

DIN EN 1300



ICS 13.310

Ersatz für
DIN EN 1300:2019-05

**Wertbehältnisse –
Klassifizierung von Hochsicherheitsschlössern nach ihrem
Widerstandswert gegen unbefugtes Öffnen;
Deutsche Fassung EN 1300:2023**

Secure storage units –

Classification for high security locks according to their resistance to unauthorized opening;
German version EN 1300:2023

Unités de stockage en lieu sûr –

Classification des serrures haute sécurité en fonction de leur résistance à l'effraction;
Version allemande EN 1300:2023

Gesamtumfang 68 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Dieses Dokument (EN 1300:2023) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat von BSI (Vereinigtes Königreich) gehalten wird.

Die nationalen Interessen bei der Erarbeitung wurden vom Arbeitsausschuss NA 060-20-01 AA „Geldschränke und Tresoranlagen (SpA CEN/TC 263, CEN/TC 263/WG 1, WG 2 und WG 3)“ des DIN-Normenausschusses Maschinenbau (NAM) wahrgenommen. Vertreter der Hersteller und Anwender von „Hochsicherheitsschlössern“ sind an der Erarbeitung beteiligt.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

EN 1143-1	siehe	DIN EN 1143-1
EN 1143-2	siehe	DIN EN 1143-2
EN 14450	siehe	DIN EN 14450
EN 17646	siehe	DIN EN 17646
EN 60068-2-1	siehe	DIN EN 60068-2-1 (VDE 0468-2-1)
EN 60068-2-2	siehe	DIN EN 60068-2-2 (VDE 0468-2-2)
EN 60068-2-6	siehe	DIN EN 60068-2-6 (VDE 0468-2-6)
EN 61000-4-2	siehe	DIN EN 61000-4-2 (VDE 0847-4-2)
EN IEC 61000-4-3	siehe	DIN EN IEC 61000-4-3 (VDE 0847-4-3)
EN 61000-4-5	siehe	DIN EN 61000-4-5 (VDE 0847-4-5)
EN ISO 22479	siehe	DIN EN ISO 22479

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

Änderungen

Gegenüber DIN EN 1300:2019-05 wurden folgende Änderungen vorgenommen:

Allgemeine Änderungen:

- a) redaktionelle Änderungen im Anwendungsbereich;
- b) Aktualisierungen in Abschnitt 2 „Normative Verweisungen“;
- c) Begriffe wurden zu Abschnitt 3 hinzugefügt (Öffnungsereignis, der Öffnung zugehöriges Ereignis, relevanter Überwachungseintrag, nicht relevanter Überwachungseintrag, Zeichen), weitere wurden aktualisiert (Einmalcode, gesperrte Tür, HSS im gesicherten Zustand, Sicherheit bei Ausfall, Sperrzeit, Authentifizierung, Firmware);
- d) Anforderungen an die verwendeten Uhren wurden hinzugefügt (siehe 8.2.2.2.1 und 8.2.3.2.1);
- e) Anforderungen wurden hinzugefügt, dass der Prüfbericht jegliche Abweichung vom beschriebenen Verfahren und jede festgestellte Besonderheit enthalten muss (siehe Abschnitt 9);
- f) Anhang C und Anhang F wurden von normativ zu informativ geändert;

- g) redaktionelle Klarstellungen in 5.1.4.5, 5.1.5.1, 5.1.5.3, 5.2.1, 5.2.6.5, 5.2.3.1, 5.2.7, 8.1.3, 8.2.1.4, 8.2.2.1, 8.2.2.3, 8.2.2.5, 8.2.4.3.2, 8.2.6.2.5, 8.2.6.3.1, 8.2.6.3.2, 8.2.6.3.3, Abschnitt 10, Abschnitt A.2 b), B.2.2, B.2.4, Anhang G, Bild 1, Tabelle 1 und Tabelle 2;

technische Änderungen zu jeder Art von Schloss:

