

DIN EN ISO/IEC 19790

ICS 35.030

**Informationstechnik –
Sicherheitstechniken –
Sicherheitsanforderungen für kryptografische Module
(ISO/IEC 19790:2012, korrigierte Fassung 2015-12);
Deutsche Fassung EN ISO/IEC 19790:2020**

Information technology –
Security techniques –
Security requirements for cryptographic modules (ISO/IEC 19790:2012, Corrected
version 2015-12);
German version EN ISO/IEC 19790:2020

Technologies de l'information –
Techniques de sécurité –
Exigences de sécurité pour les modules cryptographiques (ISO/IEC 19790:2012, Version
corrigée 2015-12);
Version allemande EN ISO/IEC 19790:2020

Gesamtumfang 89 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

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 EN ISO/IEC 19790:2020 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).

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

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

Nationaler Anhang NA (informativ)

Literaturhinweise

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

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

Deutsche Fassung

Informationstechnik —
Sicherheitstechniken —
Sicherheitsanforderungen für kryptografische Module
(ISO/IEC 19790:2012, korrigierte Fassung 2015-12)

Information technology —
Security techniques —
Security requirements for cryptographic modules
(ISO/IEC 19790:2012, Corrected version 2015-12)

Technologies de l'information —
Techniques de sécurité —
Exigences de sécurité pour les modules cryptographiques
(ISO/IEC 19790:2012, Version corrigée 2015-12)

Diese Europäische Norm wurde vom CEN am 2. März 2020 angenommen.

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

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

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



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

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	26
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	35
7.3.4 Vertrauenswürdiger Kanal	36
7.4 Rollen, Dienste und Authentifizierung	36
7.4.1 Allgemeine Anforderungen an Rollen, Dienste und Authentifizierung.....	36
7.4.2 Rollen.....	37
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

7.9.1	Allgemeine Anforderungen an die Verwaltung von sensiblen Sicherheitsparametern.....	57
7.9.2	Zufallsbitgeneratoren.....	58
7.9.3	Erzeugung sensibler Sicherheitsparameter.....	58
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.....	60
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.....	65
7.11.1	Allgemeine Anforderungen an die Lebenszyklussicherung.....	65
7.11.2	Konfigurationsmanagement.....	65
7.11.3	Auslegung.....	66
7.11.4	Endlicher Automat.....	66
7.11.5	Entwicklung.....	67
7.11.6	Prüfungen des Anbieters.....	68
7.11.7	Lieferung und Betrieb.....	69
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.....	72
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) Sicherheitsrichtlinie 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

C.1.1	Blockziffern.....	82
C.1.2	Stromchiffren.....	82
C.1.3	Asymmetrische Algorithmen und Techniken	82
C.1.4	Mitteilungsauthentisierungs-codes	82
C.1.5	Hash-Funktionen	83
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

Europäisches 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 EN ISO/IEC 19790:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis September 2020, und etwaige entgegenstehende nationale Normen müssen bis September 2020 zurückgezogen werden.

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

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

Anerkennungsnotiz

Der Text von ISO/IEC 19790:2012 wurde von CEN als EN ISO/IEC 19790:2020 ohne irgendeine Abänderung genehmigt.

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: <https://www.iso.org/foreword-supplementary-information.html>.

Die Technische Berichtigung 1 zu ISO/IEC 19790:2012 wurde vom gemeinsamen 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;

- 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.

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 nicht-invasive Sicherheit, die Verwaltung von sensiblen Sicherheitsparametern, Selbsttests, die Lebenszyklussicherung 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 Sicherheitsrichtlinien und -verfahren in der Betriebsumgebung.

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 *Information technology — Security techniques — Security requirements for cryptographic modules*, Anhänge C, D, E und F aufgelisteten Dokumente.

3 Begriffe

Für die Anwendung dieser Internationalen Norm 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.

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

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 Kryptografiertechnik
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

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 eines Krypto-Moduls auszuführen

3.20

kryptografischer Algorithmus

klar definierte Computerprozedur, die anhand von variablen Eingaben, wozu auch kryptografische Schlüssel gehören dürfen, 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

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

Sicherheitsrichtlinie für kryptografische Module

Sicherheitsrichtlinie

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

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

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

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 darf

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 darf

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 Sicherheitsrichtlinie

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

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)

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

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.

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

(asymmetrischer) kryptografischer Algorithmus mit öffentlichem Schlüssel

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

RBG, en: random bit generator

Gerät oder Algorithmus, das/der eine anscheinend statistisch unabhängige und von systematischen Fehlern freie Bitfolge ausgibt

3.101

entfernbarer Abdeckung

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

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-authentisierungs-codes, 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

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)

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 Löschrare 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

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 Kryptografiertechnik

Kryptografiertechnik, bei der sowohl für die Verschlüsselungs- als auch für die Entschlüsselungstransformation 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

Manipulationsnachweis

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

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)
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 dieses 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 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.