

DIN EN 1300

ICS 13.310

Ersatz für
DIN EN 1300:2014-05

**Wertbehälter –
Klassifizierung von Hochsicherheitsschlössern nach ihrem
Widerstandswert gegen unbefugtes Öffnen;
Deutsche Fassung EN 1300:2018**

Secure storage units –

Classification for high security locks according to their resistance to unauthorized opening;
German version EN 1300:2018

Unités de stockage en lieu sûr –

Classification des serrures haute sécurité en fonction de leur résistance à l'effraction;
Version allemande EN 1300:2018

Gesamtumfang 59 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Sie beinhaltet die Deutsche Fassung der vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ im Europäischen Komitee für Normung (CEN) ausgearbeiteten EN 1300:2018.

Die nationalen Interessen bei der Erarbeitung wurden vom Ausschuss NA 060-06-20-01 AA „Geldschränke und Tresoranlagen“ des DIN-Normenausschusses Maschinenbau (NAM) wahrgenommen. Vertreter der Hersteller und Anwender von Geldschränken und Tresoranlagen waren an der Erarbeitung beteiligt.

Die im Abschnitt 2 und den Literaturhinweisen zitierten Europäischen Normen sind als DIN-EN- bzw. DIN-EN-ISO-Normen mit gleicher Zählnummer veröffentlicht.

Für die zitierten Internationalen Normen, sofern sie nicht als DIN-ISO-Normen mit gleicher Zählnummer veröffentlicht sind, gibt es keine nationalen Entsprechungen.

Änderungen

Gegenüber DIN EN 1300:2014-05 wurden folgende Änderungen vorgenommen:

a) Allgemeine Änderungen:

- 1) Aktualisierung der Verweisungen in Abschnitt 2;
- 2) Hinzufügung von Definitionen in Abschnitt 3 (Schließeinheit, HSS im ungesicherten Zustand; Firmware, Anwendungssoftware und vertrauenswürdiges Gerät). Weitere Definitionen wurden aktualisiert;
- 3) Klarstellungen in 5.1.2.4, 5.1.5.1, 5.1.5.3, 5.1.6.7, 5.1.8.2.3, 5.2.6.3, Abschnitt 6, 8.2.5.8, 8.2.6.1, Abschnitt 10 und Abbildung 1 sowie Anhang D.

b) Technische Änderungen an jeder Art von Schloss:

- 1) Anforderungen für HSS mit mehr als einer Codierart wurden in 5.2.1 hinzugefügt;
- 2) Der Schocktest ist geändert worden (siehe 8.2.6.2);
- 3) Änderung von der Immersionsprüfung, diese wird nun mit Salzwasser durchgeführt. Zusätzlich wird diese Prüfung nun mit der Eingabeeinheit im Wasser und während einer zweiten Prüfung mit der Eingabeeinheit außerhalb des Wassers durchgeführt (siehe 8.2.6.3);
- 4) Aktualisierung der Dauerprüfung (siehe 8.3.1.1);
- 5) Aktualisierung der Manipulationsprüfung. Ein dritter Basiswert wurde hinzugefügt (siehe 8.2.2.5) und bei elektronischen Schlössern ist die Prüfung der Einflüsse bei Stromversorgung nun gefordert (5.1.6.8 und 8.2.5);
- 6) Der Prüfbericht muss nun den Namen und die Version dieser Norm enthalten (9.2);
- 7) Aktualisierung der Herstellererklärung in Anhang C.

c) Technische Änderung bei mechanischen Schlüsselschlössern:

- 1) Die Anforderungen an die Produktion von mechanischen Schlüsselschlössern wurde erhöht (siehe 5.1.4.1);

d) Technische Änderungen bei elektronischen Schlössern:

- 1) Für elektronische HSS wurden neue Anforderungen, z.B. in 5.1.6.1, 5.1.6.2, 5.1.6.3, 5.1.6.8, 5.2.5.4, 5.2.6.1, 5.2.6.3, Tabelle 2, 8.2.5.5, 8.2.5.6, 8.2.6.4, 8.2.6.5 und Anhang A hinzugefügt. Dies beinhaltet eine neue EMV-Prüfung mit höheren Frequenzen;
- 2) Anforderungen für HSS mit Einmalcodes wurden in 5.1.6.9 und Anhang A hinzugefügt;
- 3) Die Anforderungen von Schlössern der Klasse A vom Typ „elektronischer Codeträger“ und „verteiltes System“ wurden auf die Anforderungen der Klasse B erhöht worden (siehe 5.1.7.4, 5.1.8.1.6, 5.1.8.1.8, 5.1.8.1.9.1 und 5.1.8.2.2);
- 4) Anforderungen wurden beim Sichtschutz von verteilten Systemen mit abgesetzten Eingabeeinheiten hinzugefügt;
- 5) Anforderungen an die Firmware und an Firmware-Updates wurden in 5.1.9, Tabelle 1 und in Anhang F („Herstellererklärung der Firmware“) hinzugefügt;
- 6) Konstruktive Anforderungen für eine bestimmte Art von elektronischen Schlössern wurden im neuen Anhang E hinzugefügt („Herstellererklärung der Firmware“).

Frühere Ausgaben

DIN V ENV 1300: 1999-04

DIN EN 1300: 2004-09, 2011-10, 2014-05

— Leerseite —

Deutsche Fassung

Wertbehältnisse —
Klassifizierung von Hochsicherheitsschlössern nach
ihrem Widerstandswert gegen unbefugtes Öffnen

Secure storage units —
Classification for high security locks according to
their resistance to unauthorized opening

Unités de stockage en lieu sûr —
Classification des serrures haute sécurité en fonction
de leur résistance à l'effraction

Diese Europäische Norm wurde vom CEN am 3. September 2018 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-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-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

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



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

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

Inhalt

	Seite
Europäisches Vorwort	4
Einleitung	6
1 Anwendungsbereich.....	7
2 Normative Verweisungen	7
3 Begriffe	8
4 Klassifizierung.....	13
5 Anforderungen	14
5.1 Allgemeine Anforderungen.....	14
5.1.1 Allgemeine Anforderungen.....	14
5.1.2 Anforderungen an alle Klassen	14
5.1.3 HSS der Klasse D.....	14
5.1.4 Mechanische Schlüsselschlösser.....	14
5.1.5 Codierungsstufen für mechanische Schlüsselschlösser	15
5.1.6 Elektronische HSS.....	15
5.1.7 Elektronische Codeträger.....	16
5.1.8 Anforderungen an die Kryptografie in verteilten Sicherheitssystemen	17
5.1.9 Firmware-Updates	19
5.2 Sicherheitsanforderungen	19
5.2.1 Nutzbare Codes.....	19
5.2.2 Hochsicherheitsschlösser mit Parallelschloss.....	19
5.2.3 Widerstand gegen Manipulation.....	20
5.2.4 Widerstand gegen zerstörende Angriffe	20
5.2.5 Widerstand gegen Ausspähen.....	20
5.2.6 Widerstand gegen elektrische und elektromagnetische Einflüsse	20
5.2.7 Widerstand gegen physikalische Umwelteinflüsse	21
5.2.8 Temperaturwiderstand.....	21
5.3 Anforderungen an die Zuverlässigkeit	23
6 Technische Dokumentation.....	24
7 Prüfmuster	24
8 Prüfverfahren	25
8.1 Allgemeines	25
8.1.1 Allgemeines	25
8.1.2 Bewertung durch Begutachtung	25
8.2 Sicherheitsprüfungen	26
8.2.1 Nutzbare Codes.....	26
8.2.2 Widerstand gegen Manipulation.....	27
8.2.3 Widerstand gegen zerstörende Angriffe	30
8.2.4 Widerstand gegen Ausspähen.....	30
8.2.5 Widerstand gegen elektrische und elektromagnetische Einflüsse	32
8.2.6 Widerstand gegen physikalische Umwelteinflüsse	33
8.2.7 Temperaturwiderstand.....	34
8.3 Prüfung der Zuverlässigkeit	35

