

DIN EN 1300

ICS 13.310

Ersatz für
DIN EN 1300:2011-10

**Wertbehältnisse –
Klassifizierung von Hochsicherheitsschlössern nach ihrem
Widerstandswert gegen unbefugtes Öffnen;
Deutsche Fassung EN 1300:2013**

Secure storage units –

Classification for high security locks according to their resistance to unauthorized opening;
German version EN 1300:2013

Unités de stockage en lieu sûr –

Classification des serrures haute sécurité en fonction de leur résistance à l'effraction;
Version allemande EN 1300:2013

Gesamtumfang 52 Seiten

Normenausschuss Eisen-, Blech- und Metallwaren (NAEBM) im DIN

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist 2014-05-01.

Nationales Vorwort

Dieses Dokument (EN 1300:2013) wurde von der Arbeitsgruppe 3 „Sicherheitsschlösser“ (Sekretariat: SNV, Schweiz) des Technischen Komitees 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ (Sekretariat: BSI, Vereinigtes Königreich) des Europäischen Komitees für Normung (CEN) erarbeitet.

Das zuständige nationale Gremium ist der NA 020-00-15 AA „Hochsicherheitsschlösser“ im Normenausschuss Eisen-, Blech- und Metallwaren (NAEBM) im DIN, Deutsches Institut für Normung e. V.

Die im Abschnitt 2 zitierten Europäischen Normen sind als DIN-EN- bzw. DIN-EN-ISO-Normen mit gleicher Normnummer veröffentlicht.

Änderungen

Gegenüber DIN EN 1300:2011-10 wurden folgende Änderungen vorgenommen:

- a) die Anforderungen für Hochsicherheitsschlösser, die über große Distanzen angesteuert werden können, wurden neu aufgenommen, dementsprechend erfolgte eine Erweiterung der Begriffe in Abschnitt 3, die Aufnahme der neuen Unterabschnitte 5.1.6 „Elektronische Datenträger“ und 5.1.7 „Anforderungen an die Kryptografie in verteilten Sicherheitssystemen“ und eine Aktualisierung der Literaturhinweise;
- b) im Anhang A wurden Betriebshinweise aufgenommen;
- c) redaktionelle Überarbeitung.

Frühere Ausgaben

DIN V ENV 1300: 1999-04

DIN EN 1300: 2004-09, 2011-10

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 lieux sûrs —
Classification des serrures haute sécurité en fonction de
leur résistance à l'effraction

Diese Europäische Norm wurde vom CEN am 14. Mai 2013 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 Management-Zentrum des CEN-CENELEC 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, 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: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Vorwort	3
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	7
4 Klassifizierung	12
5 Anforderungen	12
6 Technische Dokumentation	21
7 Prüfmuster	22
8 Prüfverfahren	23
9 Prüfbericht	34
10 Kennzeichnung	34
Anhang A (normativ) Montageanleitung und Betriebshinweise	35
Anhang B (normativ) Bestimmung des Widerstandes gegen Manipulation aufgrund von konstruktiven Anforderungen	37
Anhang C (normativ) Herstellererklärung (nur für Schlüsselschlösser)	44
Anhang D (informativ) Schlossmaße	46
Anhang E (informativ) A-Abweichungen	47
Literaturhinweise	50

Vorwort

Dieses Dokument (EN 1300:2013) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat vom BSI gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Mai 2014, und etwaige entgegenstehende nationale Normen müssen bis Mai 2014 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können, ohne dass diese vorstehend identifiziert wurden. CEN [und/oder] CENELEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt EN 1300:2004+A1:2011.

Im Vergleich zu EN 1300:2004+A1:2011 wurden die folgenden Änderungen vorgenommen:

- Aufnahme von Begriffen (Abschnitt 3) und Anforderungen (Unterabschnitt 5.1.6) an kontaktlose Codeträger,
- Aufnahme von Begriffen (Abschnitt 3) und Anforderungen (Unterabschnitt 5.1.7) an die Kryptografie in verteilten Sicherungssystemen,
- Aktualisierung der Verweisungen an neuere Ausgaben,
- Änderung der Anforderungen an die Eingabeeinheiten (Unterabschnitt 5.1.5.4),
- Anpassung der Prüfmuster für Schlüssel an die Gestaltung Einschnitt im mittleren Bereich des Schlüsselbartes (Unterabschnitt 7.3),
- Klarstellung und Optimierung der Immersionsprüfung (Unterabschnitt 8.2.6.3),
- Korrektur der Prüfung zur Hitzebeständigkeit (Unterabschnitt 8.2.7.2);
- redaktionelle Klarstellungen u.a. in den Unterabschnitten 5.1.5.1, 5.2.7, 5.3.3, 7.1, 8.2.2.1, 8.2.4.3.2, 8.2.6.2 und 8.3.3.3.2
- Ergänzung von Parametern für die Betriebsanleitung im Anhang A.