- h) Anforderung zur Anzeige des Verriegelungszustandes (5.1.2.5 und Anhang A) wurde aktualisiert;
- i) die Prüfanforderung wurde in mehreren Unterabschnitten von „Normalzustand“ zu „funktionsfähiger Zustand“ geändert (siehe 5.2.8.1, 5.2.8.2, 8.2.5.1, 8.2.5.2, 5.3.1, 5.3.3, 8.2.6.1, 8.2.6.3.2, 8.2.6.3.3, 8.2.7.1, 8.2.7.2, 8.3.1.1, 8.3.1.4, 8.3.2.1, 8.3.2.3 und 8.3.3.1);
- j) die Anzahl der Probekörper wurde von vier auf sieben geändert (siehe 7.1);
- k) das Manipulationswerkzeug „PC“ wird nun mit dem Basiswert 0 (mit Standard-Software) und mit dem Basiswert 25 (mit HSS-spezifischer Manipulationssoftware) klassifiziert, siehe Tabelle 4;

technische Änderungen zu mechanischen Kombinationsschlössern:

- l) Hinzufügung einer Anforderung zur dynamischen Codeeingabe (siehe 5.3.4), die sich mit der bereits vorhandenen Prüfanforderung in 8.3.3 deckt;

technische Änderungen zu elektronischen Schlössern:

- m) Streichung der Anforderungen zu Verteilten Systemen und Einpflegen in die Europäische Norm EN 17646 (siehe Abschnitt 1, 5.2.5.2, 5.2.5.4, Anhang A, Anhang F);
- n) Erhöhung der Verschlüsselungsanforderung für kontaktlose Codeträger der Klasse B (von 64 bit auf 128 bit, siehe 5.1.7.2.3) und für alle Klassen, wenn der Übertragungsweg größer als 15 cm ist (müssen nach EN 17646 geprüft werden, siehe 5.1.7.2.1);
- o) 5.1.7.2.4 ist nun auch auf kontaktbasierte elektronische Codeträger anwendbar (5.1.7.3);
- p) neue Mindestanforderungen an die Aufzeichnung von Ereignissen (5.1.6.2);
- q) Aktualisierung der Anforderungen an lokale Firmware-Updates (siehe 5.1.8);
- r) Hinzufügen von Grenzüberschreitungen für nutzbare Codes für elektronische Schlösser (siehe Tabelle 1);
- s) Hinzufügen neuer Anforderungen in Bezug auf die Manipulation von elektronischen Schlössern und mechanischen Schlössern mit elektronischen Komponenten in 5.2.5.4, 8.2.2.1, Tabelle 4 und Anhang B;
- t) Aktualisierung der Prüfung mit Stromversorgung: Erhöhung der Spannung von 220 V auf einen Effektivwert von 230 V (AC) sowie Änderung zu 60 V (DC); Umstrukturierung der Abschnitte zugunsten besserer Lesbarkeit; Änderung der Kontrollzeit von 12 h zu 24 h; Hinzufügung einer Prüfanforderung für in Sicherheitsschränken genutzte elektronische HSS mit externer Auswerteeinheit nicht innerhalb der Sperreinheit (siehe 5.1.6.8, 5.2.6.1, 5.2.6.2, 8.2.5.3, 8.2.5.4 und Anhang E);
- u) Änderungen in 5.1.6.6 und 5.1.6.7.

Frühere Ausgaben

DIN V ENV 1300: 1999-04

DIN EN 1300: 2004-09, 2011-10, 2014-05, 2019-05

Nationaler Anhang NA (informativ)

Literaturhinweise

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

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

DIN EN 14450, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Sicherheitsschränke*

DIN EN 17646, *Wertbehältnisse — Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen — Verteilte Systeme*

DIN EN 60068-2-1 (VDE 0468-2-1), *Umgebungseinflüsse — Teil 2-1: Prüfverfahren — Prüfung A: Kälte (IEC 60068-2-1)*

DIN EN 60068-2-2 (VDE 0468-2-2), *Umgebungseinflüsse — Teil 2-2: Prüfverfahren — Prüfung B: Trockene Wärme (IEC 60068-2-2)*

DIN EN 60068-2-6 (VDE 0468-2-6), *Umgebungseinflüsse — Teil 2-6: Prüfverfahren — Prüfung Fc: Schwingen (sinusförmig) (IEC 60068-2-6)*

DIN EN 61000-4-2 (VDE 0847-4-2), *Elektromagnetische Verträglichkeit (EMV) — Teil 4-2: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen die Entladung statischer Elektrizität (IEC 61000-4-2)*

DIN EN IEC 61000-4-3 (VDE 0847-4-3), *Elektromagnetische Verträglichkeit (EMV) — Teil 4-3: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen hochfrequente elektromagnetische Felder*

DIN EN 61000-4-5 (VDE 0847-4-5), *Elektromagnetische Verträglichkeit (EMV) — Teil 4-5: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen Stoßspannungen (IEC 61000-4-5)*

DIN EN ISO 22479, *Korrosion von Metallen und Legierungen — Prüfung mit Schwefeldioxid in feuchter Atmosphäre (Verfahren mit festem Gasvolumen)*

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 16. Juli 2023 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, 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.



