

DIN EN 1300



ICS 13.310

Entwurf

Einsprüche bis 2022-01-26
Vorgesehen als Ersatz für
DIN EN 1300:2019-05

**Wertbehältnisse –
Klassifizierung von Hochsicherheitsschlössern nach ihrem
Widerstandswert gegen unbefugtes Öffnen;
Deutsche und Englische Fassung prEN 1300:2021**

Secure storage units –

Classification for high security locks according to their resistance to unauthorized opening;
German and English version prEN 1300:2021

Unités de stockage en lieu sûr –

Classification des serrures haute sécurité en fonction de leur résistance à l'effraction;
Version allemande et anglaise prEN 1300:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-11-26 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nam@vdma.org möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Maschinenbau (NAM), 60498 Frankfurt am Main, Postfach 71 08 64 oder Lyoner Str. 18, 60528 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 126 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

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 1300:2019-05 wurden folgende Änderungen vorgenommen:

a) Allgemeine Änderungen:

- 1) Aktualisierung der Verweisungen in Abschnitt 2;
- 2) Hinzufügung von Definitionen in Abschnitt 3 (Öffnungsereignis, der Öffnung zugehöriges Ereignis, relevanter Überwachungseintrag, nicht relevanter Überwachungseintrag). Weitere Definitionen wurden aktualisiert (HSS im gesicherten Zustand, Sicherheit bei Ausfall, Authentifizierung, Firmware);
- 3) Klarstellungen in 5.1.5.1, 5.1.5.3, 5.1.6.6, 5.2.1, 5.2.6.4, 8.2.4.3.2, B.2.4 und Tabelle 2.

b) Technische Änderungen an jeder Art von Schloss:

- 1) Aktualisierung der Anforderung zur Anzeige des Verriegelungszustandes (5.1.2.5 und Anhang A);
- 2) Änderung der Prüfanforderung „Normalzustand“ zu „funktionsfähiger Zustand“ in mehreren Abschnitten (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, 8.3.2.1 und 8.3.3.1);
- 3) die Anzahl der Probekörper wurde von vier auf sieben geändert (siehe 7.1).

c) Technische Änderungen für elektronische Schlösser:

- 1) Streichung der Anforderungen von Verteilten Systemen und Einpflegen der Europäischen Norm prEN 17646 (siehe Abschnitt 1, 5.2.5.2, 5.2.5.4, Anhang A, Anhang F);
- 2) Erhöhung der Verschlüsselungsanforderung für kontaktlose Codeträger der Klasse B (von 64 bits zu 128 bits, siehe 5.1.7.2.3) und für alle Klassen, wenn der Übertragungsweg größer als 15 cm ist (müssen nach der prEN 17646 geprüft werden, siehe 5.1.7.2.1);
- 3) Abschnitt 5.1.7.2.4 ist nun auch für kontaktbasierte elektronische Codeträger anwendbar (5.1.7.3);
- 4) neue Minimalanforderungen für die Aufzeichnung von Ereignissen (5.1.6.2);
- 5) Aktualisierung der Anforderungen für lokale Firmware-Updates (siehe 5.1.8);
- 6) Hinzufügen einer Toleranz für nutzbare Codes für elektronische Schlösser (siehe Tabelle 1);

- 7) Hinzufügen neuer Manipulationsanforderungen bei elektronischen Schlössern und mechanischen Schlössern mit elektronischen Komponenten 5.2.5.4, 8.2.2.1, Tabelle 4 und Anhang B;
- 8) geringfügige Änderung in 5.1.6.7.

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

— Leerseite —

Wertbehältnisse — Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen

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

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

ICS:

Deskriptoren

Inhalt

	Seite
Europäisches Vorwort	3
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	7
4 Klassifizierung	13
5 Anforderungen	13
6 Technische Dokumentation	23
7 Prüfmuster	23
8 Prüfverfahren	24
9 Prüfbericht	36
10 Kennzeichnung	37
Anhang A (normativ) Montageanleitung und Betriebshinweise	38
Anhang B (normativ) Bestimmung des Widerstandes gegen Manipulation aufgrund von konstruktiven Anforderungen	40
Anhang C (normativ) Herstellererklärung	55
Anhang D (informativ) Typische Maße einer Sperreinheit	57
Anhang E (normativ) Bestimmung des Einbruchwiderstandes aufgrund von konstruktiven Anforderungen	58
Anhang F (normativ) Herstellererklärung der Firmware	60
Anhang G (informativ) A-Abweichungen	61
Literaturhinweise	64

Europäisches Vorwort

Dieses Dokument (prEN 1300:2021) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat von BSI gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN 1300:2018 ersetzen.

Im Vergleich zur EN 1300:2018 wurden die folgenden Änderungen vorgenommen:

Allgemeine Änderungen:

- Aktualisierung der Verweisungen in Abschnitt 2;
- Hinzufügung von Definitionen in Abschnitt 3 (Öffnungsereignis, der Öffnung zugehöriges Ereignis, relevanter Überwachungseintrag, nicht relevanter Überwachungseintrag). Weitere Definitionen wurden aktualisiert (HSS im gesicherten Zustand, Sicherheit bei Ausfall, Authentifizierung, Firmware);
- Klarstellungen in 5.1.5.1, 5.1.5.3, 5.1.6.6, 5.2.1, 5.2.6.4, 8.2.4.3.2, B.2.4 und Tabelle 2.

Technische Änderungen an jeder Art von Schloss:

- Aktualisierung der Anforderung zur Anzeige des Verriegelungszustandes (5.1.2.5 und Anhang A);
- Änderung der Prüfanforderung "Normalzustand" zu "funktionsfähiger Zustand" in mehreren Abschnitten (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, 8.3.2.1 und 8.3.3.1);
- Die Anzahl der Probekörper wurde von vier auf sieben geändert (siehe 7.1).

Technische Änderungen für elektronische Schlösser:

- Streichung der Anforderungen von Verteilten Systemen und Einpflegen der Europäischen Norm prEN 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 bits zu 128 bits, siehe 5.1.7.2.3) und für alle Klassen, wenn der Übertragungsweg größer als 15 cm ist (müssen nach der prEN 17646 geprüft werden, siehe 5.1.7.2.1);
- Abschnitt 5.1.7.2.4 ist nun auch für kontaktbasierte elektronische Codeträger anwendbar (5.1.7.3);
- Neue Minimalanforderungen für die Aufzeichnung von Ereignissen (5.1.6.2);
- Aktualisierung der Anforderungen für lokale Firmware-Updates (siehe 5.1.8);
- Hinzufügen einer Toleranz für nutzbare Codes für elektronische Schlösser (siehe Tabelle 1);
- Hinzufügen neuer Manipulationsanforderungen bei elektronischen Schlössern und mechanischen Schlössern mit elektronischen Komponenten 5.2.5.4, 8.2.2.1, Tabelle 4 und Anhang B;

— Geringfügige Änderung in 5.1.6.7.

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*

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. Für elektronische Schlösser, die in einem Verteilten System benutzt werden, wird auf die prEN 17646 für weitere Informationen verwiesen.

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*

prEN 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*

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

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

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

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

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

EN ISO 6988, *Metallische und andere anorganische Überzüge — Schwefeldioxid-Prüfung mit allgemeiner Feuchtigkeitskondensation (ISO 6988:1985)*

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 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

Schließereinheit

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 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

die Blockiereinheit ist ausgefahren und das HSS ist verriegelt und verworfen

3.25

HSS im ungesicherten Zustand

HSS, welches nicht im gesicherten HSS-Zustand ist

3.26

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

3.27

Sicherheit bei Ausfall

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

3.28

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.

