bewertung, die der höchsten Sicherheitsstufe entspricht, für die das Modul alle Anforderungen dieses Bereichs erfüllt. In Bereichen, die keine unterschiedlichen Sicherheitsstufen vorsehen (d. h. Standardanforderungen), erhält das Krypto-Modul eine der Gesamtbewertung entsprechende Bewertung.

Zusätzlich zu den unabhängigen Bewertungen für jeden Sicherheitsbereich erhält ein Krypto-Modul auch eine Gesamtsicherheitsbewertung. Die Gesamtsicherheitsbewertung gibt die Mindeststufe der unabhängigen Bewertungen in den einzelnen Bereichen an.

Viele der Sicherheitsanforderungen dieser Internationalen Norm beinhalten spezifische Dokumentations-anforderungen, die in den Anhängen A und B zusammengefasst sind. Für ein Krypto-Modul, das einem unabhängigen Überprüfungs- oder Bewertungsverfahren zu unterziehen ist, **muss [01.04]** die vollständige Dokumentation, einschließlich Kopien der Anwender- und Installationshandbücher, Leistungs-beschreibungen und Lebenszyklusdokumentationen bereitgestellt werden.

Die Anhänge C, D, E und F verweisen auf genehmigte Sicherheitsfunktionen, genehmigte Verfahren zur Bereitstellung sensibler Sicherheitsparameter, genehmigte Authentifizierungsmechanismen und Prüfverfahren für die Schadensminderung von nicht-invasiven Angriffen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

Tabelle 1 — Zusammenfassung der Sicherheitsanforderungen

	Sicherheitsstufe 1	*Sicherheitsstufe 2*	*Sicherheitsstufe 3*	*Sicherheitsstufe 4*
Spezifikation des Krypto-Moduls	Spezifikation des Krypto-Moduls, der kryptografischen Begrenzung, der genehmigten Sicherheitsfunktionen sowie der normalen und eingeschränkten Betriebsmodi; Beschreibung des Krypto-Moduls, einschließlich aller Hardware-, Software- und Firmware-Komponenten; alle Dienste stellen Zustandsinformationen zur Verfügung, um anzuzeigen, wann der Dienst einen genehmigten kryptografischen Algorithmus, eine Sicherheits-funktion oder einen genehmigten kryptografischen Prozess in genehmigter Weise nutzt.			
Schnittstellen des Krypto-Moduls	erforderliche und optionale Schnittstellen; Spezifikation aller Schnittstellen und aller Ein- und Ausgabedatenwege		vertrauenswürdiger Kanal	
Rollen, Dienste und Authentifizierung	logische Trennung von erforderlichen und optionalen Rollen und Diensten	rollenbasierte oder identitätsbasierte Bediener-authentifizierung	identitätsbasierte Bediener-authentifizierung	Mehrfaktor-Authentifizierung
Software-/Firmware-Sicherheit	genehmigte Integritätstechnik oder EDC-basierte Integritätsprüfung; definierte SFMI, HFMI und HSMI; ausführbarer Code	genehmigte digitale Signatur oder authentisierungs-code-basierte Integritätsprüfung für verschlüsselte Nachrichten	genehmigte Integritätsprüfung anhand digitaler Signaturen	
Betriebsumgebung	nicht modifizierbar, begrenzt oder modifizierbar; Steuerung der SSP	modifizierbar; rollenbasierte oder anwenderbestimmte Zugriffskontrolle; Auditmechanismus		
Physische Sicherheit	Komponenten in Produktions-qualität	Manipulationsschutz; opake Abdeckung oder opakes Gehäuse	Manipulations-erkennung und -reaktion für Abdeckungen und Türen; widerstands-fähiges Gehäuse oder Beschichtung; Schutz vor direktem Eindringen mit einer Sonde; EFP oder EFT	Manipulations-erkennung und -reaktionshülle; EFP; Schadens-minderung bei Fehlerinjektion
Sicherheit bei nicht-invasiven Angriffen	Das Modul ist für die Schadensminderung nicht-invasiver Angriffe nach Anhang F ausgelegt.			
	Dokumentation und Wirksamkeit der in Anhang F aufgeführten Schadens-minderungstechniken		Schadens-minderungs-prüfungen	Schadens-minderungs-prüfungen
Verwaltung von sensiblen Sicherheits-parametern	Zufallsbitgeneratoren, SSP-Erzeugung, -Bereitstellung, -Eingabe und -Ausgabe, -Speicherung und -Löschen/Vernichten			
	automatisierter SSP-Transport oder SSP-Übereinstimmung mit genehmigten Verfahren			
	Manuell bereitgestellte SSP dürfen im Klartext eingegeben oder ausgegeben werden.		Manuell bereitgestellte SSP dürfen entweder verschlüsselt, über einen vertrauenswürdigen Kanal oder mittels Secret-Sharing-Verfahren eingegeben oder ausgegeben werden.	

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

		Sicherheitsstufe 1	*Sicherheitsstufe 2*	*Sicherheitsstufe 3*	*Sicherheitsstufe 4*
Selbsttests		vorbetrieblich: Prüfung der Software-/Firmware-Integrität, des Umgehens und der kritischen Funktionen			
		bedingt: Prüfung des kryptografischen Algorithmus, der paarweisen Konsistenz, des Ladens von Software/Firmware, der manuellen Eingabe, des bedingten Umgehens und der kritischen Funktionen			
Lebenszyklussicherung	**Konfigurations-management**	Konfigurationsmanagementsystem für das Krypto-Modul, die Komponenten und die Dokumentation; jedes einzelne Element wird während des gesamten Lebenszyklus eindeutig gekennzeichnet und verfolgt		automatisiertes Konfigurations-managementsystem	
	Auslegung	Auslegung des Moduls ermöglicht die Prüfung aller vorgesehenen sicherheitsbezogenen Dienste			
	EA	endlicher Automat			
	Entwicklung	kommentierter Quellcode, schematische Darstellungen oder HDL	höhere Software-Programmiersprache; höhere Hardwarebeschreibungssprache		Dokumentation mit Anmerkungen zu Vorbedingungen bei Eingabe in die Modulkomponenten und Nachbedin-gungen, deren Erfüllen nach Fertigstellung der Komponenten erwartet wird.
	Prüfungen	Funktionsprüfungen		detaillierte Prüfungen	
	Lieferung und Betrieb	Initialisierungs-verfahren	Lieferverfahren		Bediener-authentifizierung mit vom Anbieter bereitgestellten Authentisierungs-informationen
	Leitlinien	Leitlinien für Administratoren und Anwender			
Schadensminderung anderer Angriffe		Beschreibung der Schadensminderung von Angriffen, für die derzeit keine prüfbaren Anforderungen vorliegen			Beschreibung der Schadensminderung von Angriffen mit prüfbaren Anforderungen

7.2 Spezifikation des Krypto-Moduls

7.2.1 Allgemeine Anforderungen an die Spezifikation des Krypto-Moduls

Ein Krypto-Modul **muss [02.01]** aus einem Satz von Hardware, Software, Firmware oder aus einer Kombination daraus bestehen, in den mindestens ein definierter kryptografischer Dienst implementiert ist, der einen genehmigten kryptografischen Algorithmus, eine genehmigte Sicherheitsfunktion oder einen genehmigten kryptografischen Prozess nutzt, und der von einer definierten kryptografischen Begrenzung umschlossen ist.

Die in A.2.2. angegebenen Dokumentationsanforderungen **müssen [02.02]** eingehalten werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

7.2.2 Arten von Krypto-Modulen

Ein Krypto-Modul **muss [02.03]** als eine der folgenden Modularten definiert werden:

— Ein ***Hardwaremodul*** ist ein Modul, dessen kryptografische Begrenzung durch eine äußere Hardwarehülle festgelegt ist. Firmware und/oder Software, die auch ein Betriebssystem umfassen kann, dürfen sich innerhalb dieser kryptografischen Hardwarebegrenzung befinden.

— Ein ***Softwaremodul*** ist ein Modul, dessen kryptografische Begrenzung die Software eingrenzt, mit Ausnahme der Komponente(n) (es kann sich um eine oder mehrere Softwarekomponenten handeln), die in einer modifizierbaren Betriebsumgebung ausgeführt wird (werden). Die Rechnerplattform und das Betriebssystem der Betriebsumgebung, in der die Software ausgeführt wird, befinden sich außerhalb der definierten Softwaremodulbegrenzung.

— Ein ***Firmwaremodul*** ist ein Modul, dessen kryptografische Begrenzung die Firmware eingrenzt, mit Ausnahme der Komponente(n), die in einer begrenzten oder nicht modifizierbaren Betriebsumgebung ausgeführt wird (werden). Die Rechnerplattform und das Betriebssystem der Betriebsumgebung, in der die Firmware ausgeführt wird, befinden sich außerhalb der definierten Firmwaremodulbegrenzung, sind aber explizit an das Firmwaremodul gebunden.

— Ein ***Hybrid-Softwaremodul*** ist ein Modul, dessen kryptografische Begrenzung den Verbund aus einer Softwarekomponente und einer separaten Hardwarekomponente eingrenzt (d. h. die Softwarekomponente befindet sich nicht innerhalb der Hardwaremodulbegrenzung). Die Rechnerplattform und das Betriebssystem der Betriebsumgebung, in der die Software ausgeführt wird, befinden sich außerhalb der definierten Hybrid-Softwaremodulbegrenzung.