8.3.1	Dauerprüfung	35
8.3.2	Codeumstellung	35
8.3.3	Codeeingabe mit definierter Dynamik bei mechanischen Kombinations-HSS.....	36
9	Prüfbericht.....	36
10	Kennzeichnung.....	37
Anhang A (normativ) Montageanleitung und Betriebshinweise		38
A.1	Montagehinweise	38
A.2	Betriebshinweise.....	39
Anhang B (normativ) Bestimmung des Widerstandes gegen Manipulation aufgrund von konstruktiven Anforderungen		40
B.1	Allgemeines	40
B.2	Schlüsselschlösser.....	40
B.2.1	Allgemeines	40
B.2.2	Spiel zwischen Tourstift und Tourkanal.....	40
B.2.3	Tourstift.....	43
B.2.4	Täuschungsverzahnungen/falsche Touren	43
B.2.5	Weitere konstruktive Anforderungen.....	44
B.3	Mechanische Kombinationsschlösser.....	44
B.3.1	Allgemeines	44
B.3.2	Einfallfinger	45
B.3.3	Prüfung der Dauerfestigkeit.....	46
Anhang C (normativ) Herstellererklärung		47
Anhang D (informativ) Typische Maße einer Sperreinheit.....		49
Anhang E (normativ) Bestimmung des Einbruchwiderstandes aufgrund von konstruktiven Anforderungen		50
E.1	Allgemeines	50
E.2	Elektronische HSS mit externer Auswerteeinheit nicht innerhalb der Sperreinheit	50
E.2.1	Anwendungsbereich der konstruktiven Anforderungen	50
E.2.2	Konstruktive Anforderungen.....	50
Anhang F (normativ) Herstellererklärung der Firmware.....		51
Anhang G (informativ) A-Abweichungen.....		52
Literaturhinweise.....		55

Europäisches Vorwort

Dieses Dokument (EN 1300:2018) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat von BSI gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juni 2019, und etwaige entgegenstehende nationale Normen müssen bis Juni 2019 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.

Dieses Dokument ersetzt EN 1300:2013.

Im Vergleich zur EN 1300:2013 wurden die folgenden Änderungen vorgenommen:

Allgemeine Änderungen:

- Aktualisierung der Verweisungen in Abschnitt 2;
- Hinzufügung von Definitionen in Abschnitt 3 (Schließeinheit, HSS im ungesicherten Zustand; Firmware, Anwendungssoftware und vertrauenswürdiges Gerät). Weitere Definitionen wurden aktualisiert;
- Klarstellungen in 5.1.2.4, 5.1.5.1, 5.1.5.3, 5.1.6.7, 5.1.8.2.3, 5.2.6.3, Abschnitt 6, 8.2.5.8, 8.2.6.1, Abschnitt 10 und Abbildung 1 sowie Anhang D.

Technische Änderungen an jeder Art von Schloss:

- Anforderungen für HSS mit mehr als einer Codierart wurden in 5.2.1 hinzugefügt;
- Der Shocktest ist geändert worden (siehe 8.2.6.2);
- Änderung von der Immersionsprüfung, diese wird nun mit Salzwasser durchgeführt. Zusätzlich wird diese Prüfung nun mit der Eingabeeinheit im Wasser und während einer zweiten Prüfung mit der Eingabeeinheit außerhalb des Wassers durchgeführt (siehe 8.2.6.3);
- Aktualisierung der Dauerprüfung (siehe 8.3.1.1);
- Aktualisierung der Manipulationsprüfung. Ein dritter Basiswert wurde hinzugefügt (siehe 8.2.2.5) und bei elektronischen Schlössern ist die Prüfung der Einflüsse bei Stromversorgung nun gefordert (5.1.6.8 und 8.2.5);
- Der Prüfbericht muss nun den Namen und die Version dieser Norm enthalten (9.2);
- Aktualisierung der Herstellererklärung in Anhang C.

Technische Änderungen bei mechanischen Schlüsselschlössern:

- Die Anforderungen an die Produktion von mechanischen Schlüsselschlössern wurden erhöht (siehe 5.1.4.1)

Technische Änderungen bei elektronischen Schlössern:

- Für elektronische HSS wurden neue Anforderungen, z. B. in 5.1.6.1, 5.1.6.2, 5.1.6.3, 5.1.6.8, 5.2.5.4, 5.2.6.1, 5.2.6.3, Tabelle 2, 8.2.5.5, 8.2.5.6, 8.2.6.4 und Anhang A hinzugefügt. Dies beinhaltet eine neue EMV-Prüfung mit höheren Frequenzen;
- Anforderungen für HSS mit Einmalcodes wurden in 5.1.6.9 und Anhang A hinzugefügt;
- Die Anforderungen von Schlössern der Klasse A vom Typ „elektronischer Codeträger“ und „verteiltes System“ wurden auf die Anforderungen der Klasse B erhöht worden (siehe 5.1.7.4, 5.1.8.1.6, 5.1.8.1.8, 5.1.8.1.9.1 und 5.1.8.2.2);
- Anforderungen wurden beim Sichtschutz von verteilten Systemen mit abgesetzten Eingabeeinheiten hinzugefügt;
- Anforderungen an die Firmware und an Firmware-Updates wurden in 5.1.9, Tabelle 1 und in Anhang F („Herstellererklärung der Firmware“) hinzugefügt;
- Konstruktive Anforderungen für eine bestimmte Art von elektronischen Schlössern wurden im neuen Anhang E hinzugefügt („Herstellererklärung der Firmware“).