3.29

Sperrzeit

Zeitverzögerung aufgrund der Überschreitung der zulässigen Zahl der Öffnungsversuche

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

kryptografischer Algorithmus

mathematisches Verfahren zur Datentransformation, die die Definition von Parametern einschließt

BEISPIEL Schlüssellänge und Anzahl von Wiederholungen oder Runden.

3.31.1

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

3.31.2

symmetrischer kryptografischer Algorithmus

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

3.32

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.

3.33

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 (= 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.

3.34

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 (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.

3.35

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 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 Tokens (für Einzel- oder Zwei-Faktor Authentifizierung), Aktivierung der Blockiereinheit nach der Eingabe des Öffnungscodes, Öffnen der Blockiereinheit, Änderungen des HSS in den gesicherten Zustand, ferngesteuerte Änderung des Verriegelungszustandes.

Anmerkung 1 zum Begriff: Es ist nicht obligatorisch, diese Ereignisse zu speichern, allerdings sind bei deren Speicherungen die Anforderungen des Abschnittes 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 Speicherungen die Anforderungen des Abschnittes 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 Berechtigungscode), regelmäßiger Batteriestatus.

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

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 im gesicherten Zustand ist. Wenn das HSS diese Anforderung nicht eigenmächtig automatisch erfüllt und der gesicherte und verriegelte Zustand ausschließlich anhand des Versuchs der Betätigung des Riegelwerkgriffs vom Wertehaltnis überprüft werden kann, 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 Öffnungscod zu ändern, ohne einen Berechtigungscod 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.

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 Nm nicht abbrechen. Die Prüfung ist nach 8.2.1.4 durchzuführen.

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 Codierstufe.

5.1.5.3 Bei nutzbaren Codes muss der Unterschied zwischen der höchsten und tiefsten Codierungsstufe gleich oder größer als 60 % des größtmöglichen Codierstufensprungs 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 der Klasse C und 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 Mindestzahl an gespeicherten Ereignissen muss eines der folgenden Anforderungen erfüllen:

- a) enthält 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 Minimalanforderungen nach Tabelle 1 stets erfüllt sind oder
- c) enthält eine Mindestgröße nach der folgenden Formel. Falls nicht relevante Überwachungseinträge genutzt werden, müssen diese in einem separaten Speicher aufgezeichnet werden:

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

Dabei ist

R_{min} die minimale Gesamtzahl der gespeicherten Überwachungseinträge;

OR ist die Anzahl der verschiedenen einer Öffnung zugehörigen Ereignisse (siehe 3.40). Die Öffnung als solche wird nicht zu OR hinzugerechnet.

RE ist entweder **0** falls keine weiteren relevanten Überwachungseinträge aufgezeichnet werden oder **1** falls weitere relevante Überwachungseinträge aufgezeichnet werden.

F ist die Mindestanzahl der gespeicherten Firmware-Update-Aufzeichnungen 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, das nur Öffnungsereignisse ohne jegliche der Öffnung zugehörigen Ereignisse oder andere Ereignisse speichert. 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), "HSL versperrt" (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 $50 + (50 \times 2) + (5 \times 10 \times 1 + 3) = 403$.

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 und Auswerteeinheit nicht zugänglich sein.

5.1.6.4 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.

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

5.1.6.6 Bei Batterie betriebenen Schlössern, bei denen es nicht möglich ist eine Stromversorgung von außen bezogen auf das Wertbehältnisses anzulegen, müssen die folgenden Anforderungen erfüllt werden: diese 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.

5.1.6.7 Der Prozessor, der die Codeauswertung und Codespeicherung vornimmt, muss sich innerhalb des Wertbehältnisses befinden.

5.1.6.8 Elektronische HSS müssen im gesicherten Zustand verbleiben, wenn diese gegen Ausfall der Stromversorgung nach 8.2.5.3 geprüft werden und ab der Klasse B wenn eine Manipulationsprüfung mittels Stromversorgung nach 8.2.2 geprüft wird.

Bei elektronischen HSS, die nach E.2.1 konstruiert sind, findet Anhang E Anwendung.

5.1.6.9 Jede Anwendungssoftware zur Erzeugung von Einmalcodes muss ein Zugriffsberechtigungsverfahren (z. B. Passwort oder Dongle) benutzen, um Zugriff und Nutzung dieser zu erlauben. Sie muss zusätzlich über Maßnahmen zur sicheren Speicherung von Daten verfügen. Der Hersteller muss dem Prüflabor bekannt geben, welches Zugriffsberechtigungsverfahren und welche Maßnahmen zur sicheren Speicherung von Daten in seinem System benutzt werden (siehe Anhang C).

Der Hersteller muss in seinen Bedienungsanleitungen aussagen, dass jede Anwendungssoftware, die Einmalcodes generiert, nur in einer sicheren Umgebung installiert und betrieben werden darf.

5.1.7 Elektronische Codeträger

5.1.7.1 Allgemeines

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

5.1.7.2 Kontaktlose Codeträger

5.1.7.2.1 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 der prEN 17646 erfüllt werden.

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

5.1.7.2.2 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 Öffnungscode zur Öffnung des HSS verwendet werden.

5.1.7.2.3 Kryptografischer Schlüssel

Der kryptografische Schlüssel für symmetrische Algorithmen muss eine Mindestlänge von 64 bits für die Klasse A und 128 bits für die Klassen B, 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 oder der private Schlüssel für asymmetrische 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.

5.1.7.2.4 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 Auditzwecke erforderlich. Wird die Seriennummer auch als sicherheitsrelevante Information verwendet, darf sie auf dem Codeträger nicht sichtbar sein.

5.1.7.3 Kontaktbasierte elektronische Codeträger

Kontaktierte elektronische Codeträger für andere Schlösser als solche der Klasse D brauchen nicht dieselben zusätzlichen Anforderungen erfüllen wie kontaktlose elektronische Codeträger der Abschnitte 5.1.7.2.1, 5.1.7.2.2 und 5.1.7.2.3. 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.

5.1.7.4 Mehrzweckverwendung

Ist ein elektronischer Codeträger auch für die Verwendung in anderen Anwendungen als im HSS-System konzipiert, dürfen sicherheitsrelevante Informationen für diese anderen Anwendungen nicht zugänglich sein.

Ist der elektronische Datenträger nicht gegen die Mehrzweckverwendung geschützt, ist die folgende Angabe mit in die Betriebsanleitung aufzunehmen: *Der elektronische Codeträger darf zu keiner Zeit in anderen Anwendungen als in diesem HSS-Modell eingesetzt werden.*

5.1.8 Firmware-Updates

Wenn das HSS eine Firmware-Update-Funktion besitzt, ist das Folgende einzuhalten:

Firmware-Updates sind lokal mit einer kontaktbasierten Verbindung (z. B. mittels Kabel) mit einer Verschlüsselung von mindestens 64 bits für Klasse A und B oder 128 bits für die Klasse C und D an die Auswerte- und/oder Eingabeeinheit zu übertragen. Firmware-Updates müssen durch einen Berechtigungscode initiiert werden. Die Anzahl der Installationsversuche eines Firmware-Updates pro Stunde muss den Anforderungen der Tabelle 1 (Spalte „Maximale Anzahl der Öffnungsversuche je Stunde für

jede Codierart“) genügen. Wenn Firmware-Updates einen Öffnungscodex ändern, hinzufügen oder löschen, muss dies in der Bedienungsanleitung dokumentiert sein. Jedes Firmware-Update muss am HSS durch eine autorisierte Person bestätigt werden.

Das Firmware-Änderungsprotokoll, das Verfahren und die Verschlüsselung müssen in einer Herstellererklärung eingetragen werden (siehe Anhang F).

Jedes Gerät zwischen der Eingabe- und Auswerteeinheit darf keinerlei sicherheitsrelevante Informationen in Bezug auf das HSS erzeugen. Der Hersteller muss diese Anforderung in seiner Bedienungsanleitung erwähnen.