— Ein ***Hybrid-Firmwaremodul*** ist ein Modul, dessen kryptografische Begrenzung den Verbund aus einer Firmwarekomponente und einer separaten Hardwarekomponente eingrenzt (d. h. die Firmwarekomponente befindet sich nicht innerhalb der Hardwaremodulbegrenzung). Die Rechnerplattform und das Betriebssystem der Betriebsumgebung, in der die Firmware ausgeführt wird, befinden sich außerhalb der definierten Hybrid-Firmwaremodulbegrenzung, sind aber explizit an das Hybrid-Firmwaremodul gebunden.

Für Hardware- und Firmwaremodule **müssen [02.04]** die anwendbaren physischen Sicherheitsanforderungen und die Sicherheitsanforderungen für nicht-invasive Angriffe nach 7.7 und 7.8 eingehalten werden.

Für Softwaremodule, die in einer modifizierbaren Umgebung ausgeführt werden, sind die in 7.7 genannten physischen Sicherheitsanforderungen optional und die anwendbaren Sicherheitsanforderungen für nicht-invasive Angriffe nach 7.8 **müssen [02.05]** eingehalten werden.

Für Hybridmodule **müssen [02.06]** alle anwendbaren Anforderungen der Abschnitte 7.5, 7.6, 7.7 und 7.8 eingehalten werden.

7.2.3 Kryptografische Begrenzung

7.2.3.1 Allgemeine Anforderungen an die kryptografische Begrenzung

Eine kryptografische Begrenzung **muss [02.07]** aus einem explizit definierten Umfang (d. h. einem Satz von Hardware-, Software- oder Firmware-Komponenten) bestehen, der die Begrenzung aller Komponenten des Krypto-Moduls bildet. Alle Algorithmen, Sicherheitsfunktionen, Prozesse und Komponenten innerhalb der kryptografischen Begrenzung des Moduls **müssen [02.08]** die Anforderungen dieser Internationalen Norm erfüllen. Die kryptografische Begrenzung **muss [02.09]** mindestens alle sicherheitsrelevanten Algorithmen, Sicherheitsfunktionen, Prozesse und Komponenten eines Krypto-Moduls umfassen (d. h. sicherheitsrelevant im Rahmen dieser Internationalen Norm). Nicht sicherheitsrelevante Algorithmen, Sicherheitsfunktionen, Prozesse oder Komponenten dürfen sich innerhalb der kryptografischen Begrenzung befinden. Nicht

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

sicherheitsrelevante Algorithmen, Sicherheitsfunktionen, Prozesse oder Komponenten dürfen auch in einer genehmigten Betriebsart verwendet werden. Nicht sicherheitsrelevante Algorithmen, Sicherheitsfunktionen, Prozesse oder Komponenten, die in einer genehmigten Betriebsart verwendet werden, **müssen [02.10]** so implementiert werden, dass der genehmigte Betrieb des Krypto-Moduls nicht beeinträchtigt oder kompromittiert wird.

Der definierte Name eines Krypto-Moduls **muss [02.11]** repräsentativ für die Zusammenstellung der Komponenten innerhalb der kryptografischen Begrenzung und nicht repräsentativ für eine größere Zusammenstellung oder ein größeres Produkt sein. Das Krypto-Modul **muss [02.12]** mindestens spezifische Versionsinformationen für die einzelnen Hardware-, Software- und/oder Firmware-Komponenten ausweisen.

Hardware-, Software- und/oder Firmware-Komponenten innerhalb der kryptografischen Begrenzung dürfen von den Anforderungen dieser Internationalen Norm ausgenommen werden. Die ausgenommenen Hard-, Software- oder Firmwarekomponenten **müssen [02.13]** so implementiert werden, dass sie den genehmigten sicheren Betrieb des Krypto-Moduls nicht beeinträchtigen oder kompromittieren. Die ausgenommene Hardware, Software oder Firmware **muss [02.14]** angegeben werden (Anhang A).

7.2.3.2 Definitionen der kryptografischen Begrenzung

Die kryptografische Begrenzung eines **Hardware-Krypto-Moduls muss [02.15]** folgende Komponenten eingrenzen und identifizieren:

- den Satz von Hardwarekomponenten, der Folgendes beinhalten darf:
  - physische Bauteile, einschließlich Leiterplatten, Träger oder andere Montageflächen, die die physische Anschlussverdrahtung zwischen den Komponenten bereitstellen;
  - stromführende elektrische Komponenten wie teilintegrierte, kundenspezifisch integrierte oder handelsübliche integrierte Schaltungen, Prozessoren, Speicher, Stromversorgungen, Umrichter usw.;
  - physische Bauteile, wie Gehäuse, Verguss- oder Verkapselungsmassen, Stecker und Schnittstellen;
  - Firmware, die ein Betriebssystem einschließen darf;
  - andere Komponententypen, die oben nicht aufgeführt sind.

Die kryptografische Begrenzung eines **Software-Krypto-Moduls muss [02.16]** folgende Komponenten eingrenzen und identifizieren:

- den Satz von ausführbaren Dateien, die das Krypto-Modul bilden; und
- die Instanziierung des im Speicher hinterlegten und von einem oder mehreren Prozessoren ausgeführten Krypto-Moduls.

Die kryptografische Begrenzung eines **Krypto-Firmwaremoduls muss [02.17]** folgende Komponenten eingrenzen und kennzeichnen:

- den Satz von ausführbaren Dateien, die das Krypto-Modul bilden; und
- die Instanziierung des im Speicher hinterlegten und von einem oder mehreren Prozessoren ausgeführten Krypto-Moduls.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

Die kryptografische Begrenzung eines **Hybrid-Krypto-Moduls muss [02.18]**:

— die Hardwarekomponentenbegrenzung des Moduls und die Begrenzung der separaten Software- oder Firmwarekomponente(n) miteinander verbinden, und

— alle Anschlüsse und Schnittstellen jeder Komponente umfassen.

Neben der (den) separaten Software- oder Firmwarekomponente(n) kann die Hardwarekomponente auch eingebettete Software oder Firmware beinhalten.

7.2.4 Betriebsarten

7.2.4.1 Allgemeine Anforderungen an die Betriebsmodi

Der Bediener **muss [02.19]** das Modul in einer genehmigten Betriebsart betreiben können. Eine genehmigte Betriebsart **muss [02.20]** als der Satz von Diensten definiert sein, der mindestens einen Dienst, der einen genehmigten kryptografischen Algorithmus, eine genehmigte kryptografische Sicherheitsfunktion oder einen genehmigten kryptografischen Prozess nutzt, und die in Abschnitt 7.4.3 genannten Dienste oder Prozesse umfasst.

Nicht genehmigte kryptografische Algorithmen, Sicherheitsfunktionen und Prozesse oder andere Dienste, die nicht in 7.4.3 aufgeführt sind, **dürfen nicht [02.21]** vom Bediener in einer genehmigten Betriebsart genutzt werden, es sei denn, der nicht genehmigte kryptografische Algorithmus oder die nicht genehmigte Sicherheitsfunktion ist Teil eines genehmigten Prozesses und ist nicht sicherheitsrelevant für den Betrieb der genehmigten Prozesse (z. B. ein nicht genehmigter kryptografischer Algorithmus oder ein nicht genehmigter erzeugter Schlüssel darf zur Verschleierung von Daten oder CSP verwendet werden, aber das Ergebnis gilt als ungeschützter Klartext und bietet keine sicherheitsrelevante Funktionalität, bis es durch einen genehmigten kryptografischen Algorithmus geschützt wird).

7.2.4.2 Normalbetrieb

Ein Normalbetrieb liegt vor, wenn der gesamte Satz an Algorithmen, Sicherheitsfunktionen, Diensten oder Prozessen verfügbar und/oder konfigurierbar ist.

CSP **müssen [02.22]** „exklusiv“ zwischen genehmigten und nicht genehmigten Diensten und Betriebsmodi übergeben werden (d. h. nicht als gemeinsame CSP oder, wenn schon auf sie zugegriffen wird). Die Ausgabe eines genehmigten RBG darf an einen nicht genehmigten Algorithmus, eine nicht genehmigte Sicherheitsfunktion oder einen nicht genehmigten Prozess ohne Löschen des RBG-Startwerts erfolgen, solange auf den Startwert nicht in einer nicht genehmigten Betriebsart zugegriffen werden kann.

Die Sicherheitsleitlinie des Moduls **muss [02.23]** den vollständigen Satz von Diensten definieren, die für jede definierte (sowohl genehmigte als auch nicht genehmigte) Betriebsart bereitgestellt werden.

Alle Dienste **müssen [02.24]** anzeigen, wenn sie einen genehmigten kryptografischen Algorithmus, eine genehmigte Sicherheitsfunktion oder einen genehmigten kryptografischen Prozess in einer genehmigten Weise und die in 7.4.3 genannten Dienste oder Prozesse nutzen.

7.2.4.3 Eingeschränkter Betrieb

Ein Krypto-Modul darf für die Unterstützung eingeschränkter Funktionalität ausgelegt sein, wenn das Modul in den Fehlerzustand geht. Für ein Krypto-Modul im eingeschränkten Betrieb **muss [02.25]** Folgendes gelten:

— das Modul **darf [02.26]** nur nach dem Verlassen des Fehlerzustands in den eingeschränkten Betrieb gehen;

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

— das Modul **muss [02.27]** Zustandsinformationen bereitstellen, wenn es neu konfiguriert wird und in den eingeschränkten Betrieb geht;

— der Mechanismus oder die Funktion, die versagt hat, **muss [02.28]** isoliert werden;

— alle Selbsttests mit bedingten Algorithmen **müssen [02.29]** vor der ersten Verwendung des kryptografischen Algorithmus nach Eintritt in den eingeschränkten Betrieb durchgeführt werden; und

— Dienste **müssen [02.30]** Versuche anzeigen, einen nicht betriebsbereiten Algorithmus, eine nicht betriebsbereite Sicherheitsfunktion oder einen nicht betriebsbereiten Prozess zu verwenden.