Das Dokument spiegelt die Marktanforderungen wider, Anforderungen für verteilte Systeme und elektronische Codeträger aufzunehmen und geht auf die Anforderungen ein, die zum Zeitpunkt der Niederschrift dem Stand der Technik entsprechen.

Diese Europäische Norm wurde von der Arbeitsgruppe 3 des CEN/TC 263 im Rahmen einer Normenreihe zur sicheren Aufbewahrung von Wertsachen und von Datenträgern erarbeitet. Weitere Normen dieser Reihe sind unter anderen:

- EN 1047-1, *Wertbehältnisse — Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand — Teil 1: Datensicherungsschränke*
- EN 1047-2, *Wertbehältnisse — Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand — Teil 2: Datensicherungsräume und Datensicherungscontainer*
- EN 1143-1, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Teil 1: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume*
- EN 1143-2, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Teil 2: Deposit-Systeme*
- EN 14450, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstands gegen Einbruchdiebstahl — Sicherheitsschränke*

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, 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.

Einleitung

Dieses Dokument legt auch die Anforderungen für Hochsicherheitsschlösser (HSS) fest, die über große Distanzen angesteuert werden können. Was die verteilten Systeme betrifft, so geht diese Norm auf die Anforderungen ein, die zum Zeitpunkt der Niederschrift dem Stand der Technik entsprechen. Da sich sowohl die Forschung im Bereich der Kryptographie und relevanter Angriffe als auch in Bezug genommene Normen sehr schnell entwickeln, ist eine Überarbeitung dieser Norm alle drei Jahre verpflichtend.

1 Anwendungsbereich

Dieses Dokument legt die Anforderungen an Hochsicherheitsschlösser (HSS) hinsichtlich ihrer Zuverlässigkeit, ihres Widerstandswertes gegen zerstörende Angriffe und gegen unbefugtes Öffnen sowie die Prüfverfahren fest. Sie bietet außerdem ein Schema zur Klassifizierung von Hochsicherheitsschlössern auf der Grundlage einer Bewertung ihres Widerstandswertes gegen zerstörende Angriffe und gegen unbefugtes Öffnen.

Sie gilt für mechanische und elektronische HSS. Die Schlösser können die folgenden Merkmale als Option enthalten, diese sind aber nicht zwingend erforderlich:

- a) Berechtigungscode zur Verhinderung einer Codeänderung und/oder der Freigabe/Sperrung eines Parallelcodes;
- b) Berechtigungscode zur Freigabe einer Zeitschlossfunktion;
- c) Einbau von Bauteilen oder Funktionen einer Alarmanlage;
- d) Funktionen zur Fernsteuerung und -überwachung;
- e) Widerstand gegen Angriffe mit Säuren;
- f) Widerstand gegen Angriffe mit Röntgenstrahlung;
- g) Widerstand gegen Angriffe mit Sprengstoffen;
- h) Zeitfunktionen.

2 Normative Verweisungen

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

EN 1143-1, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Teil 1: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume*

EN 1143-2, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Teil 2: Deposit-Systeme*

EN 60068-2-1, *Umgebungseinflüsse — Teil 2-1: Prüfverfahren — Prüfung A: Kälte (IEC 60068-2-1)*

EN 60068-2-2, *Umgebungseinflüsse — Teil 2-2: Prüfverfahren — Prüfung B: Trockene Wärme (IEC 60068-2-2)*

EN 60068-2-6, *Umgebungseinflüsse — Teil 2-6: Prüfverfahren — Prüfung Fc: Schwingen (sinusförmig) (IEC 60068-2-6)*

EN 61000-4-2, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-2: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen die Entladung statischer Elektrizität (IEC 61000-4-2)*

EN 61000-4-3, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-3: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen hochfrequente elektromagnetische Felder (IEC 61000-4-3)*