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	5
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	9
4 Klassifizierung	15
5 Anforderungen	15
5.1 Allgemeine Anforderungen	15
5.1.1 Allgemeines	15
5.1.2 Anforderungen an alle Klassen	15
5.1.3 HSS der Klasse D	15
5.1.4 Mechanische Schlüssel-HSS	16
5.1.5 Codierungsstufen für mechanische Schlüsselschlösser	16
5.1.6 Elektronische HSS	16
5.1.7 Elektronische Codeträger	18
5.1.8 Firmware-Updates	19
5.2 Sicherheitsanforderungen	19
5.2.1 Nutzbare Codes	19
5.2.2 Hochsicherheitsschlösser mit Parallelschloss	20
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	23
7 Prüfmuster	24
8 Prüfverfahren	25
8.1 Allgemeines	25
8.1.1 Allgemeines	25
8.1.2 Bewertung durch Begutachtung	25
8.1.3 Prüfablauf	25
8.2 Sicherheitsprüfungen	27
8.2.1 Nutzbare Codes	27
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	31
8.2.6 Widerstand gegen physikalische Umwelteinflüsse	32
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	36
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

B.4 Elektronische Schlösser und mechanische Schlösser mit elektronischen Komponenten . 47

B.4.1 Allgemeines 47

B.4.2 Abhören des Codes über die Datenleitung 48

B.4.3 Abhören des Codes über Tastenbetätigungs-Aufzeichner 49

B.4.4 Replay-Angriff über die Datenleitung 50

B.4.5 Brute-Force-Angriff 51

B.4.6 Seitenkanalangriffe 51

B.4.7 Bestromung des Schlosses/„Spiking“ 53

B.4.8 Mechanische Umgehung 53

B.4.9 Optisches Ausspähen des Codes 54

Anhang C (informativ) Beispiel einer Herstellererklärung 55

Anhang D (informativ) Typische Maße einer Sperreinheit 57

Anhang E (normativ) Bestimmung des Einbruchwiderstandes aufgrund von konstruktiven Anforderungen 58

E.1 Allgemeines 58

E.2 Elektronische HSS mit externer Auswerteeinheit nicht innerhalb der Sperreinheit . . . 58

E.2.1 Allgemeine konstruktive Anforderung 58

E.2.2 Konstruktive Anforderungen 58

Anhang F (informativ) Beispiel einer Herstellererklärung der Firmware 60

Anhang G (informativ) A-Abweichungen 61

Literaturhinweise 64

Bilder

Bild 1 — Schematische Darstellung der Abdeckung und der Montageplatte 26

Bild 2 — Zwei schematische Darstellungen des Prüfaufbaus zum Ausspähen in Draufsicht und Seitenansicht 31

Bild B.1 — Schematische Darstellung der Bewegung des Tourkanals aufgrund eines Stufensprungs einer Codierungsstufe 41

Bild B.2 — Schematische Darstellung der Kantenradien am Tourkanaleingang und am Tourstift 41

Bild B.3 — Schematische Darstellung der Kantenradien am Tourkanaleingang und an der Frontseite des Tourstifts 42

Bild B.4 — Schematische Darstellung des Spiels zwischen Tourstift und Zuhaltungen 43

Bild B.5 — Schematische Darstellung der Täuschungsverzahnungen/falschen Touren 44

Bild B.6 — Schematische Darstellung des Abstandes zwischen Einfallfinger und Kombinationsscheiben 45