5.2 Sicherheitsanforderungen

5.2.1 Nutzbare Codes

Die Mindestzahl der nutzbaren Codes für alle Klassen und Arten von HSS muss den Werten von Tabelle 1 entsprechen, wenn nach 8.2.1 geprüft wird. Die Mindestzahl von 25 000 nutzbare Codes für mechanische Schlösser der Klasse A ist nur dann als ausreichend einzustufen, wenn der erforderliche Manipulationswiderstand aus Tabelle 1 nach 8.2.2 nachgewiesen wird. Ab 80 000 oder mehr nutzbaren Codes und in Übereinstimmung mit Anhang B dürfen HSS der Klasse A nicht auf Manipulationswiderstand geprüft werden.

HSS mit Parallelcodes: die Mindestzahl der nutzbaren Codes muss mit der Zahl der möglichen Parallelcodes multipliziert werden.

HSS mit variabler Länge der Öffnungscodes: die niedrigste Zahl der benutzten Zeichen, die das HSS als Öffnungscodex verarbeiten kann, ist für die Berechnung der nutzbaren Codes heranzuziehen.

Mechanische Schlüsselschlösser dürfen von den zusätzlichen Schlüsseln nicht entsperrt werden, wenn sie nach 8.2.1.3 geprüft werden.

HSS mit mehr als einer Codierart (z. B. ein mnemonischer und ein elektronischer Codeträger): mindestens eine der Codierarten muss die Sicherheitsanforderungen dieser Norm erfüllen. Bei einer zweiten vorhandenen Codierart, die nicht komplett die Anforderungen dieser Norm erfüllt, darf diese nur benutzt werden, wenn zusätzlich eine Codierart benutzt wird, die die Anforderungen in Gänze erfüllt.

5.2.2 Hochsicherheitsschlösser mit Parallelschloss

Bei HSS mit einem Parallelschloss (z. B. ein elektronisches HSS mit einem mechanischen Parallelschloss) muss die Klassifizierung nach dem Schloss mit dem geringsten Sicherheitswert erfolgen.

5.2.3 Widerstand gegen Manipulation

5.2.3.1 Höchstwerte für Öffnungsversuche

Die zulässige maximale Anzahl der Öffnungsversuche pro Stunde muss den Werten in Tabelle 1 entsprechen.

ANMERKUNG Tabelle 1 enthält für mechanische HSS mit Codeträgern keine Anforderungen an die Anzahl der Öffnungsversuche, weil der Zeitaufwand für den Wechsel der Codeträger die Anzahl der Öffnungsversuche ausreichend begrenzt.

5.2.3.2 Manipulation

Bei den Prüfungen zur Ermittlung des Widerstandswertes gegen Manipulation nach 8.2.2 müssen die Mindestwiderstandswerte M nach Tabelle 1 bei mindestens 2 der 3 Prüfmuster überschritten werden.

5.2.4 Widerstand gegen zerstörende Angriffe

Bei den Prüfungen nach 8.2.3, bei denen eine äußere Kraft aufgebracht wird, müssen die Mindestwiderstandswerte nach Tabelle 1 überschritten werden.

5.2.5 Widerstand gegen Ausspähen

5.2.5.1 Alle Eingabeinformationen in ein elektronisches HSS dürfen 30 s nach der Eingabe nicht mehr erkennbar sein, selbst wenn nur ein Teil des Öffnungscodes eingegeben wurde.

5.2.5.2 Bei allen HSS-Eingabeeinheiten der Klassen C und D, darf der Winkelbereich, in dem die Codeinformation optisch beobachtet werden kann, nicht größer als 30° gemessen von der Mittellinie aus sein, wie in 8.2.4 festgelegt.

5.2.5.3 Bei HSS der Klassen C und D ist die direkte Codeeingabe über eine Tastatur mit fester Zeichenbelegung nicht gestattet. Dies gilt nicht, wenn ein Einmalcode verwendet wird.

5.2.5.4 Kompromittierende Aussendung von Signalen:

Bei elektronischen HSS und mechanischen HSS mit elektronischen Komponenten, muss bewertet werden, dass es nicht möglich ist, sicherheitsrelevante Informationen mit von einem beliebigen Bauteil ausgesendeten Signalen zu korrelieren. Die Bewertung ist anhand von Anhang B durchzuführen.

5.2.6 Widerstand gegen elektrische und elektromagnetische Einflüsse

5.2.6.1 Befindet sich ein elektronisches Schloss im gesicherten Zustand, so muss es während der Prüfung nach 8.2.5.3 bei einem Ausfall der Versorgungsspannung gesichert bleiben.

Nach erfolgter Prüfung nach 8.2.5.4 müssen netzbetriebene HSS bei einem bis zu 12 h dauernden Ausfall der Netzversorgung gesichert bleiben können.

5.2.6.2 Elektronische HSS müssen nach der Prüfung ihrer Widerstandsfähigkeit gegen elektrostatische Entladung nach 8.2.5.5 die Anforderungen nach Tabelle 2 erfüllen. Während der Prüfung dürfen die Prüfmuster höchstens 5 ms lang in den ungesicherten Zustand gehen.

5.2.6.3 Bei der Prüfung der Widerstandsfähigkeit von elektronischen HSS gegen eingestrahlte elektromagnetische Felder nach 8.2.5.7 müssen die Anforderungen der Tabelle 2 erfüllt werden. Während dieser Prüfung dürfen die Prüfmuster höchstens 5 ms lang in den ungesicherten Zustand gehen.

5.2.6.4 Nach der Prüfung der Störfestigkeit von elektronischen HSS gegen Stoßspannungen (Surge) nach 8.2.5.7 müssen die Anforderungen der Tabelle 2 erfüllt werden. Während dieser Prüfung dürfen die Prüfmuster höchstens 5 ms lang in den ungesicherten Zustand gehen.

5.2.7 Widerstand gegen physikalische Umwelteinflüsse

Alle HSS müssen nach 8.2.6.1 und 8.2.6.2 in Bezug auf Widerstandsfähigkeit gegen Schwingen und Schockeinwirkung, nach 8.2.6.4 gegen Korrosion und elektronische Schlösser nach 8.2.6.3 gegen Immersion geprüft werden.

5.2.8 Temperaturwiderstand

5.2.8.1 Kälte

Das elektronische HSS muss sich nach einer Prüfung nach 8.2.7.1 für eine Dauer von 16 h bei –10 °C im funktionsfähigen Zustand befinden.

5.2.8.2 Trockene Wärme

Das elektronische HSS muss sich nach einer Prüfung nach 8.2.7.2 für eine Dauer von 16 h bei +55 °C, im funktionsfähigen Zustand befinden.

Tabelle 1 — Sicherheitsanforderungen für alle HSS

Klasse und Typ	Mindestanzahl der gespeicherten Aufzeichnungen der Öffnungsvorgänge	Mindestanzahl der Aufzeichnungen von Firmware-Updates, inkl. Version und Datum	Mindestanzahl der nutzbaren Codes für jede Codierart		Maximale Anzahl der Versuche je Stunde für jede Codierart	Widerstand gegen Manipulation M	Widerstand gegen zerstörende Angriffe D
			materieller Code	mnemonischer Code ^b		Mindestwiderstandseinheit RU	Mindestwiderstandseinheit RU
A elektronisch mechanisch	keine	1	25 000	80 000 ^c	300	30	80
	entfällt	entfällt	25 000	80 000	entfällt	30	80
B elektronisch mechanisch	10 (bei 3 Öffnungscodes)	1	100 000	100 000 ^c	100	60	135
	entfällt	entfällt	100 000	100 000	entfällt	60	135
C elektronisch mechanisch	50	3	1 000 000	1 000 000 ^c	30	100	250
	entfällt	entfällt	1 000 000	1 000 000	entfällt	100	250
D elektronisch mechanisch	500	5	3 000 000	3 000 000 ^c	10	620	500
	entfällt	entfällt	3 000 000	3 000 000	10 ^a	620	500
^a Ausgenommen Schlüsselschlösser. ^b Die Mindestanzahl der geforderten Zeichen ist bei elektronischen Schlössern mit mnemonischen Codes sechs (6). ^c Eine Abweichung von 0,5 % ist für spezielle Funktionen oder zur Verhinderung von einfachen Codes erlaubt.							