Das Krypto-Modul **muss [02.31]** im eingeschränkten Betrieb bleiben, bis es alle vorbetrieblichen Selbsttests erfolgreich bestanden hat. Das Krypto-Modul darf als Teil der Bedingung zum Beenden des eingeschränkten Betriebs zusätzlich zu allen vorbetrieblichen Selbsttests bestimmte Diagnosen durchführen. Wenn das Krypto-Modul die vorbetrieblichen Selbsttests nicht besteht, **darf** das Modul **nicht [02.32]** in den eingeschränkten Betrieb gehen.

7.3 Schnittstellen des Krypto-Moduls

7.3.1 Allgemeine Anforderungen an die Schnittstellen des Krypto-Moduls

Ein Krypto-Modul **muss [03.01]** den gesamten logischen Informationsfluss auf diejenigen physischen Zugangspunkte und logischen Schnittstellen beschränken, die als Ein- und Ausgangspunkte der kryptografischen Begrenzung des Moduls gekennzeichnet sind. Die logischen Schnittstellen des Krypto-Moduls **müssen [03.02]** sich eindeutig voneinander unterscheiden, obwohl sie sich möglicherweise einen physischen Anschluss teilen (z. B. dürfen Ein- und Ausgabedaten über denselben Anschluss ein- bzw. ausgelesen werden) oder auf jeweils einen oder mehrere physische Anschlüsse verteilt sein dürfen (z. B. dürfen Eingabedaten sowohl über einen seriellen als auch über einen parallelen Anschluss eingelesen werden). Eine Anwendungsprogramm-Schnittstelle (API) einer Softwarekomponente eines Krypto-Moduls darf als eine oder mehrere logische Schnittstelle(n) definiert werden.

Die in A.2.3 angegebenen Dokumentationsanforderungen **müssen [03.03]** eingehalten werden.

7.3.2 Arten von Schnittstellen

— Hardwaremodul-Schnittstelle (HMI): Der vollständige Satz der Schnittstellen, die zur Anforderung der Dienste des Hardwaremoduls dienen, einschließlich der Parameter, die im Rahmen des angeforderten Dienstes über die kryptografische Begrenzung des Moduls in beliebiger Richtung übergeben werden.

— *Software-* oder *Firmwaremodul-Schnittstelle (SFMI):* Der vollständige Satz der Schnittstellen, die zur Anforderung der Dienste des Software- oder Firmwaremoduls dienen, einschließlich der Parameter, die im Rahmen des angeforderten Dienstes über die kryptografische Begrenzung des Moduls in beliebiger Richtung übergeben werden.

— *Hybrid-Software- oder Hybrid-Firmwaremodul-Schnittstelle (HSMI oder HFMI):* Der vollständige Satz der Schnittstellen, die zur Anforderung der Dienste des Hybridsoftware- oder -Firmwaremoduls dienen, einschließlich der Parameter, die im Rahmen des angeforderten Dienstes über die kryptografische Begrenzung des Moduls in beliebiger Richtung übergeben werden.

7.3.3 Definition der Schnittstellen

Ein Krypto-Modul **muss [03.04]** die folgenden fünf Schnittstellen aufweisen („Eingabe“ und „Ausgabe“ sind aus Sicht des Moduls angegeben):

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

a) *Dateneingabeschnittstelle*: Alle Daten (mit Ausnahme der über die Steuereingabeschnittstelle eingegebenen Steuerdaten), die in ein Krypto-Modul eingegeben und von diesem verarbeitet werden (einschließlich Klartextdaten, Chiffriertextdaten, SSP und Zustandsinformationen aus einem anderen Modul), **müssen [03.05]** über die Schnittstelle „Dateneingabe“ eingelesen werden. Das Modul darf Daten über die Dateneingabeschnittstelle einlesen, während es Selbsttests durchführt (7.10).

b) *Datenausgabeschnittstelle*: Alle Daten (mit Ausnahme der Zustandsdaten, die über die Statusausgabeschnittstelle und der Steuerdaten, die über die Steuerausgabeschnittstelle ausgegeben werden), die von einem Krypto-Modul ausgegeben werden (einschließlich Klartextdaten, Chiffriertextdaten und SSP), **müssen [03.06]** über die Schnittstelle „Datenausgabe“ ausgelesen werden. Alle Datenausgaben über die Schnittstelle „Datenausgabe“ **müssen [03.07]** während manueller Eingaben, der Durchführung vorbetrieblicher Selbsttests, dem Laden von Software/Firmware und der Löschung/Vernichtung oder, wenn das Krypto-Modul in den Fehlerzustand geht, ausgesetzt werden.

c) *Steuereingabeschnittstelle*: Alle Eingabebefehle, -signale (z. B. Takteingabe) und -Steuerdaten (einschließlich Funktionsaufrufe und Daten manueller Bedienelemente, wie Schalter, Tasten und Tastaturen), die zur Steuerung des Betriebs eines Krypto-Moduls verwendet werden, **müssen [03.08]** über die Schnittstelle „Steuereingabe“ eingelesen werden.

d) *Steuerausgabeschnittstelle*: Alle Ausgabebefehle, -signale und -Steuerdaten (z. B. Steuerbefehle an ein anderes Modul), die zum Steuern oder Anzeigen des Betriebszustands eines Krypto-Moduls verwendet werden, **müssen [03.09]** über die Schnittstelle „Steuerausgabe“ ausgelesen werden. Alle Steuerausgaben über die Schnittstelle „Steuerausgabe“ **müssen [03.10]** ausgesetzt werden, wenn das Krypto-Modul in den Fehlerzustand geht, mit Ausnahme der in der Sicherheitsleitlinie angegebenen und dokumentierten Ausnahmen.

e) *Statusausgabeschnittstelle*: Alle Ausgabesignale, -anzeigen (z. B. Fehleranzeige) und -zustandsdaten (einschließlich Rückgabecodes und physischen Anzeigen, wie optischen (Bildschirm, Kontrollleuchten), akustischen (Summer, Hinweiston, Klingeln) und mechanischen (Vibration) Anzeigen), die zur Anzeige des Zustands eines Krypto-Moduls dienen, **müssen [03.11]** über die Schnittstelle „Statusausgabe“ ausgelesen werden. Die Statusausgabe darf entweder implizit oder explizit erfolgen.

Mit Ausnahme der Krypto-Softwaremodule **müssen [03.12]** alle Module auch die folgende Schnittstelle aufweisen:

f) *Stromversorgungsschnittstelle*: Die gesamte externe elektrische Energie zur Versorgung eines Krypto-Moduls **muss [03.13]** über eine Stromversorgungsschnittstelle eingespeist werden. Eine Stromversorgungsschnittstelle ist nicht erforderlich, wenn die gesamte Energie intern innerhalb der kryptografischen Begrenzung des Krypto-Moduls bereitgestellt oder bereitgehalten wird (z. B. durch eine eingebaute Batterie).

Das Krypto-Modul **muss [03.14]** zwischen Daten, Steuerinformationen und Stromversorgung für die Eingabe und Daten, Steuerinformationen, Zustandsinformationen und Stromversorgung für die Ausgabe unterscheiden.

Die Spezifikation des Krypto-Moduls **muss [03.15]** das Format der Eingabedaten und der Steuerinformationen, einschließlich Längenbeschränkungen für alle Eingaben variabler Länge, eindeutig festlegen.

7.3.4 Vertrauenswürdiger Kanal

Ein vertrauenswürdiger Kanal ist eine Verbindung zwischen dem Krypto-Modul und einem Absender oder Empfänger zur sicheren Übermittlung von ungeschützten Klartext-CSP, Schlüsselkomponenten und Authentisierungsdaten. Ein vertrauenswürdiger Kanal schützt vor Abfangversuchen und physischer oder logischer Manipulation durch unerwünschte Bediener/Entitäten, Prozesse oder andere Geräte zwischen den definierten Eingabe- oder Ausgabeanschlüssen des Krypto-Moduls und entlang der Kommunikationsverbindung mit dem beabsichtigten Sender- oder Empfängerendpunkt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

SICHERHEITSSTUFEN 1 UND 2

Für die Sicherheitsstufen 1 und 2 gibt es keine Anforderungen bezüglich eines vertrauenswürdigen Kanals.

SICHERHEITSSTUFE 3

Für Sicherheitsstufe 3

- **muss [03.16]** für die Übertragung von ungeschützten Klartext-CSP, Schlüsselkomponenten und Authentisierungsdaten zwischen dem Krypto-Modul und dem Sender- oder Empfängerendpunkt ein vertrauenswürdiger Kanal im Krypto-Modul implementiert sein,
- **muss [03.17]** der vertrauenswürdige Kanal unbefugtes Modifizieren, Ersetzen und Offenlegen entlang der Kommunikationsverbindung unterbinden,
- **müssen [03.18]** die für den vertrauenswürdigen Kanal verwendeten physischen Anschlüsse physisch von allen anderen Anschlüssen getrennt sein bzw. **müssen [03.19]** die für den vertrauenswürdigen Kanal verwendeten logischen Schnittstellen von allen anderen Schnittstellen logisch getrennt sein,
- **muss [03.20]** identitätsbasierte Authentifizierung für alle Dienste, die den vertrauenswürdigen Kanal nutzen, verwendet werden, und
- **muss [03.21]** eine Statusanzeige anzeigen, wenn der vertrauenswürdige Kanal genutzt wird.

