

**DIN EN 1300**

ICS 13.310

Einsprüche bis 2017-03-27  
Vorgesehen als Ersatz für  
DIN EN 1300:2014-05

**Entwurf**

**Wertbehältnisse –  
Klassifizierung von Hochsicherheitsschlössern nach ihrem  
Widerstandswert gegen unbefugtes Öffnen;  
Deutsche und Englische Fassung prEN 1300:2017**

Secure storage units –

Classification for high security locks according to their resistance to unauthorized opening;  
German and English version prEN 1300:2017

Unités de stockage en lieu sûr –

Classification des serrures haute sécurité en fonction de leur résistance à l'effraction;  
Version allemande et anglaise prEN 1300:2017

**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-01-27 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](http://www.din.de/go/entwuerfe) bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de), sofern dort wiedergegeben;
- oder als Datei per E-Mail an [nam@din.de](mailto:nam@din.de) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter [www.din.de/go/stellungnahmen-norm-entwuerfe](http://www.din.de/go/stellungnahmen-norm-entwuerfe) oder für Stellungnahmen zu Norm-Entwürfen der DKE unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Maschinenbau (NAM), 60498 Frankfurt am Main, Postfach 71 08 64, 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 112 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

## **Nationales Vorwort**

Dieser Norm-Entwurf beinhaltet die Deutsche Fassung der vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ im Europäischen Komitee für Normung (CEN) ausgearbeiteten prEN 1300:2017.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der prEN 1300 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.

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

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

## **Änderungen**

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

### **a) Allgemeine Änderungen:**

- 1) Aktualisierung der Verweisungen in Abschnitt 2;
- 2) Hinzufügung von Definitionen in Abschnitt 3 (Schließseinheit, HSS im ungesicherten Zustand; Firmware und Anwendungssoftware). Weitere Definitionen wurden aktualisiert;
- 3) Klarstellungen in 5.1.1.4, 5.1.4.1, 5.1.4.3, 5.1.5.8, 5.1.7.2.1, 5.2.6.3, Abschnitt 6, 8.2.5.8, 8.2.6.1, Abschnitt 10 und Abbildung 1 sowie Anhang D;

### **b) Technische Änderungen an jeder Art von Schloss:**

- 1) Anforderungen für HSS mit mehr als einer Codierart wurden in 5.2.1 hinzugefügt;
- 2) Der Shocktest ist geändert worden (siehe 8.2.6.2);
- 3) Änderung von der Immersionsprüfung, diese wird nun mit Salzwasser durchgeführt (siehe 8.2.6.3);
- 4) Aktualisierung der Dauerprüfung (siehe 8.3.1.1);
- 5) Aktualisierung der Manipulationsprüfung. Ein dritter Basiswert wurde hinzugefügt (siehe 8.2.2.5) und bei elektronischen Schlössern ist die Prüfung der Einflüsse bei Stromversorgung nun gefordert (5.1.5.9 und 8.2.5);
- 6) Aktualisierung der Herstellererklärung in Anhang C.

c) Technische Änderungen bei mechanischen Schlüsselschlössern:

- 1) Die Anforderungen an die Produktion von mechanischen Schlüsselschlössern wurden erhöht (siehe 5.1.3.1);

d) Technische Änderungen bei elektronischen Schlössern:

- 1) Für elektronische HSS wurden neue Anforderungen, z.B. in 5.1.5.1, 5.1.5.2, 5.1.5.9, 5.2.6.1, 5.2.6.3, Tabelle 2, 8.2.5.5, 8.2.5.6, 8.2.6.4, 8.2.6.5 und Anhang A hinzugefügt. Dies beinhaltet eine neue EMV-Prüfung mit höheren Frequenzen;
- 2) Anforderungen für HSS mit Einmalcodes wurden im 5.1.5.10 und Anhang A hinzugefügt;
- 3) Die Anforderungen von Schlössern der Klasse A vom Typ „elektronischer Codeträger“ und „verteiltes System“ wurden auf die Anforderungen der Klasse B erhöht worden (siehe 5.1.6.4, 5.1.7.1.6, 5.1.7.1.8, 5.1.7.1.9.1 und 5.1.7.2.2);
- 4) Anforderungen wurden beim Sichtschutz von verteilten Systemen hinzugefügt;
- 5) Anforderungen an die Firmware und an Firmware-Updates wurden in 5.1.8, Tabelle 1 und in Anhang F („Herstellererklärung der Firmware“) hinzugefügt;
- 6) Konstruktive Anforderungen für eine bestimmte Art von elektronischen Schlössern wurden im neuen Anhang E hinzugefügt („Herstellererklärung der Firmware“).