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, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Diese Europäische Norm 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 es Pflicht, dass diese Norm alle drei Jahre überarbeitet wird.

1 Anwendungsbereich

Diese Europäische Norm 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 dürfen 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, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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).

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

EN 60068-2-1:2007, *Umgebungseinflüsse — Teil 2-1: Prüfverfahren — Prüfung A: Kälte (IEC 60068-2-1:2007)*

EN 60068-2-2:2007, *Umgebungseinflüsse — Teil 2-2: Prüfverfahren — Prüfung B: Trockene Wärme (IEC 60068-2-2:2007)*

EN 60068-2-6:2008, *Umgebungseinflüsse — Teil 2-6: Prüfverfahren — Prüfung Fc: Schwingen (sinusförmig) (IEC 60068-2-6:2007)*

EN 60068-2-17:1994, *Umweltprüfungen — Teil 2: Prüfungen — Prüfung Q: Dichtheit (IEC 60068-2-17:1994)*

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 die elektromagnetische Felder (IEC 61000-4-3)*

EN 61000-4-4, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-4: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen schnelle transiente elektrische Störgrößen/Burst (IEC 61000-4-4)*

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

EN 61000-4-6, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-6: Prüf- und Messverfahren — Störfestigkeit gegen leitungsgeführte Störgrößen, induziert durch hochfrequente Felder (IEC 61000-4-6)*

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*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

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

Öffnungscod

Identifikationsinformation, die ein Entsperren des HSS gestattet

3.2.2

Berechtigungscod

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

3.2.3

Überfallcod

Parallelcod, der zusätzliche Funktionen aktiviert

3.2.4

Parallelcod

Öffnungscod, der identische Funktionen wie ein bereits existierender Öffnungscod 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

Tourstift oder Tourstifte, der Teil eines HSS ist und der die Bewegung der Blockiereinheit freigibt oder sie verhindert

3.7

Codeträger

Gegenstand, dessen physische Form oder physikalische Eigenschaften den Berechtigungscode bestimmen, z. B. ein Schlüssel

Anmerkung 1 zum Begriff: Ein kontaktbasierter elektronischer Codeträger beinhaltet einen Schaltkreis mit flüchtigem und nichtflüchtigem Speicher, damit verbundener 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

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 mechanischen Schlosses.

3.11

zerstörender Angriff

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

3.12

Zuverlässigkeit

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

3.13

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.

3.14

ausspähen

Versuch unbefugt an Information zu gelangen

3.15

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.

3.16

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

3.17

Schließsequenz

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

3.18

offene Tür

Tür liegt nicht in ihrem Rahmen

3.19

geschlossene Tür

Tür liegt in ihrem Rahmen, der/die Riegel können jetzt ausgefahren werden

3.20

verriegelte Tür

Riegel sind ausgefahren

3.21

gesperrte Tür

Riegelwerk kann nicht eingefahren werden, weil es vom HSS blockiert wird

3.22

gesicherte Tür

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

3.23

HSS im gesicherten Zustand

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

3.24

Normalzustand

das HSS Prüfmuster befindet sich nach einer Prüfung im gesicherten Zustand und alle Schlossfunktionen können ausgeführt werden

3.25

funktionsfähiger Zustand

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

3.26

Sicherheit bei Ausfall

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

3.27

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.

3.28

Sperrzeit

Zeitverzögerung aufgrund der Überschreitung der zulässigen Zahl der Öffnungsversuche

3.29

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

3.30

kryptografischer Algorithmus

mathematisches Verfahren zur Datentransformation, die die Definition von Parametern (z. B. Schlüssellänge und Anzahl von Wiederholungen oder Runden) einschließt

3.30.1

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

3.30.2

symmetrischer kryptografischer Algorithmus

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

3.31

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.