Bild B.7 — Kombinationsscheiben mit angehobenem Einfallfinger 46

Bild D.1 — Schlossmaße 57

Tabellen

Tabelle 1 — Sicherheitsanforderungen an alle HSS 22

Tabelle 2 — Mindestanforderungen an den Widerstand gegen elektrische und elektromagnetische Einflüsse bei den angegebenen Prüfbedingungen	23
Tabelle 3 — Physikalische Umweltbedingungen	23
Tabelle 4 — Werkzeugliste für die Prüfung des Manipulationswiderstandes von mechanischen und elektronischen HSS	29
Tabelle B.1 — Abhören des Codes über die Datenleitung	48
Tabelle B.2 — Abhören des Codes über Tastenbetätigungs-Aufzeichner	49
Tabelle B.3 — Replay-Angriffe	50
Tabelle B.4 — Einfache Brute-Force-Angriffe	51
Tabelle B.5 — Seitenkanalangriffe	52
Tabelle B.6 — Bestromung des Schlosses/„Spiking“	53
Tabelle B.7 — Mechanische Umgehung	54
Tabelle B.8 — Optisches Ausspähen des Codes	54
Tabelle C.1 — Allgemeine Informationen	55
Tabelle C.2 — Spezifische Informationen	55
Tabelle G.1	62

Europäisches Vorwort

Dieses Dokument (EN 1300:2023) 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 März 2024, und etwaige entgegenstehende nationale Normen müssen bis März 2024 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 1300:2018.

EN 1300:2023 enthält im Vergleich zu EN 1300:2018 die folgenden wesentlichen technischen Änderungen:

Allgemeine Änderungen:

- redaktionelle Änderungen im Anwendungsbereich;
- Aktualisierung von Verweisen in Abschnitt 2;
- Definitionen wurden zu Abschnitt 3 hinzugefügt (Öffnungsereignis, der Öffnung zugehöriges Ereignis, relevanter Überwachungseintrag, nicht relevanter Überwachungseintrag, Zeichen). Weitere Definitionen wurden aktualisiert (Einmalcode, gesperrte Tür, HSS im gesicherten Zustand, Sicherheit bei Ausfall, Sperrzeit, Authentifizierung, Firmware);
- Anforderungen an die verwendeten Uhren wurden hinzugefügt (siehe 8.2.2.2.1 und 8.2.3.2.1);
- Anforderungen wurden hinzugefügt, dass der Prüfbericht jegliche Abweichung vom beschriebenen Verfahren und jede festgestellte Besonderheit enthalten muss (siehe Abschnitt 9);
- Anhang C und Anhang F wurden von normativ zu informativ geändert;
- redaktionelle Klarstellungen in 5.1.4.5, 5.1.5.1, 5.1.5.3, 5.2.1, 5.2.6.5, 5.2.3.1, 5.2.7, 8.1.3, 8.2.1.4, 8.2.2.1, 8.2.2.3, 8.2.2.5, 8.2.4.3.2, 8.2.6.2.5, 8.2.6.3.1, 8.2.6.3.2, 8.2.6.3.3, Abschnitt 10, Abschnitt A.2 b), B.2.2, B.2.4, Anhang G, Bild 1, Tabelle 1 und Tabelle 2.

Technische Änderungen zu jeder Art von Schloss:

- Anforderung zur Anzeige des Verriegelungszustandes (5.1.2.5 und Anhang A) wurde aktualisiert;
- die Prüfanforderung wurde in mehreren Unterabschnitten von „Normalzustand“ zu „funktionsfähiger Zustand“ geändert (siehe 5.2.8.1, 5.2.8.2, 8.2.5.1, 8.2.5.2, 5.3.1, 5.3.3, 8.2.6.1, 8.2.6.3.2, 8.2.6.3.3, 8.2.7.1, 8.2.7.2, 8.3.1.1, 8.3.1.4, 8.3.2.1, 8.3.2.3 und 8.3.3.1);
- die Anzahl der Probekörper wurde von vier auf sieben geändert (siehe 7.1);
- das Manipulationswerkzeug „PC“ wird nun mit dem Basiswert 0 (mit Standard-Software) und mit dem Basiswert 25 (mit HSS-spezifischer Manipulationssoftware) klassifiziert, siehe Tabelle 4.

Technische Änderungen zu mechanischen Kombinationsschlössern:

- Hinzufügung einer Anforderung zur dynamischen Codeeingabe (siehe 5.3.4), die sich mit der bereits vorhandenen Prüfanforderung in 8.3.3 deckt.