— Leerseite —

## **Wertbehälter — 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     |
| 1 Anwendungsbereich .....                                                                                         | 6     |
| 2 Normative Verweisungen .....                                                                                    | 6     |
| 3 Begriffe .....                                                                                                  | 7     |
| 4 Klassifizierung .....                                                                                           | 12    |
| 5 Anforderungen .....                                                                                             | 12    |
| 6 Technische Dokumentation .....                                                                                  | 22    |
| 7 Prüfmuster .....                                                                                                | 22    |
| 8 Prüfverfahren .....                                                                                             | 23    |
| 9 Prüfbericht .....                                                                                               | 35    |
| 10 Kennzeichnung .....                                                                                            | 35    |
| Anhang A (normativ) Montageanleitung und Betriebshinweise .....                                                   | 36    |
| Anhang B (normativ) Bestimmung des Widerstandes gegen Manipulation aufgrund von konstruktiven Anforderungen ..... | 38    |
| Anhang C (normativ) Herstellererklärung .....                                                                     | 45    |
| Anhang D (informativ) Typische Maße einer Sperreinheit .....                                                      | 47    |
| Anhang E (normativ) Bestimmung des Einbruchwiderstandes aufgrund von konstruktiven Anforderungen .....            | 48    |
| Anhang F (normativ) Herstellererklärung der Firmware .....                                                        | 49    |
| Anhang G (informativ) A-Abweichungen .....                                                                        | 50    |
| Literaturhinweise .....                                                                                           | 53    |

## Europäisches Vorwort

Dieses Dokument (prEN 1300:2017) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat vom BSI gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN 1300:2013 ersetzen.

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

Allgemeine Änderungen:

- Aktualisierung der Verweisungen in Abschnitt 2;
- Hinzufügung von Definitionen in Abschnitt 3 (Schließeinheit, HSS im ungesicherten Zustand; Firmware und Anwendungssoftware). Weitere Definitionen wurden aktualisiert;
- Klarstellungen in 5.1.1.4, 5.1.4.1, 5.1.4.3, 5.1.5.8, 5.1.7.2.1, 5.2.6.3, Abschnitt 6, 8.2.5.8, 8.2.6.1, Abschnitt 10 und Abbildung 1 sowie Anhang D.

Technische Änderungen an jeder Art von Schloss:

- Anforderungen für HSS mit mehr als einer Codierart wurden in 5.2.1 hinzugefügt;
- der Shocktest ist geändert worden (siehe 8.2.6.2);
- Änderung von der Immersionsprüfung, diese wird nun mit Salzwasser durchgeführt (siehe 8.2.6.3);
- Aktualisierung der Dauerprüfung (siehe 8.3.1.1);
- Aktualisierung der Manipulationsprüfung. Ein dritter Basiswert wurde hinzugefügt (siehe 8.2.2.5) und bei elektronischen Schlössern ist die Prüfung der Einflüsse bei Stromversorgung nun gefordert (5.1.5.9 und 8.2.5);
- Aktualisierung der Herstellererklärung in Anhang C.

Technische Änderungen bei mechanischen Schlüsselschlössern:

- Die Anforderungen an die Produktion von mechanischen Schlüsselschlössern wurden erhöht (siehe 5.1.3.1)

Technische Änderungen bei elektronischen Schlössern:

- Für elektronische HSS wurden neue Anforderungen, z. B. in 5.1.5.1, 5.1.5.2, 5.1.5.9, 5.2.6.1, 5.2.6.3, Tabelle 2, 8.2.5.5, 8.2.5.6, 8.2.6.4, 8.2.6.5 und Anhang A hinzugefügt. Dies beinhaltet eine neue EMV-Prüfung mit höheren Frequenzen;
- Anforderungen für HSS mit Einmalcodes wurden in 5.1.5.10 und Anhang A hinzugefügt;

- Die Anforderungen von Schlössern der Klasse A vom Typ „elektronischer Codeträger“ und „verteiltes System“ wurden auf die Anforderungen der Klasse B erhöht worden (siehe 5.1.6.4, 5.1.7.1.6, 5.1.7.1.8, 5.1.7.1.9.1 und 5.1.7.2.2);
- Anforderungen wurden beim Sichtschutz von verteilten Systemen hinzugefügt;
- Anforderungen an die Firmware und an Firmware-Updates wurden in 5.1.8, Tabelle 1 und in Anhang F („Herstellererklärung der Firmware“) hinzugefügt;
- Konstruktive Anforderungen für eine bestimmte Art von elektronischen Schlössern wurden im neuen Anhang E hinzugefügt ("Herstellererklärung der Firmware").