SICHERHEITSSTUFE 4

Zusätzlich zu den Anforderungen der Sicherheitsstufe 3 **muss [03.22]** für Sicherheitsstufe 4 eine identitätsbasierte Multifaktor-Authentifizierung für alle Dienste verwendet werden, die den vertrauenswürdigen Kanal nutzen.

7.4 Rollen, Dienste und Authentifizierung

7.4.1 Allgemeine Anforderungen an Rollen, Dienste und Authentifizierung

Ein Krypto-Modul **muss [04.01]** autorisierte Rollen für Bediener und entsprechende Dienste im Rahmen der jeweiligen Rolle unterstützen. Ein einzelner Bediener darf mehrere Rollen übernehmen. Wenn ein Krypto-Modul gleichzeitig mehrere Bediener unterstützt, **muss [04.02]** das Modul intern die Trennung der von jedem Bediener übernommenen Rollen und der entsprechenden Dienste aufrechterhalten. Ein Bediener ist nicht verpflichtet, eine autorisierte Rolle zu übernehmen, um Dienste auszuführen, die CSP und PSP nicht modifizieren, offenlegen oder ersetzen (z. B. *Statusanzeigen, Selbsttests* oder andere Dienste, die die Sicherheit des Moduls nicht beeinträchtigen).

Innerhalb eines Krypto-Moduls können Authentifizierungsmechanismen erforderlich sein, um einen Bediener zu authentifizieren, der auf das Modul zugreift, und um zu überprüfen, ob der Bediener berechtigt ist, die angeforderte Rolle zu übernehmen und die Dienste im Rahmen der Rolle auszuführen.

Die in A.2.4 angegebenen Dokumentationsanforderungen **müssen [04.03]** eingehalten werden.

7.4.2 Rollen

Ein Krypto-Modul **muss [04.04]** **mindestens** eine Rolle für den *Kryptobeauftragten* unterstützen. Um kryptografische Initialisierungs- oder Verwaltungsfunktionen und allgemeine Sicherheitsdienste (z. B. Modulinitialisierung, Verwaltung von CSP, PSP und Auditfunktionen) ausführen zu können, **muss [04.05]** der Bediener die *Rolle des Kryptobeauftragten* übernehmen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

Ein Krypto-Modul kann eine *Anwenderrolle* unterstützen. Wenn das Krypto-Modul eine *Anwenderrolle* unterstützt, dann **muss [04.06]** der Bediener die *Anwenderrolle* übernehmen, um allgemeine Sicherheitsdienste, einschließlich kryptografischer Operationen und anderer zugelassener Sicherheitsfunktionen, ausführen zu können.

Ein Krypto-Modul kann eine *Wartungsrolle* unterstützen. Die *Wartungsrolle* wird für das Ausführen von physischen und/oder logischen Wartungsdiensten angenommen (z. B. Öffnen von Wartungsabdeckungen, Durchführen bestimmter Diagnosen wie eingebaute Selbsttests (BIST)). Alle ungeschützten SSP **müssen [04.07]** beim Übernehmen oder Abgeben der Wartungsrolle gelöscht/vernichtet werden.

Ein Krypto-Modul darf zusätzlich zu den oben genannten andere Rollen unterstützen.

7.4.3 Dienste

7.4.3.1 Allgemeine Anforderungen an Dienste

Dienste **müssen [04.08]** sich auf alle Dienste, Operationen oder Funktionen beziehen, die von einem Modul ausgeführt werden können. *Diensteingaben* **müssen [04.09]** aus allen Daten- oder Steuereingaben in das Modul bestehen, die bestimmte Dienste, Operationen oder Funktionen initiieren oder anfordern. *Dienstausgaben* **müssen [04.10]** aus allen Datenausgaben, Steuerausgaben und Statusausgaben bestehen, die sich aus Diensten, Operationen oder Funktionen ergeben, die durch Diensteingaben initiiert oder angefordert wurden. Jede Diensteingabe **muss [04.11]** zu einer Dienstausgabe führen.

Ein Krypto-Modul **muss [04.12]** die folgenden Dienste für die Bediener bereitstellen.

a) *Anzeige der Versionierungsinformationen des Moduls:* Das Krypto-Modul **muss [04.13]** den Namen oder die Modulkennung und die Versionierungsinformationen ausgeben, die den Angaben in einem Validierungsprotokoll entsprechen (z. B. Informationen zur Hardware-, Software- und/oder Firmware-Versionierung).

b) *Anzeige des Zustands:* Das Krypto-Modul **muss [04.14]** den aktuellen Zustand ausgeben. Es ist zulässig, die Ausgabe von Statusanzeigen als Reaktion auf eine Dienstanforderung einzuschließen.

c) *Ausführen von Selbsttests:* Das Krypto-Modul **muss [04.15]** die vorbetrieblichen Selbsttests nach 7.10.2 initiieren und durchführen.

d) *Ausführen genehmigter Sicherheitsfunktionen:* Das Krypto-Modul **muss [04.16]** mindestens eine zugelassene Sicherheitsfunktion ausführen, die in einer genehmigten Betriebsart nach 7.2 verwendet wird.

e) *Löschen/Vernichten:* Das Krypto-Modul **muss [04.17]** die Parameter löschen/vernichten wie in 7.9.7 beschrieben.

Ein Krypto-Modul darf zusätzlich zu den oben genannten Diensten weitere, sowohl genehmigte als auch nicht genehmigte Dienste, Operationen oder Funktionen bereitstellen. Spezielle Dienste dürfen in mehr als einer Rolle bereitgestellt werden (z. B. können Schlüsseleingabedienste in der Anwenderrolle und der Rolle des Kryptobeauftragten bereitgestellt werden).

7.4.3.2 Fähigkeit zum Umgehen

Die Fähigkeit zum Umgehen ist die Fähigkeit eines Dienstes, eine kryptografische Funktion oder einen kryptografischen Prozess ganz oder teilweise zu umgehen. Wenn das Modul ein bestimmtes Daten- oder Zustandselement in einer kryptografisch geschützten Form ausgeben kann oder (aufgrund der Modulkonfiguration oder des Eingriffs des Bedieners) das Element auch in einer nicht geschützten Form ausgeben kann, dann **muss [04.18]** eine Fähigkeit zum Umgehen definiert werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

Wenn in ein Krypto-Modul eine Fähigkeit zum *Umgehen* implementiert ist, dann:

a) **muss [04.19]** der Bediener vor der Konfiguration der Fähigkeit zum Umgehen eine autorisierte Rolle übernehmen;

b) **müssen [04.20]** zur Aktivierung der Fähigkeit zwei unabhängige interne Aktionen erforderlich sein, um das versehentliche Umgehen von Klartextdaten aufgrund eines einzelnen Fehlers zu vermeiden. Die beiden unabhängigen internen Aktionen **müssen [04.21]** das Software- und/oder Hardwareverhalten ändern, das für die Fähigkeit zum Umgehen zuständig ist (z. B. zwei verschiedene Soft- oder Hardwaremarkierungen, von denen eine vom Anwender gesetzt werden darf); und dann

c) **muss [04.22]** das Modul den Zustand anzeigen und dadurch angeben, ob die Fähigkeit zum Umgehen:

   1) *nicht* aktiviert *ist* und das Modul ausschließlich Dienste *mit* kryptografischer Verarbeitung bereitstellt (z. B. Klartextdaten *sind* verschlüsselt); oder

   2) aktiviert *ist* und das Modul ausschließlich Dienste *ohne* kryptografische Verarbeitung bereitstellt (z. B. Klartextdaten *sind nicht* verschlüsselt); oder

   3) *abwechselnd* aktiviert und deaktiviert *wird* und das Modul einige Dienste mit kryptografischer Verarbeitung und einige Dienste *ohne* kryptografische Verarbeitung bereitstellt (z. B. sind bei Modulen mit mehreren Kommunikationskanälen Klartextdaten je nach Kanalkonfiguration verschlüsselt oder nicht).

7.4.3.3 Fähigkeit zur selbstinitiierten kryptografischen Ausgabe

Die Fähigkeit zur selbstinitiierten kryptografischen Ausgabe ist die Fähigkeit des Moduls, kryptografische Operationen und andere genehmigte Sicherheitsfunktionen oder SSP-Verwaltungstechniken ohne externe Bedieneranforderung durchzuführen. Die Fähigkeit zur selbstinitiierten kryptografischen Ausgabe **muss [04.23]** vom Kryptobeauftragten konfiguriert werden und diese Konfiguration darf beim Zurücksetzen, Neustarten oder Aus- und Wiedereinschalten des Moduls erhalten bleiben.

Wenn in einem Krypto-Modul eine *Fähigkeit zur selbstinitiierten kryptografischen Ausgabe* implementiert ist, dann:

— **müssen [04.24]** für die Aktivierung der Fähigkeit zwei unabhängige interne Aktionen erforderlich sein, um die versehentliche Ausgabe von Klartextdaten aufgrund eines einzelnen Fehlers zu vermeiden. Die beiden unabhängigen internen Aktionen **müssen [04.25]** das für das Bereitstellen dieser Fähigkeit zuständige Software- und/oder Hardwareverhalten ändern (z. B. zwei verschiedene Soft- oder Hardwaremarkierungen, von denen eine vom Anwender gesetzt werden darf); und dann

— **muss [04.26]** das Modul den Zustand anzeigen und dadurch angeben, ob die Fähigkeit zur selbstinitiierten kryptografischen Ausgabe aktiviert ist.