3.32

kryptografisches Modul

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

3.33

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 Wertbehälter und das andere räumlich getrennt (= verteilte Eingabeeinheit), ist ein Beispiel für ein verteiltes System. Ein elektronisches Schloss mit einem unzugänglichen Übertragungssystem im Sinne von 5.1.5.3 dieser Norm oder mit einer temporären Drahtverbindung zu einer mobilen Vorrichtung (z. B. Personal Computer), die von einer autorisierten Person überwacht wird, wird nicht als verteiltes System angesehen.

3.34

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

3.35

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.

3.36

sicherheitsrelevante Information

Codes nach 3.2, Authentifizierungen, alle Code- oder Schlüsselübertragungen und -änderungen sowie Firmware-Updates von Prozessoren

3.37

automatischer Schlüsselaustausch

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

3.38

Verfügbarkeit

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

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

Alle Anforderungen sind nach 8.1.2 zu prüfen.

5.1.1 Anforderungen an alle Klassen

5.1.1.1 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.

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

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

5.1.1.4 Eine Eingabeeinheit ist ein notwendiger Teil eines HSS, obwohl mit einer Eingabeeinheit auch mehr als ein HSS (Auswerteeinheit) bedient werden darf. Jedes HSS muss eine Auswerteeinheit besitzen, die den richtigen Code von der Eingabeeinheit 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.

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

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

5.1.2 HSS der Klasse D

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

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

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

5.1.3 Mechanische Schlüsselschlösser

5.1.3.1 Bei HSS der Klasse A (siehe Abschnitt 4) darf der gleiche Code erst dann wiederholt werden, wenn mindestens 80 % der nutzbaren Codes schon verwendet wurden.

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

5.1.3.3 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.

5.1.3.4 Es darf nicht möglich sein den Schlüssel von einem HSS abzuziehen, wenn das HSS entsperrt ist, außer für die Codeumstellung. Diese Anforderung gilt für alle Klassen. Es ist zulässig, dass diese Funktion erst vor der ersten Nutzung des HSS aktiviert wird.

5.1.3.5 Der Schlüssel darf bei Anwendung eines maximalen Drehmoments von 2,5 Nm nicht abbrechen. Die Prüfung ist nach 8.2.1.4 durchzuführen.

5.1.3.6 Neben der Erfüllung der vorhergehenden Anforderungen muss der Hersteller auch eine Herstellererklärung nach Anhang C abgeben.

5.1.4 Codierungsstufen für mechanische Schlüsselschlösser

5.1.4.1 Nutzbare Codes dürfen höchstens 40 % der Codierelemente (Zuhaltungen) mit gleich hohen Codierungsstufen enthalten.

5.1.4.2 Bei nutzbaren Codes dürfen höchstens zwei gleiche Codierungsstufen einander benachbart sein, z. B. zwei gleiche Zuhaltungen.

5.1.4.3 Bei nutzbaren Codes muss der Unterschied zwischen der höchsten und tiefsten Codierungsstufe größer als 60 % des größtmöglichen Stufensprungs des HSS sein.

5.1.5 Elektronische HSS

5.1.5.1 Bei elektronischen HSS der Klasse B und mit mehr als zwei Benutzercodes müssen die Aufzeichnungen der durchgeführten Öffnungsvorgänge nach Tabelle 1 gespeichert werden. Die gespeicherten Daten müssen selbst bei Stromausfall mindestens 1 Jahr erhalten bleiben.

5.1.5.2 Bei elektronischen HSS in gesichertem Zustand darf ein Datenverkehr mit der Auswerteeinheit nur möglich sein zur Eingabe eines Berechtigungscode und Anzeige des Schlosszustandes.

5.1.5.3 Bei nicht verteilten Systemen müssen alle Komponenten der Eingabeeinheit am Wertbehältnis befestigt sein. Bei am Wertbehältnis befestigter Eingabeeinheit darf die Verkabelung von Eingabeeinheit und Auswerteeinheit nicht zugänglich sein.

5.1.5.4 In Klasse C und D muss jegliche Manipulation oder jeglicher Austausch der Eingabeeinheit einen Überwachungseintrag auslösen und dem Benutzer automatisch bei jedem Gebrauch eine Information angezeigt werden, bis diese von einer autorisierten Person neutralisiert wird.

5.1.5.5 Bei elektronischen HSS aller Klassen muss dem Nutzer eindeutig angezeigt werden, wenn eine Sperrzeit aktiviert ist.