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

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

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

## Einleitung

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

## 1 Anwendungsbereich

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

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

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

## 2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 1143-1:2012, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Teil 1: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume*

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

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

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

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

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

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

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

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

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

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

### 3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

#### 3.1

##### **Hochsicherheitsschloss**

##### **HSS**

unabhängige Einheit, die gewöhnlich an Türen von Wertbehältnissen angebracht ist

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

#### 3.2

##### **Code**

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

##### 3.2.1

##### **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 Servicecode können ein Berechtigungscodes sein.

##### 3.2.3

##### **Überfallcodes**

Parallelcodes, der zusätzliche Funktionen aktiviert

##### 3.2.4

##### **Parallelcodes**

Öffnungscodes, der identische Funktionen wie ein bereits existierender Öffnungscodes 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 als Teil eines HSS, welche die Blockiereinheit 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, z. B. ein Schlüssel

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

### 3.11

#### **Schließeinheit**

Teil eines HSS, welches das Bewegen der Blockiereinheit ermöglicht

BEISPIELE      Zuhaltung, Spindel, Kombinationsscheiben, Motoren, Zylinderspulen

### 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 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 liegt nicht in ihrem Rahmen

### 3.20

#### **geschlossene Tür**

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

### 3.21

#### **verriegelte Tür**

Riegel sind ausgefahren

### 3.22

#### **gesperrte Tür**

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

### 3.23

#### **gesicherte Tür**

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

### 3.24

#### **HSS im gesicherten Zustand**

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

### 3.25

#### **HSS im ungesicherten Zustand**

HSS, welches nicht im gesicherten Zustand ist

### 3.26

#### **Normalzustand**

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

### 3.27

#### **funktionsfähiger Zustand**

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

### 3.28

#### **Sicherheit bei Ausfall**

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

### 3.29

#### **Widerstandseinheit**

##### **RU**

(en: resistance unit)

Widerstandswert gegen Diebstahl und Manipulation

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

### 3.30

#### **Sperrzeit**

Zeitverzögerung aufgrund der Überschreitung der zulässigen Zahl der Öffnungsversuche

### 3.31

#### **Authentifizierung**

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

### 3.32

#### **kryptografischer Algorithmus**

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

### 3.32.1

#### **asymmetrischer kryptografischer Algorithmus**

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

### 3.32.2

#### **symmetrischer kryptografischer Algorithmus**

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

### 3.33

#### **kryptografischer Schlüssel**

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

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

### 3.34

#### **kryptografisches Modul**

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

### 3.35

#### **verteiltes System**

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

Anmerkung 1 zum Begriff: Es wird angenommen, dass die übertragenen Informationen Dritten zugänglich sind. Ein Hochsicherheitsschloss mit Komponenten an unterschiedlichen Orten wird als verteiltes System definiert. Ein Schließsystem mit zwei Eingabeeinheiten, eines am Wertbehälter und das andere räumlich getrennt (= verteilte Eingabeeinheit), ist ein Beispiel für ein verteiltes System. Ein elektronisches Schloss mit einem unzugänglichen Übertragungssystem im Sinne von 5.1.5.3 dieser Norm oder mit einer temporären Drahtverbindung zu einer mobilen Vorrichtung (z. B. Personal Computer), die von einer autorisierten Person überwacht wird, wird nicht als verteiltes System angesehen.

### 3.36

#### **Verschlüsselung**

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

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

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

### 3.37

#### **Übertragungssystem**

Kommunikationssystem zwischen den Elementen eines verteilten Systems

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

### 3.38

#### **sicherheitsrelevante Information**

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

### 3.39

#### **automatischer Schlüsselaustausch**

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

### 3.40

#### **Verfügbarkeit**

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

### 3.41

#### **Firmware**

Softwarecode, welcher die zugeordnete Hardware nach 5.1.7.2.3 oder die Auswerte- oder Eingabeeinheit des HSS betreibt

### 3.42

#### **Anwendungssoftware**

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

## 4 Klassifizierung

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

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

## 5 Anforderungen

### 5.1 Allgemeine Anforderungen

Alle Anforderungen sind nach 8.1.2 zu prüfen.