7.4.3.4 Laden von Software/Firmware

Wenn ein Krypto-Modul die Fähigkeit besitzt, Software oder Firmware von einer externen Quelle zu laden, **müssen [04.27]** die folgenden Anforderungen eingehalten werden:

— die geladene Software oder Firmware **muss [04.28]** vor dem Laden von einer Validierungsinstanz validiert werden, um die Validierung weiterhin sicherzustellen;

— alle Datenausgaben über die Datenausgabeschnittstelle **müssen [04.29]** ausgesetzt werden, bis die Software/Firmware erfolgreich geladen und die Prüfung zum Laden der Software erfolgreich abgeschlossen wurde;

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

— die in 7.10.3.4 beschriebene *Prüfung zum Laden der Software/Firmware* **muss [04.30]** durchgeführt werden, bevor der geladene Code ausgeführt werden kann;

— das Krypto-Modul **muss [04.31]** die Ausführung aller geladenen oder geänderten genehmigten Sicherheitsfunktionen aussetzen, bis die in 7.10.2 genannten vorbetrieblichen Selbsttests erfolgreich durchgeführt wurden; und

— die Versionierungsinformationen des Moduls **müssen [04.32]** geändert werden, um hinzugefügte, aktualisierte oder neu geladene Firmware (7.4.3) auszuweisen.

Wenn durch das Laden neuer Software oder Firmware das Image vollständig ersetzt wird, **muss [04.33]** das Modul als vollkommen neu gelten und zur weiteren Sicherstellung der Validierung durch eine Validierungsinstanz validiert werden. Das neue Image der Software oder Firmware **darf [04.34]** erst dann ausgeführt werden, wenn das Modul durch einen „Power-on Reset“ neu gestartet wurde. Alle SSP **müssen [04.35]** vor dem Ausführen des neuen Image gelöscht/vernichtet werden.

7.4.4 Authentifizierung

Innerhalb eines Krypto-Moduls können Authentifizierungsmechanismen erforderlich sein, um einen Bediener zu authentifizieren, der auf das Modul zugreift, und um zu überprüfen, ob der Bediener berechtigt ist, die angeforderte Rolle zu übernehmen und die Dienste im Rahmen dieser Rolle auszuführen. Die folgenden Arten von Mechanismen werden verwendet, um den Zugriff auf das Krypto-Modul zu kontrollieren:

a) *Rollenbasierte Authentifizierung:* Wenn rollenbasierte Authentifizierungsmechanismen von einem Krypto-Modul unterstützt werden, **muss [04.36]** das Modul verlangen, dass der Bediener eine oder mehrere Rollen entweder implizit oder explizit auswählt und es **muss [04.37]** die Übernahme der ausgewählten Rolle (oder Rollen) authentifizieren. Das Krypto-Modul muss nicht die Identität des jeweiligen Bedieners authentifizieren. Die Auswahl der Rollen und die Authentifizierung der Übernahme ausgewählter Rollen dürfen kombiniert werden. Wenn ein Krypto-Modul dem Bediener erlaubt, Rollen zu wechseln, dann **muss [04.38]** das Modul die Übernahme jeder Rolle authentifizieren, die zuvor nicht für diesen Bediener authentifiziert wurde.

b) *Identitätsbasierte Authentifizierung:* Wenn identitätsbasierte Authentifizierungsmechanismen von einem Krypto-Modul unterstützt werden, **muss [04.39]** das Modul eine individuelle und eindeutige Identifizierung des Bedieners erforderlich machen. Es **muss [04.40]** verlangen, dass der Bediener eine oder mehrere Rollen entweder implizit oder explizit auswählt und es **muss [04.41]** die Identität des Bedieners und die Berechtigung des Bedieners, die ausgewählte Rolle oder Rollen zu übernehmen, authentifizieren. Die Authentifizierung der Identität des Bedieners, die Auswahl der Rollen und die Berechtigung zur Übernahme der ausgewählten Rollen dürfen kombiniert werden. Wenn ein Krypto-Modul dem Bediener erlaubt, Rollen zu wechseln, **muss [04.42]** das Modul die Berechtigung des identifizierten Bedieners, eine Rolle zu übernehmen, für alle Rollen überprüfen, die zuvor nicht autorisiert wurden.

Ein Krypto-Modul darf einem authentifizierten Bediener erlauben, alle im Rahmen einer autorisierten Rolle genehmigten Dienste auszuführen, oder darf eine separate Authentifizierung für jeden Dienst oder für verschiedene Dienste verlangen. Wenn ein Krypto-Modul zurückgesetzt, neu gestartet, ausgeschaltet und anschließend eingeschaltet wird, **muss [04.43]** das Modul die Authentifizierung des Bedieners erforderlich machen.

Verschiedene Arten von Authentisierungsdaten können von einem Krypto-Modul benötigt werden, um die unterstützten Authentifizierungsmechanismen zu implementieren, einschließlich (aber nicht ausschließlich) der Kenntnis oder des Besitzes eines Passworts, einer PIN, eines kryptografischen Schlüssels oder ähnlichem, des Besitzes eines physischen Schlüssels, Token oder ähnlichem oder der Überprüfung persönlicher Merkmale (z. B. biometrischer Merkmale). Authentisierungsdaten innerhalb eines Krypto

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

Moduls **müssen [04.44]** vor unbefugtem Verwenden, Offenlegen, Ändern und Ersetzen geschützt sein. Genehmigte Sicherheitsfunktionen dürfen als Teil des Authentifizierungsmechanismus verwendet werden.

Die Initialisierung von Authentifizierungsmechanismen kann unter Umständen eine besondere Behandlung sicherstellen. Enthält ein Krypto-Modul nicht die Authentisierungsdaten, die für die erstmalige Authentifizierung des Bedieners beim ersten Zugriff auf das Modul erforderlich sind, **müssen [04.45]** andere genehmigte Verfahren (z. B. Verfahrenskontrollen oder die Verwendung von werkseitig eingestellten oder voreingestellten Authentisierungsdaten) verwendet werden, um den Zugriff auf das Modul zu steuern und die Authentifizierungsmechanismen zu initialisieren. Wenn voreingestellte Authentisierungsdaten verwendet werden, um den Zugriff auf das Modul zu kontrollieren, **müssen [04.46]** die voreingestellten Authentisierungsdaten bei der erstmaligen Authentifizierung ersetzt werden. Diese voreingestellten Authentisierungsdaten müssen nicht die Anforderungen bezüglich der Löschung/Vernichtung (7.9.7) erfüllen.

Der Authentifizierungsmechanismus darf aus einer Gruppe von Mechanismen mit unterschiedlichen Authentifizierungseigenschaften bestehen, die gemeinsam die Anforderungen dieses Abschnitts erfüllen. Wenn das Krypto-Modul Sicherheitsfunktionen zur Authentifizierung des Bedieners verwendet, dann **muss [04.47]** es sich um genehmigte Sicherheitsfunktionen handeln.

— Im Modul **muss [04.48]** ein genehmigter Authentifizierungsmechanismus nach Anhang E implementiert sein.

— Die Stärke des genehmigten Authentifizierungsmechanismus **muss [04.49]** in der Sicherheitsleitlinie (Anhang B) festgelegt sein.

— Bei jedem Versuch, den genehmigten Authentifizierungsmechanismus zu verwenden, **muss [04.50]** das Modul die Anforderungen an die Stärke des Ziels der Authentifizierung erfüllen. Bei mehrfachen Versuchen, den genehmigten Authentifizierungsmechanismus innerhalb einer Minute zu verwenden, **muss [04.51]** das Modul die Anforderungen an die Stärke des Ziels der Authentifizierung erfüllen.

— Der genehmigte Authentifizierungsmechanismus **muss [04.52]** durch eine entsprechende Implementierung des Moduls gestützt sein und nicht von dokumentierten Verfahrenskontrollen oder Sicherheitsregeln (z. B. Beschränkungen der Passwortlänge) abhängen.

— Für ein Krypto-Softwaremodul der Sicherheitsstufe 2 darf der Authentifizierungsmechanismus im Betriebssystem implementiert sein. Wenn der Authentifizierungsmechanismus im Betriebssystem implementiert ist, **muss [04.53]** er die Anforderungen dieses Abschnitts erfüllen.

— Die Rückmeldung von Authentisierungsdaten an einen Bediener **muss [04.54]** während des Authentifizierungsprozesses verdeckt werden (z. B. keine sichtbare Anzeige der Zeichen eines Passworts bei der Eingabe). Anstelle der eigentlichen Authentisierungsdaten dürfen Zeichen ohne Bedeutung angezeigt werden.

— Rückmeldungen, die einem Bediener während einer versuchten Authentifizierung gegeben werden, **müssen [04.55]** verhindern, dass der Authentifizierungsmechanismus über die erforderliche Authentifizierungsstärke hinaus geschwächt wird.

SICHERHEITSSTUFE 1

Für Sicherheitsstufe 1 muss ein Krypto-Modul keine Authentifizierungsmechanismen einsetzen, um den Zugriff auf das Modul zu kontrollieren. Wenn ein Modul keine Authentifizierungsmechanismen unterstützt, **muss [04.56]** das Modul vom Bediener verlangen, implizit oder explizit eine oder mehrere Rollen auszuwählen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

SICHERHEITSSTUFE 2

Für Sicherheitsstufe 2 **muss [04.57]** ein Krypto-Modul mindestens eine *rollenbasierte* Authentifizierung einsetzen, um den Zugriff auf das Modul zu kontrollieren.

SICHERHEITSSTUFE 3

Für Sicherheitsstufe 3 **muss [04.58]** ein Krypto-Modul *identitätsbasierte* Authentifizierungsmechanismen einsetzen, um den Zugriff auf das Modul zu kontrollieren.