Technische Änderungen zu elektronischen Schlössern:

- Streichung der Anforderungen zu Verteilten Systemen und Einpflegen in die Europäische Norm EN 17646 (siehe Abschnitt 1, 5.2.5.2, 5.2.5.4, Anhang A, Anhang F);
- Erhöhung der Verschlüsselungsanforderung für kontaktlose Codeträger der Klasse B (von 64 bit auf 128 bit, siehe 5.1.7.2.3) und für alle Klassen, wenn der Übertragungsweg größer als 15 cm ist (müssen nach EN 17646 geprüft werden, siehe 5.1.7.2.1);
- 5.1.7.2.4 ist nun auch auf kontaktbasierte elektronische Codeträger anwendbar (5.1.7.3);
- neue Mindestanforderungen an die Aufzeichnung von Ereignissen (5.1.6.2);
- Aktualisierung der Anforderungen an lokale Firmware-Updates (siehe 5.1.8);
- Hinzufügen von Grenzabweichungen für nutzbare Codes für elektronische Schlösser (siehe Tabelle 1);
- Hinzufügen neuer Anforderungen in Bezug auf die Manipulation von elektronischen Schlössern und mechanischen Schlössern mit elektronischen Komponenten in 5.2.5.4, 8.2.2.1, Tabelle 4 und Anhang B;
- Aktualisierung der Prüfung mit Stromversorgung: Erhöhung der Spannung von 220 V auf einen Effektivwert von 230 V (AC) sowie Änderung zu 60 V (DC), Umstrukturierung der Abschnitte zugunsten besserer Lesbarkeit, Änderung der Kontrollzeit von 12 h zu 24 h. Hinzufügung einer Prüfanforderung für in Sicherheitsschränken genutzte elektronische HSS mit externer Auswerteeinheit nicht innerhalb der Sperreinheit (siehe 5.1.6.8, 5.2.6.1, 5.2.6.2, 8.2.5.3, 8.2.5.4 und Anhang E);
- Änderungen in 5.1.6.6 und 5.1.6.7.

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 und Disketteneinsätze*
- 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*

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

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.

1 Anwendungsbereich

Dieses Dokument legt die Anforderungen an Hochsicherheitsschlösser (HSS) hinsichtlich ihrer Zuverlässigkeit, ihres Widerstandswertes gegen zerstörende Angriffe und gegen Manipulation 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.

Es ist anzuwenden für mechanische und elektronische HSS. Für elektronische Schlösser, die in einem Verteilten System benutzt werden, wird auf EN 17646 für weitere Informationen verwiesen.

Die folgenden Merkmale können als Option enthalten sein, 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) Widerstand gegen Angriffe mit Säuren;
- e) Widerstand gegen Röntgenstrahlung;
- f) Widerstand gegen Sprengstoffe;
- g) 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 14450, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Sicherheitsschränke*

EN 17646, *Wertbehältnisse — Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen — Verteilte 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 IEC 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 22479, *Korrosion von Metallen und Legierungen — Prüfung mit Schwefeldioxid in feuchter Atmosphäre (Verfahren mit festem Gasvolumen) (ISO 22479)*

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*

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 des Öffnungscodes kann eine Blockiereinheit bewegt werden.

3.2

Code

erforderliche Identifikationsinformationen, die, wenn sie die richtigen sind, es bei Eingabe in ein HSS ermöglichen, den Sicherheitszustand des Schlosses zu ändern

3.2.1

Öffnungscodes

Identifikationsinformationen, die ein Entsperren des HSS gestatten

3.2.2

Berechtigungscodes

Identifikationsinformationen, die einen Zugang zur Auswerteeinheit gestatten und auch ein Öffnungscodes sein können

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

3.2.3

Überfallcode

Parallelcode, der eine zusätzliche Funktion aktiviert

3.2.4

Parallelcode

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

3.3

Codierart

Verfahren, durch das 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

temporärer Code, welcher nach einmaliger Nutzung erlischt

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, üblicherweise ein Riegel, 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 Schlosses.