Tabelle 2 — Mindestanforderungen an den Widerstand gegen elektrische und elektromagnetische Einflüsse bei den angegebenen Prüfbedingungen

Störfestigkeit gegen hochfrequente elektromagnetische Felder (Prüfverfahren EN 61000-4-3)			
HSS-Klasse	Schlosszustand ^a		
A bis B	FS ^b		
C bis D	O ^b		
Prüfschärfegrad	4 ^c		
Störfestigkeit gegen elektrostatische Entladung und hochenergetische Stoßspannungen			
HSS-Klasse	Prüfmethode	Prüfschärfegrad	Schlosszustand ^a
A bis D	EN 61000-4-2	4	O ^b
A bis D	EN 61000-4-5	4 ^d	FS ^b

^a O = funktionsfähig FS = Sicherheit bei Ausfall

^b Bezeichnet den Zustand, in dem das HSS im schlimmsten Fall während und nach der Prüfung sein sollte.

^c Frequenzbereich 80 MHz bis 2,7 GHz. Vorderseite, 2 Polarisationen, AM-Modulationsverfahren (80 %, 1 kHz sinusförmig).

^d Die Prüfung ist nur mit dem Grad 4 durchzuführen, auch wenn die Standard-Prüfmethode fordert, dass niedrigere Grade zusätzlich zu prüfen sind.

Tabelle 3 — Physikalische Umweltbedingungen

Vibrationswiderstand (Prüfverfahren EN 60068-2-6, Dauerbeanspruchung mit gleitender Frequenz)			
HSS-Klasse	Beschleunigung <i>g</i>	Frequenzbereich Hz	Zyklen
A bis B	1	10 bis 150	10
C bis D	2	10 bis 150	10

5.3 Anforderungen an die Zuverlässigkeit

5.3.1 HSS müssen sich nach 10 000 Schließzyklen nach 8.3.1 im funktionsfähigen Zustand befinden.

5.3.2 Bei HSS, bei denen die Codeeingabe über einen drehbaren Zahlenknopf erfolgt, darf sich die Codeeinstellung um höchstens 1 % des Gesamteinstellbereichs ändern, wenn sie einer Codeeingabe mit definierter Dynamik nach 8.3.3 unterzogen werden.

5.3.3 Umstellbare mechanische HSS müssen sich nach 100 durchgeführten Codeänderungen nach 8.3.2 im funktionsfähigen Zustand befinden.

6 Technische Dokumentation

Die folgende Technische Dokumentation ist mit den Prüfmustern mitzuliefern:

6.1 Detaillierte Konstruktionszeichnungen mit Maß- und Toleranzangaben, inklusive der Eigenschaften der Sicherungseinheiten, mit mindestens folgenden Angaben:

- Abmessungen des Riegelkopfes oder anderer Blockiereinheiten;
- Bewegung der Blockiereinheit (Riegelausschluss);
- HSS-Einbaumaße (Beispiele von typischen Einbaumaßen werden in Anhang D gezeigt).

6.2 Die Berechnung der nutzbaren Codes und alle wesentlichen Parameter für diese Berechnung.

6.3 Alle Maßangaben, die für einen Anschluss oder eine Verbindung des HSS mit außen liegenden Bauteilen (z. B. Codeeingabeeinheit, Vorrichtung zum Bewegen der Blockiereinheit) erforderlich sind, einschließlich der Größe, Form und zugelassenen Position von Öffnungen, die für Schlüssel, Spindeln, Zahlenknopfgehäuse und Kabel benötigt werden.

6.4 Detaillierte Beschreibung des Mittels zum Ein- und Umstellen des Codes und Vorsichtsmaßnahmen, die dabei zu beachten sind.

6.5 Parameter zur Montage.

6.6 Betriebsanleitung.

6.7 Dokumentation zur Firmware und Hardware bei elektronischen HSS, einschließlich

- Struktur der Firmware;
- Schaltplan;
- Programmcode-Listing.

6.8 Beschreibung der Firmwareverfahren, die angewandt werden, um

- den Code zu speichern;
- den Code auszulesen;
- vor dem Zugriff auf gespeicherte Daten und Programme zu schützen;
- ein Löschen des Speichers zu verhindern;
- eine Manipulation zu unterbinden.

6.9 Angabe der Hochsicherheitsschloss(HSS)-Klasse, die von dem HSS erreicht werden soll.

7 Prüfmuster

7.1 Es müssen mindestens sieben Prüfmuster zur Verfügung gestellt werden. Wenn der Widerstandswert gegen Manipulation geprüft werden soll, müssen drei zusätzliche Prüfmuster zur Verfügung gestellt werden. Die Öffnungscodes dieser drei Prüfmuster müssen im Zufallsverfahren ausgewählt werden und diese Codes dürfen den Prüfern vor der Prüfung nicht bekannt sein oder werden.

Die Prüfmuster für die Manipulationsprüfung sind vom Antragsteller auf Stahlplatten montiert mit einem Gehäuse nach 8.1.3 zu liefern.

ANMERKUNG Prüfmuster für die Manipulationsprüfung können spezielle Maße haben, die aber innerhalb der Toleranzen der Technischen Dokumentation liegen. Sie werden von der Prüfstelle ausgewählt.

7.2 Jedes Prüfmuster muss alle sicherheitsrelevanten Teile eines HSS enthalten, insbesondere:

- die Eingabeeinheit;
- die Auswerteeinheit;
- die Sperreinheit;
- die Blockiereinheit;
- jedes Parallelschloss;
- alle anderen Teile, welche die Sicherheit des Prüfmusters beeinflussen.

7.3 Handelt es sich bei den Prüfmustern um mechanische Schlüsselschlösser, dann muss eines der Prüfmuster neben dem passenden Schlüssel mit zwei zusätzlichen Schlüsseln ausgestattet werden. Einer der Zusatzschlüssel muss bei einem Einschnitt im mittleren Bereich des Schlüsselbartes eine Codierungsstufe einen Stufensprung **höher** als die entsprechende Codierungsstufe des passenden Schlüssels haben. Der andere Zusatzschlüssel muss die gleiche Codierungsstufe einen Stufensprung **tiefer** als der passende Schlüssel haben.

8 Prüfverfahren

8.1 Allgemeines

8.1.1 Allgemeines

Die Prüfmuster werden hinsichtlich ihres Sicherheitswertes und ihrer Zuverlässigkeit geprüft. Bei Sicherheitsprüfungen ist es das Ziel, das Prüfmuster zu entsperren oder es bei Ausfall in den ungesicherten Zustand zu bringen; bei Zuverlässigkeitsprüfungen ist es das Ziel, festzustellen, ob das Prüfmuster nach Durchlaufen des Prüfverfahrens weiter ohne Sicherheitseinschränkungen funktionsfähig ist.

Prüfmuster von mechanischen HSS für die Prüfung des Widerstands gegen Manipulation (siehe 8.2.2) dürfen vor der Manipulationsprüfung einer Dauerbelastung von bis zu 1 000 Zyklen (siehe 8.3.1) ausgesetzt werden. Diese Prüfmuster dürfen vor der Manipulationsprüfung keiner weiteren Prüfung unterzogen werden.