SICHERHEITSSTUFE 4

Für Sicherheitsstufe 4 **muss [04.59]** ein Krypto-Modul *identitätsbasierte Multi-Faktor*-Authentifizierungsmechanismen einsetzen, um den Zugriff auf das Modul zu kontrollieren.

7.5 Software-/Firmware-Sicherheit

Ein Krypto-Modul ist definiert als Hardware-, Software-, Firmware- oder Hybridmodul (7.2.2). Die Software- und Hardwarekomponenten eines Krypto-Moduls **müssen [05.01]** die Anforderungen dieses Abschnitts erfüllen.

Die Sicherheitsanforderungen dieser Internationalen Norm an die Software- und Firmware gelten nicht für ein Krypto-Modul, das vollständig in der Hardware implementiert ist.

Der für eine genehmigte Integritätstechnik verwendete öffentliche Verifizierungsschlüssel oder Authentifizierungsschlüssel für verschlüsselte Nachrichten darf im Modulcode enthalten sein und gilt nicht als SSP.

Die in A.2.5. angegebenen Dokumentationsanforderungen **müssen [05.02]** eingehalten werden.

SICHERHEITSSTUFE 1

Für Sicherheitsstufe 1 **müssen [05.03]** die folgenden Anforderungen an Software- und Firmwarekomponenten eines Krypto-Moduls eingehalten werden:

— die gesamte Software und Firmware **muss [05.04]** in einer Form vorliegen, die den Anforderungen dieser Internationalen Norm ohne Modifizierung vor der Installation (7.11.7) entspricht;

— für Software- und Firmwaremodule und die Software- oder Firmware-Komponente eines Hybridmoduls (mit Ausnahme der Software- und Firmwarekomponenten innerhalb einer separaten Hardwarekomponente eines Hybridmoduls) gilt Folgendes:

  — Auf alle Software- und Firmwarekomponenten innerhalb der definierten kryptografischen Begrenzung des Moduls **muss [05.05]** ein kryptografischer Mechanismus, der eine genehmigte Integritätstechnik verwendet, auf eine der folgenden Arten angewendet werden:

    — durch das Krypto-Modul selbst; oder

    — durch ein anderes validiertes Krypto-Modul, das in einer genehmigten Betriebsart arbeitet;

— für Software- und Firmware-Komponenten eines Krypto-Hardwaremoduls und die Software- oder Firmware-Komponenten innerhalb einer separaten Hardwarekomponente eines Krypto-Hybridmoduls gilt Folgendes:

  — auf alle Software- und Firmwarekomponenten innerhalb der definierten kryptografischen Begrenzung des Hardwaremoduls oder innerhalb separater Hardwarekomponenten des

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

Hybridmoduls **muss [05.06]** ein kryptografischer Mechanismus, der eine genehmigte Integritätstechnik oder einen Fehlererkennungscode (EDC) verwendet, angewendet werden. Wird ein EDC verwendet, **muss [05.07]** dieser Code mindestens 16 Bit lang sein;

— wenn die Integritätsprüfung fehlschlägt (d. h. die Überprüfung des berechneten Ergebnisses ist nicht erfolgreich oder der EDC kann je nach Modultyp nicht überprüft werden), **muss [05.08]** das Modul in den Fehlerzustand gehen. Die genehmigte Integritätstechnik darf aus einem Gesamt-Mitteilungsauthentisierungscode oder einer Gesamtsignatur oder aus mehreren Teilauthentisierungscodes oder -signaturen bestehen. Bei einer gescheiterten Authentifizierung eines Teilcodes oder einer -signatur **muss [05.09]** das Modul in den Fehlerzustand gehen. Die entsprechende erwartete Ausgabe des Integritätstechnikmechanismus darf als Daten betrachtet werden und unterliegt selbst nicht der Integritätstechnik. Der (die) temporäre(n) Wert(e), der (die) während der Integritätsprüfung der Software oder Firmware des Moduls erzeugt wird (werden), **muss (müssen) [05.10]** nach Beendigung der Integritätsprüfung vom Modul gelöscht/vernichtet werden;

— ein Bediener **muss [05.11]** in der Lage sein, die Integritätsprüfung auf Anforderung über einen HMI-, SFMI-, HSMI- oder HFMI-Dienst durchzuführen (7.3.2);

— alle Daten- und Steuereingaben sowie Daten-, Steuer- und Statusausgaben (beschrieben in 7.3.3) des Krypto-Moduls und der kryptografischen Dienste (7.4.3) **müssen [05.12]** über eine definierte HMI, SFMI, HFMI oder HSMI eingelesen bzw. ausgelesen werden; und

— wenn bei einem Software- oder Firmwaremodul das geladene Software- oder Firmware-Image das validierte Modul-Image vollständig ersetzt oder überlagert, ist die Prüfung zum Laden der Software-/Firmware nicht anwendbar (NA), da durch das Ersetzen oder Überlagern das Modul als neues Modul gilt.

Wenn die geladene Software oder Firmware dem validierten Modul zugewiesen oder daran gebunden ist oder ein ausführbarer Bestandteil des validierten Moduls ist oder einen solchen modifiziert, dann ist die Prüfung zum Laden von Software-/Firmware anwendbar und **muss [05.13]** vom validierten Modul durchgeführt werden. Es gelten folgende Ausnahmen:

— das Krypto-Modul ist ein Softwaremodul und das geladene Software-Image ersetzt oder überlagert vollständig das Image des validierten Moduls;

— das Krypto-Modul ist ein Firmwaremodul der physischen Sicherheitsstufe 1 und das geladene Firmware-Image ersetzt oder überlagert vollständig das Image des validierten Moduls;

— das Krypto-Modul ist ein Hybrid-Softwaremodul und das geladene Softwareimage ersetzt oder überlagert vollständig das Image der separaten Softwarekomponenten;

— das Krypto-Modul ist ein Hybrid-Firmwaremodul der physischen Sicherheitsstufe 1 und das geladene Firmware-Image ersetzt oder überlagert vollständig das Image der separaten Firmwarekomponenten.

SICHERHEITSSTUFE 2

Zusätzlich zu den Anforderungen der Sicherheitsstufe 1 **müssen [05.14]** die Software- und Firmwarekomponenten eines Krypto-Moduls für Sicherheitsstufe 2 die folgenden Anforderungen erfüllen:

— Die Software- und Firmwarekomponenten eines Krypto-Moduls **müssen [05.15]** ausschließlich Code in ausführbarer Form enthalten (z. B. keinen Quellcode, Objektcode oder just-in-time kompilierten Code).

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

— Es **darf [05.16]** keine Dienste oder Steuereinstellungen über die HMI-, SFMI-, HFMI- oder HSMI-Schnittstelle geben, die es dem Bediener ermöglichen, Debugging-Techniken zu initiieren oder durchzuführen.

— Für Software- und Firmwaremodule und die Software- oder Firmwarekomponente eines Hybridmoduls (mit Ausnahme der Software- und Firmwarekomponenten innerhalb einer separaten Hardwarekomponente eines Hybridmoduls) gilt für Sicherheitsstufe 2 Folgendes:

  — Auf die gesamte Software und Firmware innerhalb der definierten kryptografischen Begrenzung des Moduls **muss [05.17]** eine genehmigte digitale Signatur oder ein verschlüsselter Mitteilungsauthentisierungscode angewendet werden. Wenn die Überprüfung des berechneten Ergebnisses nicht erfolgreich war, schlägt die Prüfung fehl und das Modul **muss [05.18]** in den Fehlerzustand gehen.

SICHERHEITSSTUFEN 3 UND 4

Zusätzlich zu den Anforderungen der Sicherheitsstufen 1 und 2 **müssen [05.19]** die Software- und Firmwaremodule und die Software- oder Firmwarekomponente eines Hybridmoduls die folgenden Anforderungen für die Sicherheitsstufen 3 und 4 erfüllen (mit Ausnahme der Software- und Firmwarekomponenten innerhalb einer separaten Hardwarekomponente eines Hybridmoduls):

Auf alle Software- und Firmwarekomponenten innerhalb der definierten kryptografischen Begrenzung des Moduls **muss [05.20]** ein kryptografischer Mechanismus, der eine genehmigte digitale Signatur verwendet, angewendet werden. Wenn die Überprüfung des berechneten Ergebnisses nicht erfolgreich war, schlägt die Prüfung fehl und das Modul **muss [05.21]** in den Fehlerzustand gehen.

Die Technik der digitalen Signatur darf aus einer digitalen Gesamtsignatur oder aus mehreren Teilsignaturen bestehen. Bei einer gescheiterten Authentifizierung einer Teilsignatur **muss [05.22]** das Modul in den Fehlerzustand gehen. Der private Signierschlüssel **muss [05.23]** sich außerhalb des Moduls befinden.

7.6 Betriebsumgebung

7.6.1 Allgemeine Anforderungen an die Betriebsumgebung

Die Betriebsumgebung eines Krypto-Moduls bezieht sich auf die Verwaltung der für den Betrieb des Moduls erforderlichen Software, Firmware und/oder Hardware. Die Betriebsumgebung eines Software-, Firmware- oder Hybridmoduls umfasst mindestens die Modulkomponenten, die Rechnerplattform und das Betriebssystem, das die Ausführung der Software oder Firmware auf der Rechnerplattform steuert oder ermöglicht. Ein Hardwaremodul darf eine Betriebsumgebung innerhalb des Moduls haben, die aus einem Betriebssystem besteht, das die Ausführung interner Software oder Firmware ermöglicht. Das Betriebssystem gilt als ein System, das ggf. die virtuelle(n) Maschine(n) (System und/oder Prozess) und die Laufzeitumgebung (z. B. Java Runtime Environment – JRE) umfasst.