EN 61000-4-5, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-5: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen Stoßspannungen (IEC 61000-4-5)*

EN ISO 6988, *Metallische und andere anorganische Überzüge — Schwefeldioxid-Prüfung mit allgemeiner Feuchtigkeitskondensation (ISO 6988)*

ISO/IEC 9798-1:2010, *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 9798-2, *Information technology — Security techniques — Entity authentication — Part 2: Mechanisms using symmetric encipherment algorithms*

ISO/IEC 9798-4, *Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function*

NIST SP 800-57, *Recommendation for Key Management — Part 1: General*

NIST SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*

FIPS PUB 140-2:2002, *Security Requirements for Cryptographic Modules*

FIPS 197, *Advanced Encryption Standard (AES)*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

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

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Hochsicherheitsschloss

HSS

unabhängige Einheit, die gewöhnlich an Türen von Wertbehältnissen angebracht ist

Anmerkung 1 zum Begriff: In ein HSS kann die Eingabe von Codes erfolgen, die dann mit gespeicherten Codes verglichen werden (Auswerteeinheit). Bei Übereinstimmung der Codes kann eine Blockiereinheit bewegt werden.

3.2

Code

erforderliche Identifikationsinformation, die, wenn sie die richtige ist, es bei Eingabe in ein HSS ermöglicht, den Sicherheitszustand des Schlosses zu ändern

3.2.1

Öffnungscodes

Identifikationsinformation, die ein Entsperren des HSS gestattet

3.2.2

Berechtigungscodes

Identifikationsinformation, die einen Zugang zur Auswerteeinheit gestattet und auch ein Öffnungscodes sein kann

Anmerkung 1 zum Begriff: Mastercodes, Managercodes, Autorisierungscodes und Servicecodes können Berechtigungscodes sein.

3.2.3

Überfallcode

Parallelcode, der zusätzliche Funktionen aktiviert

3.2.4

Parallelcode

Öffnungscode, der identische Funktionen wie ein bereits existierender Öffnungscode aufweist, aber aus anderen Zeichen besteht

3.3

Codierarten

Mittel/Verfahren, durch die der Code gespeichert wird

3.3.1

materieller Code

Code, der durch physikalische Merkmale oder andere Eigenschaften des Codeträgers bestimmt wird

3.3.2

mnemonischer Code

Code, der aus numerischen und/oder alphabetischen Informationen besteht und im Gedächtnis festgehalten wird

3.3.3

biometrischer Code

Code, der aus charakteristischen Merkmalen des Menschen besteht

3.3.4

Einmalcode

Code, welcher sich nach jeder Verwendung verändert und mit Hilfe eines Algorithmus erzeugt wird

3.4

Eingabeeinheit

Teil eines HSS, über das Codes in die Auswerteeinheit eingegeben werden

3.5

Auswerteeinheit

Teil eines HSS, das auswertet, ob der eingegebene Code richtig ist und die Bewegung einer Sperreinheit freigibt oder sie verhindert

3.6

Sperreinheit

mechanische Einheit innerhalb des Wertbehältnisses als Teil eines HSS, welche die Blockiereinheit, das Schlossgehäuse, dessen Abdeckplatte und weitere mechanische und/oder elektronische Komponenten enthält

Anmerkung 1 zum Begriff: In Anhang D wird eine Sperreinheit beispielhaft dargestellt.

3.7

Codeträger

Gegenstand, dessen physische Form oder physikalische Eigenschaften den Berechtigungscode bestimmen

BEISPIEL Ein Schlüssel.

Anmerkung 1 zum Begriff: Ein elektronischer Codeträger beinhaltet einen integrierten Schaltkreis mit flüchtigem und nichtflüchtigem Speicher, damit verbundene Firmware/Software und in vielen Fällen einen Mikrocontroller, der über Kontakt- oder kontaktlose Mittel mit einer Eingabeeinheit kommuniziert.

3.8

mechanisches HSS

HSS, das nur durch mechanische Elemente gesichert wird

3.9

elektronisches HSS

HSS, das teilweise oder vollständig durch elektrische oder elektronische Elemente gesichert wird

3.10

Blockiereinheit

Teil eines HSS, das sich nach Eingabe des richtigen Öffnungscodes bewegt oder bewegt werden kann, normalerweise ist dies ein Riegel

Anmerkung 1 zum Begriff: Eine Blockiereinheit sichert entweder eine Tür oder verhindert die Bewegung eines Riegelwerks. Ein Beispiel für eine Blockiereinheit ist der Riegel eines Schlosses.