Die Prüfung auf kryptografische Anforderungen gründet sich auf die Prüfung der Systembeschreibung durch den Hersteller, die eine Liste der in Bezug genommenen Normen enthalten muss.

8.1.2 Bewertung durch Begutachtung

Alle Anforderungen nach 5.1 sind durch Begutachtung zu bewerten.

8.1.3 Prüfablauf

Um den Einsatz in einem Wertbehältnis zu simulieren, ist das Prüfmuster für die folgenden Prüfungen auf einer Montageplatte aus Stahl nach der Montageanleitung des Herstellers zu befestigen und mit einer Abdeckung zu versehen, die keine anderen als die für die Montage nach der Technischen Dokumentation (siehe Abschnitt 6) und Bild 1 erforderlichen Löcher aufweisen darf: Widerstand gegen Manipulation (siehe 8.2.2), Widerstand gegen zerstörende Angriffe (siehe 8.2.3), Widerstand gegen Ausspähen (siehe 8.2.4), Widerstand gegen elektrische und elektromagnetische Einflüsse (siehe 8.2.5).

Für die dynamische Codeeingabe mit einer Dauerprüfeinrichtung ist es nicht erforderlich, eine Vorrichtung zu verwenden, die ein Wertbehältnis simuliert (Dummy).

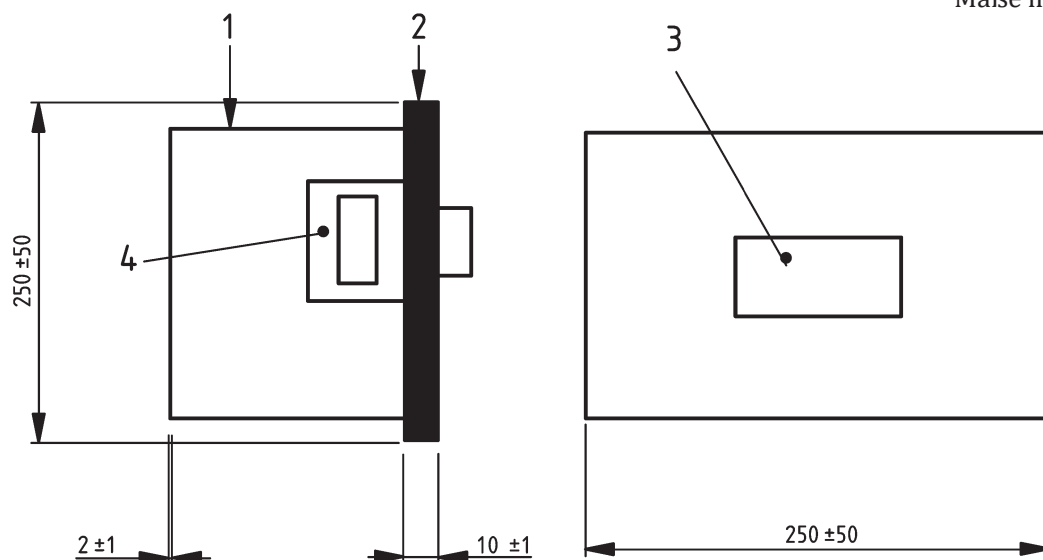
Zugriff auf das Prüfmuster darf nur in Übereinstimmung mit der Technischen Dokumentation nach Abschnitt 6 möglich sein. Handelt es sich bei dem Prüfmuster um ein elektronisches HSS, muss die Abdeckung aus Stahlblech gefertigt werden und mit der Montageplatte allseitig verschraubt werden, wobei der Schraubenabstand kleiner als 50 mm um alle vier Seiten der Stahlplatte sein muss.

Bei den Prüfungen des Widerstandes gegen Manipulation (siehe 8.2.2), Widerstandes gegen zerstörende Angriffe (siehe 8.2.3) und Widerstandes gegen Ausspähen (siehe 8.2.4) sind in die Angriffe nur jene Teile des Prüfmusters einzubeziehen, auf die ein Zugriff möglich ist, wenn das Prüfmuster auf der Montageplatte befestigt ist und keine Durchbrüche durch Montageplatte oder Abdeckung geschaffen werden.

Bei der Prüfung auf Widerstand gegen zerstörende Angriffe sind Angriffe auszuschließen, die vom Inneren des Schlosses aus gegen das Gehäuse der Sperreinheit oder dessen Abdeckplatte gerichtet sind mit dem Ziel, Teile des Gehäuses oder der Abdeckplatte der Sperreinheit zu beschädigen und/oder teilweise oder vollständig zu entfernen.

Muss der gesicherte Zustand des Prüfmusters überwacht werden, ist die Überwachung mit einer Genauigkeit von 5 ms durchzuführen.

Maße in Millimeter



Legende

- 1 Abdeckung aus Stahlblech
- 2 Montageplatte aus Stahl
- 3 Eingabeeinheit
- 4 Schloss

ANMERKUNG Mindestabstand der Stahlabdeckung vom Schloss 20 mm.

Bild 1 — Schematische Darstellung der Abdeckung und der Montageplatte

8.2 Sicherheitsprüfungen

8.2.1 Nutzbare Codes

8.2.1.1 Die vom Hersteller bereitgestellte Berechnung der nutzbaren Codes (siehe 6.2) ist auf ihre Richtigkeit zu überprüfen.

8.2.1.2 Anhand der Vorgehensweise im folgenden Beispiel und mit Hilfe einer Dauerprüfvorrichtung ist die Anzahl der nutzbaren Codes eines mechanischen Kombinations-HSS zu berechnen:

- a) die Kombinationsscheiben, mit Ausnahme der Scheibe, die als letzte eingestellt wird, werden auf ihre Öffnungszahlen eingestellt,
- b) die letzte Kombinationsscheibe wird dann auf die Prüfwahl eingestellt, dabei beginnt die Öffnungszahl minus 5 Teilstriche,
- c) es ist zu prüfen, ob das Schloss entsperrt werden kann. Wenn das Schloss entsperrt werden kann, sind die kleinste Öffnungszahl $N_{\min}$ und die größte Öffnungszahl $N_{\max}$ aufzuzeichnen,
- d) die Prüfwahl wird um 0,25 Teilstriche erhöht,
- e) die Schritte a) bis d) werden wiederholt bis die Prüfwahl die Öffnungszahl plus 5 Teilstriche beträgt.

Die Einstelltoleranz ist: $T = N_{\max} - N_{\min}$.

Die Zahl der nutzbaren Codes ist:

bei einem 3-Scheiben-Schloss: $C_n = (D_1/T) \times (D_2/T) \times (D_3/T)$
d. h. $(100/1,75) \times (100/1,75) \times (80/1,75) = 149\,271$

bei einem 4-Scheiben-Schloss: $C_n = (D_1/T) \times (D_2/T) \times (D_3/T) \times (D_4/T)$
d. h. $(100/1,75) \times (100/1,75) \times (100/1,75) \times (80/1,75)$
 $= 8\,529\,779$

D_x = die Zahl der Teilstriche der Kombinationsscheibe x ist, abzüglich des verbotenen Bereichs nach Angaben der Hersteller (gewöhnlich auf der letzten einzustellenden Kombinationsscheibe).

8.2.1.3 Bei mechanischen Schlüsselschlössern muss mit den Zusatzschlüsseln, die in einer Codierungsstufe einen Unterschied von einem Stufensprung aufweisen (siehe 7.3), mit einem maximalen Drehmoment von 1,5 Nm versucht werden, zu bestimmen, ob sie jeweils das Prüfmuster entsperren.

8.2.1.4 Um die Festigkeit des Schlüssels zu prüfen, muss das Schloss auf einer Montageplatte nach Bild 1 montiert sein. Anschließend ist der Schlüssel vollständig in das Schloss einzuführen und beständig bis zu einem Drehmoment von $(2,5 \pm 0,1)$ Nm für 5^{+1}_0 s zu belasten. Danach muss der Schlüssel aus dem Schloss entfernt werden und zum Öffnen desselben Schlosses bei einem Drehmoment maximal 1,5 Nm wieder verwendet werden können.