5.1.5.6 Anzeige des Spannungsabfalls bei Batterien: mit Batterie betriebene Schlösser müssen für mindestens 3 000 vollständige Öffnungsvorgänge funktionsfähig bleiben. Die Batteriekapazität muss überwacht werden. Im Falle eines Spannungsabfalls der Batterien muss während oder unmittelbar nach dem Entsperrvorgang ein akustisches oder optisches Signal erfolgen. Nach der ersten Anzeige des Spannungsabfalls der Batterien müssen noch mindestens zehn (10) vollständige Entsperr- und Sperrvorgänge möglich sein. Diese Anforderung muss nicht erfüllt werden, wenn eine Stromversorgung von außen möglich ist.

5.1.5.7 Der Prozessor, der die Codeauswertung vornimmt, muss sich innerhalb des Wertbehältnisses befinden.

5.1.5.8 HSS der Klasse B oder höher sind auf Einflüsse durch Stromversorgung nach 8.2.5 zu prüfen.

5.1.6 Elektronische Codeträger

5.1.6.1 Allgemeines

Der Hersteller muss in seinen Anleitungen darauf hinweisen, dass elektronische Codeträger wie mechanische Schlüssel zu sichern sind.

5.1.6.2 Kontaktlose Codeträger

5.1.6.2.1 Allgemeines

Die folgenden Anforderungen für kontaktlose elektronische Codeträger gelten nur für Kommunikationseinrichtungen im Nahbereich, bei denen ein typischer Betriebsbereich unter 15 cm liegt, z. B. NFC oder Mifare.

Ist der Abstand zur Datenübertragung zwischen elektronischem Codeträger und der Eingabeeinheit größer als 15 cm oder werden die elektronischen Codeträger für HSS der Klasse D verwendet, müssen die Anforderungen an verteilte Systeme nach 5.1.7 erfüllt werden.

ANMERKUNG Optische Systeme werden als verteilte Systeme angesehen. Ein Beispiel für einen kontaktlosen elektronischen Codeträger ist eine RFID Karte.

5.1.6.2.2 Gegenseitige Authentifizierung

Die gegenseitige Authentifizierung nach ISO/IEC 9798-2 oder ISO 9798-4 ist einzusetzen. Zeitlich variable Parameter wie Zeitstempel, Zahlenreihen oder Zufallszahlen, die verhindern, dass gültige Authentifizierungsinformationen zu einem späteren Zeitpunkt oder mehr als einmal verwendet werden (siehe ISO/IEC 9798-1:2010, Anhang B), müssen mindestens 32 bits aufweisen. Zusätzlich zu der gegenseitigen Authentifizierung muss ein gültiger Öffnungscod zur Öffnung des HSS verwendet werden.

5.1.6.2.3 Kryptografischer Schlüssel

Der kryptografische Schlüssel für symmetrische Algorithmen muss eine Mindestlänge von 64 bits für die Klassen A und B und 128 bits für die Klassen C und D haben und ist nur für das spezifische HSS-Modell vorzusehen. Asymmetrische Algorithmen müssen vergleichbare Schlüssellängen im Hinblick auf die Sicherheitsstufe (NIST SP 800-57) haben. Der kryptografische Schlüssel für symmetrische Algorithmen darf nie vom Codeträger aus gesendet werden. Er darf Teil der zu Initiierungszwecken in den elektronischen Codeträger übertragenen Kommunikationsdaten sein. Der Initiierungsvorgang muss von einer autorisierten Person in einer sicheren Umgebung vorgenommen werden. Dies muss in der Betriebsanleitung aufgeführt sein.

5.1.6.2.4 Identifikationsnummer

Jeder elektronische Codeträger muss eine einzigartige Identifikationsnummer besitzen. Die Identifikationsnummer muss eine Länge von mindestens 32 bits haben. Üblicherweise ist die Identifikationsnummer nur für die Durchführung von Auditfunktionen erforderlich. Wird die Seriennummer auch als sicherheitsrelevante Information verwendet, darf sie auf dem Codeträger nicht sichtbar sein.

5.1.6.3 Kontaktbasierte elektronische Codeträger

Kontaktierte elektronische Codeträger für andere Schlösser als solche der Klasse D müssen nicht dieselben zusätzlichen Anforderungen erfüllen wie kontaktlose elektronische Codeträger. Der Hersteller muss dann in seiner Betriebsanleitung angeben, ob irgendeine sicherheitsrelevante Information unverschlüsselt gespeichert ist.

Sicherheitsrelevante Informationen sollten sicher in einem Codeträger gespeichert werden, und es sollte eine Sicherheitsauthentifizierung geben.