3.11

Schließseinheit

Teil eines HSS, welches das Bewegen der Blockiereinheit ermöglicht

BEISPIELE Zuhaltungen, Spindeln, Kombinationsscheiben, Motoren, Elektromagneten.

3.12

zerstörender Angriff

Angriff, der an einem HSS Schäden verursacht, die irreversibel sind und vor dem rechtmäßigen Benutzer nicht verborgen werden können

3.13

Zuverlässigkeit

Fähigkeit, nach einer großen Anzahl von Schließzyklen noch richtig zu funktionieren und die Sicherheitsanforderungen dieser Norm zu erfüllen

3.14

Manipulation

Angriffsverfahren, das darauf abzielt, die Blockierfunktion aufzuheben, ohne dabei Schäden zu verursachen, die für den Nutzer offensichtlich sind

Anmerkung 1 zum Begriff: Nach einer Manipulation kann ein HSS funktionsfähig bleiben, obwohl sein Sicherheitswert dauerhaft beeinträchtigt sein könnte.

3.15

ausspähen

Versuch unbefugt an Information zu gelangen

3.16

nutzbare Codes

Codes oder Codeträger, die vom Hersteller zugelassen sind und die den Anforderungen dieser Norm entsprechen

Anmerkung 1 zum Begriff: Bei mechanischen HSS ist im Allgemeinen die Anzahl der nutzbaren Codes weit geringer als die Gesamtzahl der Codes, auf die das HSS eingestellt werden kann.

3.17

Verworfen-Zustand

Zustand, bei dem sich die Codierungselemente nicht in der Anordnung befinden, die erforderlich ist, um das HSS ohne Eingabe des richtigen Codes oder passenden Codeträger zu entsperren

3.18**Schließsequenz**

Handlungsablauf, der mit einer offenen Tür beginnt und der beendet ist, wenn die Tür geschlossen, verriegelt, gesperrt und gesichert ist

3.19**offene Tür**

Tür, die nicht in ihrem Rahmen liegt

3.20**geschlossene Tür**

Tür, die in ihrem Rahmen liegt und bereit ist, ihre Riegel auszufahren

3.21**verriegelte Tür**

geschlossene Tür, bei der die Riegel vom Riegelwerk ausgefahren sind, das HSS allerdings noch offen ist

3.22**gesperrte Tür**

verriegelte Tür, bei der das Riegelwerk nicht eingefahren werden kann, weil es von der HSS-Sperreinheit blockiert wird

3.23**gesicherte Tür**

Tür, die geschlossen, verriegelt und mit einem HSS, das sich im gesicherten HSS-Zustand befindet, gesperrt ist

3.24**HSS im gesicherten Zustand**

Blockiereinheit ist ausgefahren und kann nur nach Eingabe des/der Öffnungscodes wieder eingefahren werden

3.25**HSS im ungesicherten Zustand**

HSS, welches nicht im gesicherten HSS-Zustand ist

3.26**Normalzustand**

das HSS-Prüfmuster befindet sich im gesicherten HSS-Zustand und alle Schlossfunktionen sind funktionsfähig

3.27**funktionsfähiger Zustand**

das HSS-Prüfmuster befindet sich im gesicherten HSS-Zustand und kann mit dem (den) Öffnungscod(e)s entsperrt werden, es sind aber nicht alle Schlossfunktionen ausführbar

3.28**Sicherheit bei Ausfall**

das HSS-Prüfmuster befindet sich im gesicherten HSS-Zustand, aber nicht alle Schlossfunktionen sind funktionsfähig, es kann deshalb mit dem (den) Öffnungscod(e)s nicht entsperrt werden

3.29**Widerstandseinheit****RU**

(en: resistance unit)

Widerstandswert gegen Diebstahl und Manipulation

Anmerkung 1 zum Begriff: Er zeigt ein berechnetes Ergebnis bei Einsatz eines Werkzeugs mit einem bestimmten Wert über eine Zeitspanne.

3.30

Sperrzeit

Zeitverzögerung aufgrund der Überschreitung der zulässigen Zahl der Öffnungsversuche

3.31

Authentifizierung

Verfahren zur Verhinderung von Missbrauch durch Maßnahmen zur Sicherstellung, dass eine Kommunikation mit den Komponenten eines verteilten Systems nur nach ordnungsgemäßer Bestätigung der Identität der Komponenten aufgebaut werden kann

3.32

kryptografischer Algorithmus

mathematisches Verfahren zur Datentransformation, die die Definition von Parametern einschließt.