8.2.2 Widerstand gegen Manipulation

8.2.2.1 Kurzbeschreibung

Nach Überprüfung der Prüfmuster und der Technischen Dokumentation (siehe Abschnitt 6) ist unter Beachtung der folgenden Punkte das Verfahren zur Beurteilung des Widerstandes gegen Manipulation festzulegen:

Mechanische HSS der Klasse A mit 80 000 nutzbaren Codes, die die konstruktiven Anforderungen des Anhang B erfüllen, dürfen nicht auf ihren Widerstand gegen Manipulation geprüft werden.

Mechanische HSS der Klasse B, die die konstruktiven Anforderungen des Anhang B erfüllen, müssen nur dann geprüft werden, wenn von Seiten der Prüfstelle Unsicherheit besteht, dass die Anforderungen an den Widerstand gegen Manipulation (siehe Tabelle 1) erfüllt werden.

Bei allen mechanischen HSS der Klassen C und D muss eine Prüfung des Widerstandes gegen Manipulation erfolgen.

Bei mechanischen HSS der Klassen A und B, die die konstruktiven Anforderungen des Anhang B nicht erfüllen, oder für die nicht gezeigt werden kann, dass die konstruktiven Anforderungen erfüllt werden, darf auf Wunsch des Antragstellers eine Prüfung des Widerstands gegen Manipulation durchgeführt werden. Für die Bewertung, ob die Anforderungen an den Manipulationswiderstand erfüllt werden, gibt das Ergebnis der Prüfung und nicht die Beurteilung der Maßtoleranzen den Ausschlag.

Bei elektronischen HSS und mechanischen HSS mit elektronischen Komponenten der Klassen A und B, die die konstruktiven Anforderungen des Anhang B erfüllen, dürfen nicht auf ihren Widerstand gegen Manipulation geprüft werden. Bei elektronischen HSS und mechanischen HSS mit elektronischen Komponenten der Klassen C und D, die die konstruktiven Anforderungen des Anhangs B erfüllen, müssen nur dann geprüft werden, wenn von Seiten der Prüfstelle Unsicherheit besteht, dass die Anforderungen an den Widerstand gegen Manipulation (siehe Tabelle 1) erfüllt werden (siehe Abschnitt B.4.1.3).

8.2.2.2 Geräte

8.2.2.2.1 Uhr, die Stunden, Minuten und Sekunden anzeigt.

8.2.2.2.2 Werkzeuge nach den Kriterien der Tabelle 4.

8.2.2.3 Durchführung

Auf der Grundlage einer Vorprüfung einer ausreichenden Anzahl von Prüfmustern (siehe Abschnitt 7) anhand der Technischen Dokumentation (siehe 6.2) und des Anhangs B ist ein Prüfprogramm zur Manipulationsprüfung mit Werkzeugen (siehe Tabelle 4) aufzustellen, das nach Einschätzung des Prüfungsteams den niedrigsten Widerstandswert gegen Manipulation erzielt. An unversiegelten Prüfmustern (siehe Abschnitt 7) sind alle erforderlichen Vorversuche und Messungen zur Ermittlung der für ein Entsperren des HSS geeigneten Manipulationsverfahren durchzuführen.

8.2.2.4 Unter Anwendung des in 8.2.2.3 festgelegten Prüfverfahrens für die Manipulationsprüfung sind alle drei versiegelten Prüfmuster zu manipulieren. Die für die Manipulation erforderliche Zeit ist zu messen, wobei die Prüfung dann abgebrochen wird, wenn der Widerstandswert gegen Manipulation M der jeweiligen Schlossklasse (siehe Tabelle 1) überschritten wurde.

8.2.2.5 Darstellung der Ergebnisse

Der Widerstandswert gegen Manipulation M ist anhand der folgenden Formel zu berechnen:

$$M = t + B$$

Dabei ist

t die Zeit in Minuten zum Entsperren des Prüfmusters;

B der Basiswert. Der Basiswert ist einer der drei Werte (0, 15, 25 nach Tabelle 4) entsprechend der höchsten Kategorie des verwendeten Werkzeugs;

M der Manipulationswiderstand in Widerstandseinheiten (RU).

Tabelle 4 — Werkzeugliste für die Prüfung des Manipulationswiderstandes von mechanischen und elektronischen HSS

Nummer	Kategorie-Bezeichnung	Basiswert	Beschreibung	Beispiele mechanisch	Beispiele elektronisch
1.	Handelsübliche Geräte, Werkzeuge und Instrumente	0	Handelsübliche Werkzeuge und Geräte, die von jedermann im Werkzeughandel legal erworben werden können. Diese Werkzeuge sind klein genug, dass sie unauffällig mit sich geführt werden können. Es sind keine besonderen Fertigkeiten erforderlich, um sie wirkungsvoll einzusetzen, sie benötigen keinen Stromanschluss und ihr Gebrauch verursacht keinen Lärm, der Aufmerksamkeit erregt.	Schraubendreher	Spannungsmessgerät
				Kombizange	Strommessgerät
				Zange	Lötkolben
				Pinzetten	Kabel
				Feilen	Phasenmessgerät
				Durchtreiber	PC
				Hammer	Batterien
				Messmittel	Stromversorgungen
				Lupen	
2.	Werkzeuge zum Öffnen von HSS	15	Allgemeine Werkzeuge und Instrumente zum Öffnen von HSS, die nur bei speziellen Firmen legal gekauft werden können, und nur an ausgewiesene Schlosser/Schlüsseldienste abgegeben werden. Der wirkungsvolle Einsatz dieser Werkzeuge erfordert besondere Fertigkeiten und eine detaillierte Kenntnis des HSS und der Sperrverfahren für HSS.	Allgemeine Picking-Werkzeuge	Spektrumanalysator
				Schlossersatzteile	Oszilloskop
				Schlüsselrohlinge (ungeschnitten)	Gerät zur Schallverstärkung
				Spezialschlüssel	optische Sonden
				Gerät zur Schallverstärkung	Empfangs-/Auswertegeräte für elektromagnetische Strahlung
				optische/faser-optische Sonden	automatische Öffnungsvorrichtungen
				Maschinen zum automatischen Einstellen des Zahlencodes	

Nummer	Kategorie- Bezeichnung	Basis- wert	Beschreibung	Beispiele mechanisch	Beispiele elektronisch
3.	Spezifische HSS- Öffnungs- werkzeuge für die Verwendung an einem einzelnen Schlosstyp	25	Jedes spezifische HSS-Werkzeug und Instrument zum Öffnen von HSS, das nur bei speziellen Firmen legal gekauft werden kann, und nur an ausgewiesene Schlosser/Schlüsseldienste abgegeben werden oder speziell konstruiert, hergestellt oder verändert werden. Der wirkungsvolle Einsatz dieser Werkzeuge erfordert besondere Fertigkeiten und eine detaillierte Kenntnis des HSS und der Sperrverfahren für HSS.	HSS spezifische Picking-Werkzeuge HSS spezifische Dekoder	HSS spezifisch konstruierte elektronische Analysiereinheiten

8.2.3 Widerstand gegen zerstörende Angriffe

8.2.3.1 Kurzbeschreibung

Nach Überprüfung der Prüfmuster und der Technischen Dokumentation (siehe Abschnitt 6) wird das Verfahren zur Beurteilung des Widerstandes gegen zerstörende Angriffe festgelegt und durchgeführt.