Als *Universalbetriebsumgebung* wird der Einsatz eines handelsüblichen Universalbetriebssystems (d. h. eines Ressourcenmanagers) bezeichnet, das die Software- und Firmwarekomponenten sowie System- und Bedienerprozesse/-Threads einschließlich Universalanwendungssoftware verwaltet, wie z. B. Textverarbeitungsprogramme.

Die Betriebsumgebung kann *nicht modifizierbar*, *begrenzt* oder *modifizierbar* sein.

Der folgende Abschnitt beschreibt die drei jeweiligen Betriebsumgebungen.

a) Eine ***nicht modifizierbare Betriebsumgebung*** ist so ausgelegt oder konfiguriert, dass eine Änderung der Modulkomponenten, der Rechnerplattform oder des Betriebssystems durch einen Bediener oder Prozess unterbunden wird. Diese Umgebung darf aus einem Firmwaremodul bestehen, das auf einer

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

nicht programmierbaren Rechnerplattform läuft oder aus einem Hardwaremodul, das das Laden zusätzlicher Software oder Firmware unterbindet.

b) Eine ***begrenzte Betriebsumgebung*** ist so ausgelegt oder konfiguriert, dass eine kontrollierte Modifizierung der Modulkomponenten, der Rechnerplattform oder des Betriebssystems durch einen Bediener oder Prozess möglich ist. Bei dieser Umgebung darf es sich um Firmware handeln, die in einem programmierbaren Hardwaremodul ausgeführt wird und in der das Laden zusätzlicher Firmware die in 7.4.3.4 angegebenen Anforderungen an das Laden von Firmware erfüllt.

c) Als ***modifizierbare Betriebsumgebung*** wird eine Betriebsumgebung bezeichnet, die neu konfiguriert werden darf, um Funktionalität hinzuzufügen/zu löschen/zu modifizieren, und/oder Fähigkeiten eines Universalbetriebssystems enthalten darf (z. B. Verwendung eines Computer-Betriebssystems, eines konfigurierbaren Smartcard-Betriebssystems oder programmierbarer Software). Betriebssysteme werden als modifizierbare Betriebsumgebungen angesehen, wenn Softwarekomponenten durch einen Bediener oder Prozess modifiziert werden können und/oder ein Bediener oder Prozess Software (z. B. eine Textverarbeitung) laden und ausführen kann, die nicht Teil des definierten Software-, Firmware- oder Hybridmoduls ist.

   Eine modifizierbare Betriebsumgebung weist folgende Merkmale auf:

   Funktionen dürfen innerhalb der Betriebsumgebung hinzugefügt oder modifiziert werden. Bei diesen Funktionen wird nicht notwendigerweise davon ausgegangen, dass sie den Betrieb des Krypto-Moduls nicht beeinträchtigen, es sei denn, derartige Beeinträchtigungen werden durch die Betriebsumgebung unterbunden.

   In einer solchen Umgebung darf keine Funktion, die in der Betriebsumgebung arbeitet und nicht zum vertrauenswürdigen Teil dieser Betriebsumgebung gehört, auf SSP zugreifen können, außer über die definierten Schnittstellen des Krypto-Moduls.

   Daher ist es erforderlich, dass die Betriebsumgebung die Möglichkeit bietet, das Krypto-Modul während des Betriebs von anderen Funktionen in der Betriebsumgebung zu trennen, so dass diese Funktionen weder Informationen vom Krypto-Modul in Bezug auf die CSP erhalten noch in der Lage sind, CSP, PSP oder den Ausführungsablauf des Krypto-Moduls anders als über die vom Krypto-Modul selbst bereitgestellten Schnittstellen zu ändern.

   Eine spezielle Konfiguration der Betriebsumgebung kann unter Umständen erforderlich sein, um einen angemessenen Schutz für das Krypto-Modul, seinen Code und seine Daten zu erreichen (z. B. durch Unterbinden einer bestimmten Art der Interprozesskommunikation für das Krypto-Modul, durch Zuweisen eingeschränkter Zugriffsrechte auf Dateien, die SSP oder den Code des Krypto-Moduls enthalten).

Einige Beispiele für Betriebsumgebungen sind in der folgenden Tabelle aufgeführt.

Tabelle 2 — Beispiele für Betriebsumgebungen

Konfigurationsbeispiele	Betriebsumgebung
eine Rechnerplattform, die das Laden von Code nicht zulässt und es den Bedienern nicht erlaubt, die Konfiguration der Rechnerplattform, des Betriebssystems oder des Krypto-Moduls zu ändern	nicht modifizierbar
eine Rechnerplattform mit einem Betriebssystem, das das Laden von zusätzlichem Code erlaubt, wenn er authentifiziert ist und alle anwendbaren Anforderungen dieser Internationalen Norm erfüllt	begrenzt
eine Rechnerplattform, die das Laden von Code erlaubt, ohne dass die Anforderungen dieser Internationalen Norm an das Laden von Software oder	modifizierbar

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

Konfigurationsbeispiele	Betriebsumgebung
Firmware erfüllt sind	
eine Rechnerplattform, die einen Code enthält, dessen Betriebssystem vom Bediener neu konfiguriert werden kann, so dass Sicherheitsmaßnahmen aufgehoben werden können	modifizierbar

Bei einer *nicht modifizierbaren* oder *begrenzten* Umgebung dürfen die Steuerkomponenten, die die *nicht modifizierbare* oder *begrenzte* Umgebung aufrechterhalten, Attribute der Rechnerplattform, des Betriebssystems oder des Krypto-Moduls selbst *oder* alle oben genannten umfassen.

Code, der in einer *nicht modifizierbaren* oder *begrenzten* Umgebung ausgeführt wird, wird in dieser Internationalen Norm als *Firmware* bezeichnet. Code, der in einer *modifizierbaren* Umgebung ausgeführt wird, wird in dieser Internationalen Norm als *Software* bezeichnet.

Ist die Betriebsumgebung *nicht modifizierbar* oder *begrenzt*, **müssen [06.01]** lediglich die in 7.6.2 angegebenen Anforderungen an das Betriebssystem eingehalten werden.

Ist die Betriebsumgebung *modifizierbar*, **müssen [06.02]** die in 7.6.3 angegebenen Anforderungen an das Betriebssystem eingehalten werden.

Die in A.2.6 genannten Dokumentationsanforderungen **müssen [06.03]** eingehalten werden.

7.6.2 Anforderungen an das Betriebssystem in begrenzten oder nicht modifizierbaren Betriebsumgebungen

SICHERHEITSSTUFE 1

Die Anforderungen in 7.6.3 für Sicherheitsstufe 1 **müssen [06.04]** eingehalten werden, wenn das Modul der Sicherheitsstufe 1 nach 7.7 entspricht.

SICHERHEITSSTUFEN 2, 3 UND 4

Es gibt keine zusätzlichen Anforderungen.

7.6.3 Anforderungen an das Betriebssystem in modifizierbaren Betriebsumgebungen

SICHERHEITSSTUFE 1

Die folgenden Anforderungen gelten für Betriebssysteme der Sicherheitsstufe 1:

— Jede Instanz eines Krypto-Moduls **muss [06.05]** die Kontrolle über ihre eigenen SSP haben.

— Die Betriebsumgebung **muss [06.06]** über die Fähigkeit verfügen, einzelne Anwendungsprozesse voneinander zu trennen, um einen unkontrollierten Zugriff auf CSP und unkontrollierte Änderungen von SSP zu verhindern, unabhängig davon, ob sich diese Daten im Prozessspeicher oder auf einem dauerhaften Speicher innerhalb der Betriebsumgebung befinden. Dadurch wird sichergestellt, dass der direkte Zugriff auf CSP und SSP auf das Krypto-Modul und die vertrauenswürdigen Teile der Betriebsumgebung beschränkt ist. Einschränkungen der Konfiguration der Betriebsumgebung **müssen [06.07]** in der Sicherheitsleitlinie des Krypto-Moduls dokumentiert werden.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

— Die vom Krypto-Modul erzeugten Prozesse **müssen [06.08]** zum Modul gehören und nicht zu externen Prozessen/Bedienern.

ANMERKUNG Diese Anforderungen können nicht durch administrative Dokumentation und Verfahren, sondern müssen durch das Krypto-Modul selbst durchgesetzt werden.