BEISPIEL Schlüssellänge und Anzahl von Wiederholungen oder Runden.

3.32.1

asymmetrischer kryptografischer Algorithmus

kryptografischer Algorithmus, der zwei miteinander in Beziehung stehende Schlüssel verwendet, nämlich einen öffentlichen und einen privaten Schlüssel, welche die Eigenschaft haben, dass die Ableitung des privaten Schlüssels vom öffentlichen Schlüssel rechnerisch unmöglich ist

3.32.2

symmetrischer kryptografischer Algorithmus

kryptografischer Algorithmus, der einen einzelnen Geheimschlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet

3.33

kryptografischer Schlüssel

Parameter, der in Verbindung mit einem kryptografischen Algorithmus verwendet wird, der zur Steuerung eines kryptografischen Prozesses wie Verschlüsselung, Entschlüsselung oder Authentifizierung verwendet wird

Anmerkung 1 zum Begriff: Die Kenntnis eines geeigneten Schlüssels ermöglicht korrekte Ver- und/oder Entschlüsselung oder Bestätigung einer Botschaft.

3.34

kryptografisches Modul

Satz von Hardware und Firmware/Software, der Sicherheitsfunktionen für verteilte Systeme und elektronische Codeträger einschließlich kryptografischer Algorithmen wahrnimmt

3.35

verteiltes System

System mit Komponenten, die über ein verdrahtetes oder drahtloses Übertragungssystem verbunden sind

Anmerkung 1 zum Begriff: Es wird angenommen, dass die übertragenen Informationen Dritten zugänglich sind. Ein Hochsicherheitsschloss mit Komponenten an unterschiedlichen Orten wird als verteiltes System definiert. Ein Schließsystem mit zwei Eingabeeinheiten, eines am Wertbehältnis und das andere räumlich getrennt (= abgesetzte Eingabeeinheit), ist ein Beispiel für ein verteiltes System. Ein elektronisches Schloss mit einem unzugänglichen Übertragungssystem im Sinne von 5.1.6.3 dieser Norm oder mit einer temporären Drahtverbindung zu einem vertrauenswürdigen Gerät (z. B. vertrauenswürdiger Personal Computer), die von einer autorisierten Person überwacht wird, wird nicht als verteiltes System angesehen.

3.36**Verschlüsselung**

Vorgang, der die Inhalte einer Nachricht oder einer Datei für jeden nicht autorisierten Leser unverständlich macht

Anmerkung 1 zum Begriff: Während des Verschlüsselungsvorgangs wird ein kryptografischer Algorithmus angewandt, der den kryptografischen Schlüssel verwendet, um den Klartext in einen chiffrierten Text zu verwandeln. Dieser Vorgang besteht aus

- dem Betriebsmodus (en: mode of operation), der die Art der Datenverarbeitung durch den Algorithmus beschreibt,
- dem Füllschema (en: padding scheme), das den Weg des Auffüllens von Datenstrings zu einer definierten Länge beschreibt.

3.37**Übertragungssystem**

Kommunikationssystem zwischen den Elementen eines verteilten Systems

Anmerkung 1 zum Begriff: Speziell zugewiesene Datenverbindungen oder drahtgebundene bzw. drahtlose öffentliche Netzwerke dürfen für den Übertragungsweg verwendet werden.

3.38**sicherheitsrelevante Information**

Codes nach 3.2, Authentifizierungen, alle Code- oder Schlüsselübertragungen und -änderungen sowie Firmware-Updates an Eingabeeinheiten und Auswerteeinheiten

3.39**automatischer Schlüsselaustausch**

kryptografisches Protokoll, welches es zwei einander möglicherweise unbekannten Komponenten ermöglicht, gemeinsam einen geheimen Schlüssel über einen unsicheren Verbindungskanal einzurichten

3.40**Verfügbarkeit**

Zeitanteil, in dem sich ein System in einem funktionsfähigen Zustand befindet

3.41**Firmware**

Softwarecode, welcher die zugeordnete Hardware nach 5.1.8.2.3 oder die Auswerte- oder Eingabeeinheit des HSS betreibt