#### 5.1.1 Anforderungen an alle Klassen

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

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

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

**5.1.1.4** Eine Eingabeeinheit ist ein notwendiger Teil eines mnemonischen und elektronischen HSS, obwohl 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.

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

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

### **5.1.2 HSS der Klasse D**

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

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

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

### **5.1.3 Mechanische Schlüsselschlösser**

**5.1.3.1** Bei jedem mechanischen Schlüsselschloss der Klasse A (siehe Abschnitt 4) darf der gleiche Code erst dann wiederholt werden, wenn mindestens 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 muss nicht erfolgen. Allerdings ist es nicht erlaubt, dass mehrere Produktionsstätten bei einem identischen Code zeitgleich anfangen zu produzieren.

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

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

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

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

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

### **5.1.4 Codierungsstufen für mechanische Schlüsselschlösser**

**5.1.4.1** Die Anzahl der maximal erlaubten Codierelemente (Zuhaltungen) mit gleich hohen Codierungsstufen wird mit 40% der Codierelemente berechnet. Das Ergebnis ist mathematisch zu runden.

**ANMERKUNG** Bei einem Ergebnis von 2,5 wäre das gerundete Ergebnis 3. Bei einem Ergebnis von 2,4 wäre das gerundete Ergebnis 2.

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

**5.1.4.3** Bei nutzbaren Codes muss der Unterschied zwischen der höchsten und tiefsten Codierungsstufe gleich oder größer als 60 % des größtmöglichen Stufensprungs des HSS sein. Das Ergebnis ist mathematisch zu runden.

### 5.1.5 Elektronische HSS

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

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

Die Aufzeichnungen dürfen keine sicherheitsrelevanten Informationen enthalten.

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

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

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

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

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

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

**5.1.5.9** 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.

**5.1.5.10** 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 einen Datenschutz zur Speicherung jeglicher Daten verfügen. Der Hersteller muss dem Prüflabor bekannt geben, welches Zugriffsberechtigungsverfahren und welcher Datenschutz in seinem System benutzt wird (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.

### 5.1.6 Elektronische Codeträger

#### 5.1.6.1 Allgemeines

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

#### 5.1.6.2 Kontaktlose Codeträger

##### 5.1.6.2.1 Allgemeines

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

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

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

##### 5.1.6.2.2 Gegenseitige Authentifizierung

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

##### 5.1.6.2.3 Kryptografischer Schlüssel

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

##### 5.1.6.2.4 Identifikationsnummer

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

#### 5.1.6.3 Kontaktbasierte elektronische Codeträger

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

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

#### 5.1.6.4 Mehrzweckverwendung

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

### 5.1.7 Anforderungen an die Kryptografie in verteilten Sicherheitssystemen

#### 5.1.7.1 Informationssicherheit

##### 5.1.7.1.1 Allgemeines

Dieser Unterabschnitt befasst sich mit den Themen Vertraulichkeit, Authentifizierung, Integrität, Verfügbarkeit, Datenübertragung, Informationsspeicherung, kryptografische Schlüssel und ihre Verwaltung.

##### 5.1.7.1.2 Vertraulichkeit

Sicherheitsrelevante Informationen, die über ein verteiltes System übertragen werden, müssen verschlüsselt werden, um unautorisiertes Lesen zu vermeiden. Für sicherheitsrelevante Datenübertragungsprozesse in verteilten Systemen sind symmetrische Algorithmen wie TDEA 64 bit Block und AES 128 bit Block Mindestanforderungen nach NIST SP 800-67 bzw. FIPS 197. Der kryptische Algorithmus ist in einem gesicherten Arbeitsmodus wie CBC, CFB oder GCM zu verwenden.

##### 5.1.7.1.3 Authentifizierung

Die Authentifizierung ist eine Voraussetzung für die Kommunikation zwischen den Komponenten eines verteilten Systems. Das Authentifizierungsverfahren ist vom Hersteller zu beschreiben.