3.11

Schließeinheit

Teil eines HSS, welches das Bewegen der Blockiereinheit ermöglicht

BEISPIEL Zuhaltungen, Spindeln, Kombinationsscheiben, Motoren, Elektromagneten

3.12

zerstörender Angriff

Angriff, der an einem HSS Schäden verursacht, die irreversibel sind und vor dem rechtmäßigen Nutzer 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 Informationen 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 vollständige Eingabe des richtigen Codes oder passenden Codeträgers 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 sein kann

3.22

gesperrte Tür

verriegelte Tür, bei der das Riegelwerk nicht eingefahren werden kann, weil es vom HSS 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

HSS, das verriegelt und verworfen wurde, dessen Blockiereinheit ausgefahren ist

3.25

HSS im ungesicherten Zustand

HSS, welches nicht im gesicherten HSS-Zustand ist

3.26

funktionsfähiger Zustand

gesicherter HSS-Zustand eines HSS-Prüfmusters, in dem es mit dem/den Öffnungscode(s) entsperrt werden kann, aber nicht alle Schlossfunktionen ausführbar sind

3.27

Sicherheit bei Ausfall

gesicherter HSS-Zustand eines HSS-Prüfmusters, in dem nicht alle Schlossfunktionen funktionsfähig sind und es deshalb mit dem/den Öffnungscode(s) nicht entsperrbar sein könnte

3.28

Widerstandseinheit

RU, en: resistance unit

Widerstandswert gegen Einbruchdiebstahl und Manipulation

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

3.29

Sperrzeit

Zeitspanne, während derer das HSS nicht bedient werden kann, um zu verhindern, dass die zulässige Zahl an falsch eingegebenen Codes nicht überschritten wird

3.30

Authentifizierung

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

3.31

kryptographischer Algorithmus

mathematisches Verfahren zur Datentransformation, das die Definition von Parametern einschließt

BEISPIEL Schlüssellänge und Anzahl von Wiederholungen oder Runden

3.31.1

asymmetrischer kryptographischer Algorithmus

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

3.31.2

symmetrischer kryptographischer Algorithmus

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

3.32

kryptographischer Schlüssel

Parameter, der in Verbindung mit einem kryptographischen Algorithmus verwendet wird, der zur Steuerung eines kryptographischen 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.

3.33

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, einer am Wertbehälter und der anderen 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 vor Ort zu einem vertrauenswürdigen Gerät (z. B. vertrauenswürdiger Personal Computer), das 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 kryptographischer Algorithmus angewandt, der den kryptographischen Schlüssel verwendet, um Klartext in 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 auf eine spezifizierte 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 Informationen

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

3.37

Firmware

Softwarecode, welcher die Auswerte- oder Eingabeeinheit des HSS betreibt

3.38

vertrauenswürdige Gerät

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

3.39

Öffnungsereignis

Eingabe eines Berechtigungscodes mit dem Ziel, das HSS in den ungesicherten Zustand zu ändern

Anmerkung 1 zum Begriff: Die Eingabe eines Berechtigungscodes mit dem Ziel, Einstellungen zu ändern, oder für andere Zwecke, die nicht das HSS in den ungesicherten Zustand ändern, ist kein Öffnungsereignis (z. B. Änderung der Zeit, Hinzufügen von Nutzern etc.).

3.40

der Öffnung zugehöriges Ereignis

gespeichertes Ereignis, das direkt mit einer Öffnung in Verbindung steht

BEISPIEL Eingabe eines Öffnungscodes, Eingabe von Teilen eines Öffnungscodes (Doppelcode-Funktion), Vorzeigen eines Codeträgers (für Einzel- oder Zwei-Faktor-Authentifizierung), Aktivierung der Schließeinheit nach der Eingabe des Öffnungscodes, Öffnen der Blockiereinheit, Änderungen des HSS in den gesicherten Zustand

Anmerkung 1 zum Begriff: Es ist nicht obligatorisch, diese Ereignisse zu speichern, allerdings sind bei deren Speicherung die Anforderungen nach 5.1.6.2 relevant.

3.41

relevanter Überwachungseintrag

gespeichertes Ereignis, das direkt mit dem HSS zusammenhängt und weder ein Öffnungsereignis noch ein der Öffnung zugehöriges Ereignis ist

BEISPIEL Aktivierung der Sperrzeit, Hinzufügen eines neuen Nutzers, Löschen eines Nutzers, Sabotagekontaktaktivierung, Änderung der Verzögerungszeit, Zeitumstellung, falsche Codeeingabe, Verbindung mit einem dem HSS zugehörigen Gerät zur Programmierung oder für Überwachungseinträge, Batterietiefstandsanzeige, Änderung von Nutzerprofilen, Änderung von Schlossprofilen, Sicherheits- und Kommunikationsfehlermeldungen, Zurücksetzen des Schlosses

Anmerkung 1 zum Begriff: Es ist nicht obligatorisch, diese Ereignisse zu speichern, allerdings sind bei deren Speicherung die Anforderungen nach 5.1.6.2 relevant.