3.42**Anwendungssoftware**

Software, welche auf jedem Gerät (wie z. B. auf einem PC) betrieben werden kann, die zusätzliche Funktionalitäten besitzt, allerdings keine sicherheitsrelevanten Informationen enthält bzw. speichert

3.43**vertrauenswürdige Gerät**

mit einem Kabel verbundenes Gerät, auf dem unautorisierte Personen keinen Zugang zu sicherheitsrelevanten Informationen bekommen

4 Klassifizierung

Aufgrund der Sicherheitsanforderungen erfolgt bei HSS die Klassifizierung in die HSS-Klassen (A, B, C oder D) nach den Tabellen 1, 2 und 3. Allgemeine Anforderungen, Sicherheits- und Zuverlässigkeitsanforderungen (siehe 5.1, 5.2 und 5.3) müssen erfüllt sein.

ANMERKUNG Für HSS der Klasse A gelten die niedrigsten Anforderungen und für HSS der Klasse D die höchsten Anforderungen.

5 Anforderungen

5.1 Allgemeine Anforderungen

5.1.1 Allgemeine Anforderungen

Alle Anforderungen sind nach 8.1.2 zu prüfen.

5.1.2 Anforderungen an alle Klassen

5.1.2.1 HSS dürfen nur mit gültigen Öffnungscodes geöffnet werden. Der (die) Öffnungscod(e)s müssen so lange als allein gültige Codes erhalten bleiben, bis sie absichtlich umgestellt werden. Übergelagerte oder undokumentierte Codes sind nicht zulässig.

5.1.2.2 Werden bei HSS mnemonische Codes benutzt, müssen diese geändert werden können.

5.1.2.3 Es darf nicht möglich sein, dass durch zusätzliche vom HSS-Hersteller eingebaute Vorrichtungen (z. B. Mikroschalter) Informationen über den Code gewonnen werden können.

5.1.2.4 Eine Eingabeeinheit ist ein notwendiger Teil eines mnemonischen und elektronischen HSS, wobei jedoch mit einer Eingabeeinheit auch mehr als eine Auswerteeinheit bedient werden darf.

Jedes HSS muss eine Auswerteeinheit besitzen, die den richtigen Code bestätigt. Jedes HSS muss auch eine Blockiereinheit enthalten oder die Bewegung einer Blockiereinheit steuern können. Wenn diese Einheit vor der ersten Nutzung aktiviert werden muss, ist in der Bedienungsanleitung des Schlosses darauf hinzuweisen.

5.1.2.5 Wird die Blockiereinheit nicht manuell betätigt, muss eine Vorrichtung vorhanden sein, die anzeigt, ob das HSS gesichert, verriegelt und verworfen ist.

5.1.2.6 Es darf nicht möglich sein, einen Öffnungscod(e) zu ändern, ohne einen Berechtigungscod(e) einzugeben.

5.1.3 HSS der Klasse D

5.1.3.1 Ein Mittel ist vorzusehen, so dass der Verschlusszustand, ob gesperrt oder entsperrt, offensichtlich ist.

5.1.3.2 Ein mechanisches HSS-Kombinationsschloss muss sich nach dem Sperren im Verworfen-Zustand befinden.

5.1.3.3 Ein HSS der Klasse D muss eine Vorrichtung enthalten, die den Verworfen-Zustand anzeigt.

5.1.4 Mechanische Schlüsselschlösser

5.1.4.1 Für jedes mechanische Schlüsselschloss (siehe Abschnitt 4) darf der gleiche Code eines Schlüsselsatzes erst dann wiederholt werden, wenn 100 % der nutzbaren Codes schon verwendet wurden. Für Hersteller mit mehr als einer Produktionsstätte muss diese Anforderung für jede Produktionsstätte erfüllt sein. Eine Synchronisation zwischen den Produktionsstätten ist nicht erforderlich. Allerdings ist es nicht erlaubt, dass mehrere Produktionsstätten bei einem identischen Code zeitgleich anfangen zu produzieren.

5.1.4.2 Codes (und gleichschließende Codeträger) müssen nach einem Zufallsverfahren ausgewählt werden.

5.1.4.3 Weder auf dem Codeträger noch auf dem HSS darf sich eine Nummer oder eine Kennzeichnung befinden, mit der sich der Code feststellen lässt. Es darf außerdem keine Legitimationskarte ausgegeben werden.