SICHERHEITSSTUFE 2

Zusätzlich zu den Anforderungen aus Sicherheitsstufe 1 **muss [06.09]** eine Betriebsumgebung für Sicherheitsstufe 2 folgende Anforderungen oder die von der Validierungsbehörde genehmigten Anforderungen erfüllen:

— die gesamte kryptografische Software, SSP sowie Kontroll- und Zustandsinformationen **müssen [06.10]** unter der Kontrolle eines Betriebssystems stehen, in das entweder rollenbasierte Zugriffskontrollen oder zumindest eine anwenderbestimmte Zugriffskontrolle mit widerstandsfähigen Mechanismen zur Definition neuer Gruppen und zur Zuweisung eingeschränkter Berechtigungen, z. B. durch Zugriffskontrolllisten (ACL), implementiert sind/ist und das über die Fähigkeit verfügt, jeden Anwender mehr als einer Gruppe zuzuweisen. Das Betriebssystem **muss [06.11]** so konfiguriert sein, dass es vor unbefugtem Ausführen, Modifizieren und Auslesen von SSP, Steuer- und Zustandsdaten schützt;

— um Klartextdaten, kryptografische Software, SSP und Authentisierungsdaten zu schützen, gilt Folgendes für die Zugriffskontrollmechanismen des Betriebssystems:

  — sie **müssen [06.12]** so konfiguriert werden, dass die Rollen oder Gruppen, die über exklusive Rechte zur Ausführung der gespeicherten kryptografischen Software verfügen, sowie die zu diesen Rollen und Gruppen gehörenden einschränkenden Rechte definiert sind und durchgesetzt werden;

  — sie **müssen [06.13]** so konfiguriert werden, dass die Rollen oder Gruppen, die über exklusive Rechte zur Änderung (d. h. Schreiben, Ersetzen und Löschen) der folgenden kryptografischen Modulsoftware verfügen, die innerhalb der kryptografischen Begrenzung gespeichert ist: kryptografische Programme, kryptografische Daten (z B. kryptografische Audit-Daten), SSP und Klartextdaten, sowie die zu diesen Rollen und Gruppen gehörenden einschränkenden Rechte definiert sind und durchgesetzt werden;

  — sie **müssen [06.14]** so konfiguriert werden, dass die Rollen oder Gruppen, die über exklusive Rechte zum Lesen von kryptografischen Daten (z. B. kryptografische Audit-Daten), CSP und Klartextdaten verfügen, sowie die zu diesen Rollen und Gruppen gehörenden einschränkenden Rechte definiert sind und durchgesetzt werden; und

  — sie **müssen [06.15]** so konfiguriert werden, dass die Rollen oder Gruppen, die über exklusive Rechte zur Eingabe von SSP verfügen, sowie die zu diesen Rollen und Gruppen gehörenden einschränkenden Rechte definiert sind und durchgesetzt werden;

  und

— die folgenden Angaben **müssen [06.16]** mit den in der Sicherheitsleitlinie festgelegten Rollen oder den Rechten und Diensten der benannten Gruppen übereinstimmen:

  — wenn das Betriebssystem keine Wartungsrolle unterstützt, **muss [06.17]** es verhindern, dass Bediener oder laufende Prozesse laufende kryptografische Prozesse (d. h. geladene und ausgeführte kryptografische Programm-Images) modifizieren. In diesem Fall beziehen sich laufende Prozesse auf alle Prozesse, sowohl kryptografische als auch andere, die nicht zum Betriebssystem gehören oder von ihm (d. h. vom Bediener) initiiert werden;

  — das Betriebssystem **muss [06.18]** verhindern, dass Anwenderprozesse Lese- oder Schreibzugriff auf SSP, die zu anderen Prozessen gehören, und auf System-SSP erhalten; und

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03

— die Konfiguration des Betriebssystems, das die oben angegebenen Anforderungen erfüllt, **muss [06.19]** in den Administratorleitlinien beschrieben werden. In den Administratorleitlinien **muss [06.20]** darauf hingewiesen werden, dass das Betriebssystem wie angegeben zu konfigurieren ist, damit der Modulinhalt als geschützt gilt.

Der Mechanismus zur Identifizierung und Authentisierung gegenüber dem Betriebssystem **muss [06.21]** die Anforderungen aus 7.4.3 einhalten und in der Sicherheitsleitlinie des Moduls beschrieben sein.

Die gesamte kryptografische Software, SSP, Steuer- und Zustandsinformationen **müssen [06.22]** unter der Kontrolle eines Betriebssystems stehen,

— das mindestens die folgenden Attribute aufweisen **muss [06.23]**:

— Das Betriebssystem **muss [06.24]** einen Audit-Mechanismus mit Datum- und Zeitstempel für jedes auditierte Ereignis bereitstellen. Das Krypto-Modul **darf [06.25]** keine SSP in ein Auditprotokoll einschließen.

— Das Krypto-Modul **muss [06.26]** die folgenden Ereignisse zur Aufzeichnung durch den Audit-Mechanismus des Betriebssystems bereitstellen:

— Modifizieren, Zugreifen auf, Löschen und Hinzufügen von kryptografischen Daten und SSP;

— Versuche, ungültige Eingaben für die Funktionen des Kryptobeauftragten zu machen;

— Hinzufügen eines Bedieners für die Rolle des Kryptobeauftragten oder Löschen eines Bedieners für diese Rolle (wenn diese Rollen durch das Krypto-Modul verwaltet werden);

— Verwenden einer sicherheitsrelevanten Funktion des Kryptobeauftragten;

— Zugriffsanfragen für Authentisierungsdaten, die dem Krypto-Modul zugeordnet sind;

— Verwendung eines Authentisierungsmechanismus (z. B. einloggen), der dem Krypto-Modul zugeordnet ist; und

— explizite Anfragen, die Rolle des Kryptobeauftragten zu übernehmen.

— Der Audit-Mechanismus des Betriebssystems **muss [06.27]** in der Lage sein, die folgenden betriebssystembezogenen Ereignisse zu auditieren:

— alle Lese- oder Schreibzugriffe des Bedieners auf die in der Zugriffsprotokollierung gespeicherten Audit-Daten;

— Zugriff auf Dateien, die vom Krypto-Modul zur Speicherung kryptografischer Daten oder SSP verwendet werden;

— Hinzufügen eines Bedieners für die Rolle des Kryptobeauftragten oder Löschen eines Bedieners für diese Rolle (wenn diese Rollen durch die Betriebsumgebung verwaltet werden);

— Anforderungen bezüglich der Verwendung von Mechanismen zur Verwaltung von Authentisierungsdaten;

— Versuche, die Funktion des vertrauenswürdigen Kanals zu verwenden, und ggf. die Bewilligungen dieser Anforderungen, wenn der vertrauenswürdige Kanal auf dieser Sicherheitsstufe unterstützt wird; und

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19790:2020-03

— Identifizierung des Initiators und des Ziels eines vertrauenswürdigen Kanals, wenn der vertrauenswürdige Kanal auf dieser Sicherheitsstufe unterstützt wird.

— Das Betriebssystem **muss [06.28]** so konfiguriert sein, dass die Modifizierung des Krypto-Moduls und der in der Betriebsumgebung des Krypto-Moduls gespeicherten Audit-Daten durch Bediener, die nicht über die entsprechenden in der Sicherheitsleitlinie festgelegten Berechtigungen verfügen, unterbunden wird.

Nur Betriebssysteme, die so konfiguriert sind, dass die oben angegebenen Sicherheitsanforderungen eingehalten werden, **sind [06.29]** auf dieser Sicherheitsstufe zulässig, unabhängig davon, ob das Krypto-Modul in einer genehmigten Betriebsart betrieben wird oder nicht. Das Zugriffsprotokoll sollte durch eine genehmigte Sicherheitsfunktion vor unbefugten Modifizierungen geschützt werden.

7.7 Physische Sicherheit

7.7.1 Ausführungen der physischen Sicherheit

Ein Krypto-Modul **muss [07.01]** physische Sicherheitsmechanismen aufweisen, um den unbefugten physischen Zugriff auf den Inhalt des Moduls zu beschränken und um die unbefugte Verwendung oder Änderung des Moduls (einschließlich Austausch des gesamten Moduls) im eingebauten Zustand zu unterbinden. Die gesamte Hardware, Software, Firmware sowie alle Datenkomponenten und SSP innerhalb der kryptografischen Begrenzung **müssen [07.02]** geschützt werden.

Ein Krypto-Modul, das vollständig software-implementiert ist, so dass die physische Sicherheit ausschließlich durch die Rechnerplattform gewährleistet wird, unterliegt nicht den physischen Sicherheitsanforderungen dieser Internationalen Norm.

Die Anforderungen dieses Abschnitts **müssen [07.03]** für Hardware- und Firmwaremodule sowie Hardware- und Firmwarekomponenten von Hybridmodulen eingehalten werden.

Die Anforderungen dieses Abschnitts **müssen [07.04]** an der definierten physischen Grenze des Moduls anwendbar sein.

Physische Sicherheitsanforderungen werden für drei definierte physische Ausführungsformen eines Krypto-Moduls beschrieben:

a) ***Einzelchip-Krypto-Module*** sind physische Ausführungen, bei denen ein einzelner integrierter Schaltkreis (IC) als eigenständiges Gerät verwendet oder in ein Gehäuse oder ein Produkt eingebettet sein darf, das möglicherweise nicht über einen physischen Schutz verfügt. Beispiele für Einzelchip-Krypto-Module sind einzelne Chips mit integriertem Einzelschaltkreis oder einzelne Chipkarten mit integriertem Einzelschaltkreis.

b) ***Eingebettete Multichip-Krypto-Module*** sind physische Ausführungen, bei denen zwei oder mehr integrierte Schaltkreise miteinander verbunden und in ein Gehäuse oder ein Produkt eingebettet sind, das möglicherweise nicht über einen physischen Schutz verfügt. Beispiele für eingebettete Multichip-Krypto-Module sind Adapter und Erweiterungskarten (en: expansion boards).

c) ***Eigenständige Multichip-Krypto-Module*** sind physische Ausführungen, bei denen zwei oder mehr integrierte Schaltkreise miteinander verbunden sind und das gesamte Gehäuse physisch geschützt ist. Beispiele für eigenständige Multichip-Krypto-Module sind Router mit verschlüsselter Übertragung, sichere Funkanlagen oder USB-Token.

Abhängig von den physischen Sicherheitsmechanismen eines Krypto-Moduls **müssen [07.05]** Versuche unbefugten physischen Zugriffs, unbefugter Nutzung oder Modifizierung mit einer hohen Wahrscheinlichkeit erkannt werden:

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 19790:2020-03