3.42

nicht relevanter Überwachungseintrag

gespeichertes Ereignis, das nicht direkt mit dem HSS zusammenhängt

BEISPIEL Temperatur, Feuchtigkeit, Druck, Vibration, Tür offen, Tür geschlossen, Riegelwerk offen, Riegelwerk verriegelt, Verbindung zu einem Alarmsystem (ausgenommen Überfallcode als Berechtigungscodes), regelmäßiger Batteriestatus

Anmerkung 1 zum Begriff: Es ist nicht obligatorisch, diese Ereignisse zu speichern, allerdings sind bei deren Speicherung die Anforderungen nach 5.1.6.2 relevant.

3.43

Zeichen

Buchstabe, Ziffer oder anderes Symbol, das mindestens zehn unterscheidbare Varianten besitzt, um Teile eines mnemonischen Codes darzustellen

BEISPIEL Eines der Zeichen 0 bis 9 in einem numerischen Dezimalsystem

4 Klassifizierung

Anhand der Sicherheitsanforderungen erfolgt bei HSS die Klassifizierung in die HSS-Klassen (A, B, C oder D) nach Tabelle 1, Tabelle 2 und Tabelle 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 Allgemeines

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 Öffnungscode(s) muss/müssen so lange als allein gültige(r) Code(s) erhalten bleiben, bis er/sie absichtlich umgestellt wird/werden. Überlagerte 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 Alle vom HSS-Hersteller zusätzlich eingebaute Vorrichtungen (z. B. Mikroschalter) dürfen nicht in der Lage sein, Informationen über den Code zu gewinnen.

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 veranlassen 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 im gesicherten Zustand ist. Wenn das HSS diese Anforderung nicht selbsttätig automatisch erfüllt und der gesicherte und verriegelte Zustand ausschließlich überprüft werden kann, indem versucht wird, den Riegelwerksgriff des Wertbehältnisses zu betätigen, dann müssen spezifische Anforderungen in den Montagehinweisen sowie in den Betriebshinweisen (nach Anhang A) enthalten sein.

5.1.2.6 Es darf nicht möglich sein, einen Öffnungscode zu ändern, ohne einen Berechtigungscode einzugeben.

5.1.3 HSS der Klasse D

5.1.3.1 Ein Mittel ist vorzusehen, durch das 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 Schlüssel-HSS

5.1.4.1 Für jedes mechanische Schlüssel-HSS (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.

5.1.4.4 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 unmittelbar vor der ersten Nutzung des HSS aktiviert wird.

5.1.4.5 Der Schlüssel darf bei Anwendung eines maximalen Drehmoments von $(2,5 \pm 0,1)$ Nm nicht abbrechen und der geprüfte Schlüssel muss noch zum Öffnen des HSS verwendbar sein. Die Prüfung muss nach 8.2.1.4 durchgeführt werden.

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

5.1.5 Codierungsstufen für mechanische Schlüsselschlösser

5.1.5.1 Die Anzahl der maximal erlaubten Codierelemente (Zuhaltungen) mit gleich hohen Codierungsstufen wird mit 40 % der Codierelemente berechnet. Das Ergebnis ist nach dem unteren Beispiel zu runden.

BEISPIEL Bei einem Ergebnis von 0,405 ist das gerundete Ergebnis 41 %. Bei einem Ergebnis von 0,404 ist das gerundete Ergebnis 40 %.

5.1.5.2 Bei nutzbaren Codes dürfen höchstens zwei gleiche Codierungsstufen einander benachbart sein, z. B. zwei Zuhaltungen mit derselben Codierungsstufe.

5.1.5.3 Bei nutzbaren Codes muss der Unterschied zwischen der höchsten und tiefsten Codierungsstufe gleich oder größer als 60 % des größtmöglichen Codierungsstufensprungs des HSS sein. Das Ergebnis ist nach dem in 5.1.5.1 angegebenen Beispiel zu runden.