8.2.3.2 Geräte

8.2.3.2.1 Uhr, die Stunden, Minuten und Sekunden anzeigt.

8.2.3.2.2 Werkzeuge der Kategorie A aus EN 1143-1.

8.2.3.2.3 Werkzeuge nach den Kriterien der Tabelle 4.

8.2.3.3 Durchführung

Auf der Grundlage von Vorprüfungen am/an unversiegelten Prüfmuster(n) anhand der Technischen Dokumentation (siehe Abschnitt 6) und nach allen erforderlichen Vorversuchen und Messungen sind das Prüfverfahren und die Prüfwerkzeuge festzulegen, mit denen der niedrigste Widerstandswert gegen zerstörende Angriffe erzielt wird. Ein Prüfmuster ist zu prüfen und die Prüfzeit ist zu messen. Die Prüfung darf beendet werden, wenn der Widerstandswert gegen zerstörende Angriffe der jeweiligen Klasse (siehe Tabelle 1) überschritten wird.

8.2.3.4 Darstellung der Ergebnisse

Der Widerstandswert D gegen zerstörende Angriffe ist anhand der folgenden Formel zu berechnen:

$$D = 5t + \sum BV + B$$

Dabei ist

D der Widerstand gegen zerstörende Angriffe in Widerstandseinheiten (en: resistance units, RU);

t die zum Entsperren des Prüfmusters ermittelte Zeit in Minuten;

$\sum BV$ die Summe der Basiswerte für alle verwendeten Werkzeuge der Kategorie A nach EN 1143-1;

B der Wert 0, 15 oder 25 je nach der höchsten Kategorie der verwendeten Werkzeuge aus Tabelle 4.

8.2.4 Widerstand gegen Ausspähen

8.2.4.1 Kurzbeschreibung

Das Prüfmuster ist nach Bild 1 zu montieren und in senkrechter Lage so hoch aufzustellen, dass alle Stellen des HSS und die Eingabe des Codes beobachtet werden können.

Es ist zu prüfen, ob die Eingabeinformation bei der Eingabe erkannt wird.

Zur Begrenzung des Ausspähwinkels werden zwei Schirme am Prüfmuster positioniert.

Es sind Ausspähversuche durchzuführen, um festzustellen, ob außerhalb dieses Winkelbereiches noch Eingabeinformationen erkannt werden können.

8.2.4.2 Geräte

8.2.4.2.1 Prüfvorrichtung, mit der das montierte Prüfmuster in senkrechter Lage gehalten werden kann.

8.2.4.2.2 Uhr, die Stunden, Minuten und Sekunden anzeigt.

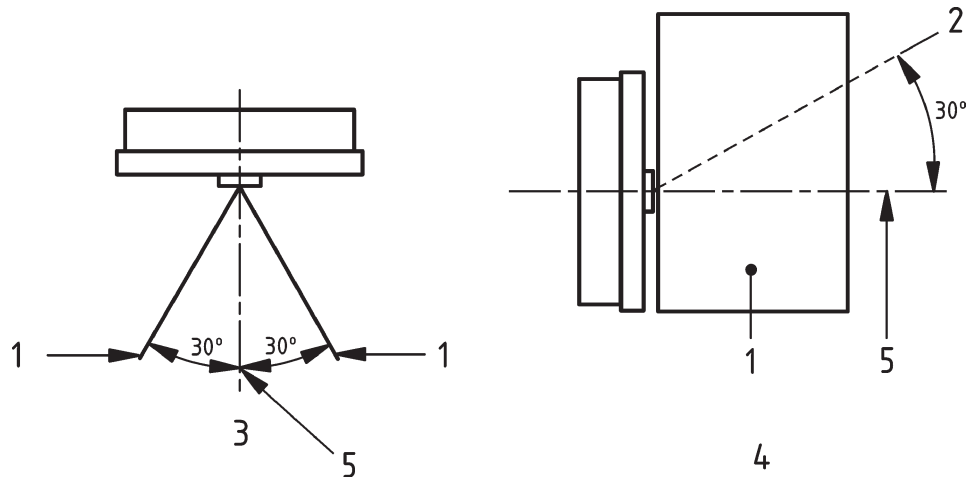
8.2.4.2.3 Zwei Schirme, mit denen ein begrenzter Ausspähwinkel bestimmt werden kann.

Für HSS-Klassen C und D kann es notwendig sein, die Prüfung des Ausspähens bei unterschiedlichen Lichtverhältnissen durchzuführen.

8.2.4.3 Durchführung

8.2.4.3.1 An einem elektronischen HSS wird der Öffnungscode eingegeben. Es wird gemessen, ob 30 s nach der letzten Eingabe eines Zeichens alle Eingabeinformationen nicht mehr feststellbar sind. Diese Prüfung ist unter Eingabe des vollständigen Codes und dann unter Eingabe nur eines Teils des Codes durchzuführen.

8.2.4.3.2 Zwei Schirme (siehe 8.2.4.2.3) werden nach Bild 2 in einem horizontalen Winkel von 60° gemessen von einer simulierten Wertbehältertür vor dem Prüfmuster positioniert. Während die Codes eingegeben werden, ist zu bestätigen, dass keine Eingabeinformationen außerhalb der 60°-Schirme in einem vertikalen Winkel von 0° bis 30° erkannt werden können.



Legende

- 1 Schirm
- 2 Blickwinkel
- 3 Draufsicht
- 4 Seitenansicht
- 5 Mittellinie

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

8.2.5 Widerstand gegen elektrische und elektromagnetische Einflüsse

8.2.5.1 Kurzbeschreibung

Elektronische HSS Prüfmuster müssen sich vor jeder Prüfung im funktionsfähigen Zustand befinden, bevor sie auf Widerstand gegen elektrische und elektromagnetische Einflüsse nach Tabelle 2 geprüft werden.

8.2.5.2 Durchführung

Die Prüfstücke sind nach den Anforderungen in 5.2.6 zu prüfen und nach jeder Prüfung ist zu bewerten, ob sich das HSS im funktionsfähigen Zustand befindet, funktionsfähig ist oder sich nach Ausfall im gesicherten Zustand befindet, jeweils entsprechend den Anforderungen.

8.2.5.3 Prüfung des Verhaltens bei Ausfall der Stromversorgung

Das Prüfmuster ist in den gesicherten Zustand zu bringen, und die zugängliche Stromversorgung, die den HSS gesicherten Zustand beeinflusst, ist abzuklemmen. Nach 24 h ist festzustellen, ob dabei der HSS-gesicherte Zustand erhalten bleibt.

Danach ist auf mögliches unbeabsichtigtes Entsperren bei Gleichstrom- oder Wechselstromzufuhr bei stetiger Erhöhung von 0 V bis 220 V zu prüfen, dabei ist das Schloss mit von außen zugänglichen Kabeln verbunden.

8.2.5.4 Erneutes Sichern des Schlosses nach Stromausfall

Ein netzbetriebenes HSS-Prüfmuster wird in den ungesicherten HSS -Zustand gebracht. Die Netzversorgung wird abgeklemmt. Es ist festzustellen, ob das HSS noch 12 h nach Abschalten der Stromversorgung erneut gesichert werden kann.

8.2.5.5 Elektrostatische Entladung

Die Prüfung der elektrostatischen Entladung ist nach EN 61000-4-2 durchzuführen, wobei die Entladung mit den Prüfschärfegraden der Tabelle 2 über die Teile des HSS-Prüfmusters erfolgen muss, die vom Benutzer bei Bedienvorgängen wie Codeeingabe, Entsperren, Sperren oder Codeumstellung, berührt werden. Die Polarität der Montageplatte ist + oder –, deshalb muss mit beiden Polaritäten geprüft werden.

Falls die Montageanleitung keine Forderung enthält, dass das Wertbehältnis aus Metall sein muss, dürfen zusätzliche Prüfungen durchgeführt werden.