5.1.6 Elektronische HSS

5.1.6.1 Elektronische HSS dürfen nicht eine elektrische Spannung benötigen, um im gesicherten Zustand zu bleiben.

5.1.6.2 Bei elektronischen HSS der Klasse B und mit mehr als zwei Öffnungscodes sowie bei allen HSS von Klasse C und Klasse D muss Folgendes eingehalten werden:

Das HSS muss die Aufzeichnungen der durchgeführten Öffnungsvorgänge speichern und muss Maßnahmen enthalten, die sicherstellen, dass die gespeicherten Daten selbst bei Stromausfall mindestens 1 Jahr erhalten bleiben.

Die Aufzeichnungen dürfen keine sicherheitsrelevanten Informationen enthalten.

Die Mindestanzahl gespeicherter Ereignisse muss eine der folgenden Anforderungen erfüllen:

- a) umfasst eine Mindestgröße von 2 000 Einträgen; oder
- b) speichert Öffnungsereignisse (siehe 3.39) und Überwachungseinträge, die sich auf Firmware-Updates beziehen, in solcher Weise, dass die Mindestanforderungen nach Tabelle 1 stets erfüllt sind; oder
- c) enthält eine Mindestgröße nach der folgenden Gleichung. Falls nicht relevante Überwachungseinträge genutzt werden, müssen diese in einem separaten Speicher gespeichert werden:

$$R_{min} = T + \left(T \times \sum OR \right) + (5 \times T \times RE) + F$$

Dabei ist

- R_{min} die Mindest-Gesamtzahl der gespeicherten Ereignisse;
- T die Mindestanzahl der gespeicherten Aufzeichnungen der Öffnungsvorgänge (siehe Spalte 2 der Tabelle 1);
- OR die Anzahl der verschiedenen einer Öffnung zugehörigen Ereignisse (siehe 3.40). Die Öffnung als solche wird nicht zu OR hinzugerechnet;
- RE entweder **0**, falls keine weiteren relevanten Überwachungseinträge aufgezeichnet werden, oder **1**, falls weitere relevante Überwachungseinträge aufgezeichnet werden;
- F die Mindestanzahl der aufgezeichneten Firmware-Update-Ereignisse inklusive Version und Datum bezogen auf die relevante HSS-Klasse nach Tabelle 1 (nicht relevant, wenn das HSS keine Firmware-Update-Funktion besitzt).

BEISPIEL 1 Ein HSS der Klasse B speichert nur Öffnungsereignisse ohne jegliche der Öffnung zugehörigen Ereignisse oder andere Ereignisse. Die Mindestanzahl an aufgezeichneten Überwachungseinträgen ist dann $10 + (10 \times 0) + (5 \times 10 \times 0) + 0 = 10$.

BEISPIEL 2 Ein HSS der Klasse C zeichnet die folgenden Überwachungseinträge auf: „Nutzer gibt Code ein, um eine HSS-Öffnung einzuleiten“ (siehe 3.39), „HSS entsperrt“ (einer Öffnung zugehörig, siehe 3.40), „HSS gesperrt“ (einer Öffnung zugehörig, siehe 3.40), Nutzercode geändert (mit HSS zusammenhängend, siehe 3.41), Sabotagekontaktaktivierung (mit HSS zusammenhängend, siehe 3.41 und 5.1.6.4), Sperrzeit aktiviert (siehe 3.41 und 5.2.3.1) sowie "Firmware-Update durchgeführt" (siehe Tabelle 1). Die Mindestanzahl an aufgezeichneten Überwachungseinträgen ist dann $50 + (50 \times 2) + (5 \times 50 \times 1) + 3 = 403$.

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

5.1.6.4 In Klasse C und Klasse D muss jegliche Manipulation oder jeglicher Austausch der Eingabeeinheit einen Überwachungseintrag auslösen und müssen dem Nutzer automatisch bei jedem Gebrauch Informationen angezeigt werden, bis diese von einer autorisierten Person neutralisiert werden.

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

5.1.6.6 Bei batteriebetriebenen Schlössern, bei denen es nicht möglich ist, eine Stromversorgung von außen an das Wertbehältnis anzulegen oder ein mechanisches Parallelschloss nicht vorhanden ist, müssen die folgenden Anforderungen erfüllt werden: Sie müssen über 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.