8.2.5.6 Störfestigkeit gegen Stoßspannungen

Die Prüfung erfolgt nach EN 61000-4-5, wobei die Prüfschärfegrade nach Tabelle 2 anzuwenden sind.

8.2.5.7 Elektromagnetische Einstrahlung

Die Prüfung erfolgt nach EN 61000-4-3 unter Verwendung der Prüfwerte in Tabelle 2.

8.2.5.8 Darstellung der Ergebnisse

Es ist festzustellen, ob eine Änderung des Zustandes des HSS-Prüfmusters nach den Anforderungen dieser Norm oder Tabelle 2 aufgetreten ist.

8.2.6 Widerstand gegen physikalische Umwelteinflüsse

8.2.6.1 Schwingen

Die Prüfung der Widerstandsfähigkeit gegen Schwingen an einem HSS-Prüfmuster im funktionsfähigen Zustand, die für alle drei Achsen x, y und z durchgeführt wird, erfolgt nach EN 60068-2-6 unter Verwendung der Prüfwerte in Tabelle 3.

Prüfverfahren: (1) Dauerbeanspruchung mit gleitender Frequenz;
(2) zehn (10) Zyklen.

Nachdem sie Schwingungen ausgesetzt wurden, müssen sich die Prüfmuster im schlimmsten Fall in einem funktionsfähigen Zustand befinden.

8.2.6.2 Schockprüfung

8.2.6.2.1 Allgemeines

Während der Prüfung ist ständig zu überwachen, ob der gesicherte Zustand des Prüfmusters für mehr als 5 ms aufgehoben wurde. Es ist außerdem festzustellen, ob das Prüfmuster nach Durchführung der Schockprüfung nach 8.2.6.2.4 noch funktionsfähig ist.

8.2.6.2.2 Kurzbeschreibung

HSS-Prüfmuster sind einem Aufprallschock auszusetzen. Die Prüfung wird fünfmalig in einer Achse, die vom Prüfer gewählt wird, ausgeführt.

Nach fünfmaligem Fallenlassen mit $50_{-5}^0 g$ ist der Zustand des Prüfmusters festzustellen (siehe 5.2.7). Abhängig vom Ergebnis der ersten fünf Aufprallschocks kann das Prüfinstitut entscheiden, einen zusätzlichen Test mit maximal 50 Schocks mit mehr oder weniger als 50 g durchzuführen.

8.2.6.2.3 Prüfvorrichtung

Es ist eine Prüfvorrichtung zu verwenden, an der das Prüfmuster senkrecht aus einer Höhe von $(1\,000 \pm 5)$ mm fallen kann und mit einem geeigneten Dämpfer abgebremst wird. Der Dämpfer muss für die benötigte Abbremsbeschleunigung geeignet und muss am Aufprallort positioniert sein. Das Prüfmuster ist dazu auf einer starren Montageplatte entsprechend der Montageanleitung der Technischen Dokumentation (siehe Abschnitt 66) zu befestigen. Die Abbremsbeschleunigung wird an der Montageplatte gemessen und nur die Montageplatte hat Kontakt mit der übrigen Prüfvorrichtung. Die Prüfvorrichtung muss in der Lage sein, den gesicherten HSS-Zustand (z. B. die Position der Schließeinheit) laufend zu überwachen. Die Überwachung muss zum Zeitpunkt des Aufpralls beginnen und so lange anhalten, bis das System stabilisiert ist, mindestens jedoch 10 ms überwachen. Die Überwachungsvorrichtung muss geeignet sein, Stufen von 1 ms oder weniger zu messen.

8.2.6.2.4 Durchführung

- a) Das Prüfmuster ist so zu betätigen, dass das HSS in den gesicherten HSS-Zustand gebracht wird;
- b) Das Prüfmuster wird so positioniert, dass es $(1\,000 \pm 5)$ mm tief fallen kann;
- c) Es werden fünf (5) Aufschläge mit $50_{-5}^0 g$ in der gewählten Achse und Richtung durchgeführt und ermittelt, ob das Schloss im gesicherten Zustand geblieben ist;
- d) Falls eine Änderung des Zustandes ersichtlich ist (z. B. eine Bewegung der Schließeinheit), müssen zusätzliche Schocks mit mehr oder weniger als 50 g bis zu einer Anzahl von 50 Schocks durchgeführt werden.

8.2.6.2.5 Darstellung der Ergebnisse

Der Zustand des Prüfmusters ist nach der Schockprüfung aufzuzeichnen. Nach und während das HSS dem Schock ausgesetzt ist, muss das HSS sich mindestens im Zustand „Sicherheit bei Ausfall“ befinden.

8.2.6.3 Immersionsprüfung

8.2.6.3.1 Allgemeines

NaCl ist in destilliertem Wasser in einem Verhältnis von 150 ± 20 g pro Liter bei $20 \pm 5^\circ\text{C}$ aufzulösen.

8.2.6.3.2 Prüfung ohne eine im Wasser befindliche Eingabeeinheit

Prüfe das elektronische HSS im funktionsfähigen Zustand mit:

- der Auswerteeinheit,
- der Sperreinheit
- und mit der Batterie, wenn sich die Batterie nicht innerhalb der Eingabeeinheit befindet,

komplett im Salzwasser eingetaucht für 10_0^1 min. Die Eingabeeinheit muss sich außerhalb des Salzwassers befinden und muss nach der Montageanleitung verbunden sein.

Das HSS darf sich nicht unbeabsichtigt während der 10 Minuten öffnen.

8.2.6.3.3 Prüfung mit einer im Wasser befindlichen Eingabeeinheit

Prüfe das elektronische HSS im funktionsfähigen Zustand mit:

- der Auswerteeinheit,
- der Sperreinheit,
- der Eingabeeinheit
- und mit der Batterie

komplett im Salzwasser eingetaucht für 10₀¹ min. Die Eingabeeinheit muss nach der Montageanleitung verbunden sein.

Das HSS darf sich nicht unbeabsichtigt während der 10 Minuten öffnen.

8.2.6.4 Korrosionsprüfung

Nach der Prüfung auf Korrosionswiderstand durch Beanspruchung in drei Zyklen (8 h Beanspruchung durch SO₂ und 16 h durch Beanspruchung bei Umgebungstemperatur) nach EN ISO 6988 muss sich das HSS in funktionsfähigem Zustand befinden. Diese Prüfung muss ein vollständig zusammengebautes HSS durchlaufen, bei elektronischen HSS sind Batterien jedoch davon ausgeschlossen. Es müssen stattdessen Batterieattrappen verwendet werden.

8.2.7 Temperaturwiderstand

8.2.7.1 Kälte

Das elektronische HSS, das sich im funktionsfähigen Zustand befindet, ist 16 h bei –10 °C nach EN 60068-2-1, Prüfung Ab, zu prüfen. Hat das Prüfmuster nach Abschluss der Prüfung eine Temperatur von mindestens +5 °C erreicht, ist sein Zustand zu bewerten.

Batterien dürfen nach der Prüfung ersetzt werden.

8.2.7.2 Wärme

Das elektronische HSS, das sich im funktionsfähigen Zustand befindet, ist 16 h bei +55 °C nach EN 60068-2-2, Prüfung Bb, zu prüfen. Unmittelbar nach der Prüfung, bevor sich das Prüfmuster auf unter 45 °C abgekühlt hat, ist sein Zustand zu bewerten.

Batterien dürfen nach der Prüfung ersetzt werden.

8.3 Prüfung der Zuverlässigkeit

8.3.1 Dauerprüfung

8.3.1.1 Kurzbeschreibung

Ein HSS-Prüfmuster, das sich vor jeder Prüfung im funktionsfähigen Zustand befindet, ist einer Dauerbelastung mit folgendem Zyklusablauf auszusetzen: Code eingeben, entsichern, entsperren, sperren, sichern.