##### 5.1.7.1.4 Integrität

Es ist sicherzustellen, dass Daten nach deren Erstellung, Übertragung oder Speicherung nicht unautorisiert geändert werden können. Dies schließt das Einfügen, Löschen oder Ersetzen von Daten ein. Ein Beispiel für anerkannte Verfahren zur Sicherstellung der Integrität sind MAC-Algorithmen oder digitale Signaturen.

##### 5.1.7.1.5 Verfügbarkeit

Ist ein verteiltes System vorübergehend nicht verfügbar, darf dieser Zustand nicht das Sicherheitsniveau gefährden.

##### 5.1.7.1.6 Speicherung sicherheitsrelevanter Information

Zur Speicherung sicherheitsrelevanter Information in HSS müssen kryptografischen Konzepte, wie in 5.1.7.1.2 erwähnt, gewählt werden.

##### 5.1.7.1.7 Kryptografische Schlüsselverwaltung

Kryptografische Schlüssel müssen gegen unbefugten Zugang geschützt werden. Das Verfahren zur Speicherung, Erstellung, Übertragung und zum Zugang zu kryptografischen Schlüsseln muss vom Hersteller beschrieben werden. Diese Anforderungen gelten auch für den Initialisierungsprozess des Herstellers.

#### **5.1.7.1.8 Kryptografische Schlüssel zur Datenübertragung**

Verteilte Systeme müssen mit kryptografischen Schlüsseln ausgestattet sein, die bei Initialisierung per Zufall generiert werden, ausgenommen sind die Werkeinstellungen für kryptografische Schlüssel bei allen Klassen. Die Sicherheitsanforderungen nach FIPS Pub 140-2, 4.7.1 (zufällige Nummerngenerierung) sind bei der Generierung zufälliger Zahlen zu berücksichtigen.

Die kryptografischen Schlüssel müssen von HSS im Feldeinsatz veränderbar sein. Sobald ein neuer Schlüssel bestätigt ist, muss der neue Schlüssel der einzig anwendbare sein.

#### **5.1.7.1.9 Änderung der kryptografischen Schlüssel**

##### **5.1.7.1.9.1 Allgemeines**

Vor Inbetriebnahme der verteilten Systeme müssen die Werkeinstellungen kryptografischer Schlüssel geändert werden.

##### **5.1.7.1.9.2 Schlüsselaustausch**

Schlüsselaustausche müssen asymmetrische Verfahren (auf Grundlage von Algorithmen wie RSA, ECC) oder symmetrische Verfahren (wie Kerberos 5) verwenden. Das Verfahren zum Schlüsselaustausch muss mindestens die äquivalente Sicherheitsstufe wie das Verfahren zur Datenübertragung aufweisen. Eine Übersicht geeigneter Schlüsselgrößen und der Gleichwertigkeit von symmetrischen und asymmetrischen Schlüssellängen ist NIST /SP 800-57 zu entnehmen. Wird der Schlüsselaustausch automatisch oder manuell angestoßen, muss die Häufigkeit des Schlüsselaustauschs den Vorgaben der NIST /SP 800-57 folgen.

##### **5.1.7.1.9.3 Schlüsseländerung**

Der Hersteller muss in der Bedienungsanleitung den Ablauf und die Häufigkeit der Schlüsseländerungen erklären. Änderungen dürfen nur nach Eingabe eines Autorisierungscode erfolgen. Erfolgt die Schlüsseländerung außer Band (außerhalb des vorher eingerichteten Kommunikationsverfahrens), ist 5.1.7.1.7 anzuwenden.

#### **5.1.7.2 Sicherheit einer verteilten Eingabeeinheit**

##### **5.1.7.2.1 Allgemeines**

Diese Anforderung ist nur zu erfüllen, wenn sicherheitsrelevante Daten übermittelt werden.

##### **5.1.7.2.2 Physikalische Sicherheit**

In einem verteilten System muss jede Eingabeeinheit jeder HSS Klasse 5.1.5.4 folgen.

##### **5.1.7.2.3 Informationssicherheit**

Sicherheitsrelevante Informationen dürfen nur in vertrauenswürdige (abgesicherte) und ausschließlich für diesen Verwendungszweck vorgesehene Eingabeeinheiten nach 5.1.7.1 eingegeben werden. Im Fall von unautorisierten Versuchen, Zugang zu diesen Eingabeeinheiten zu erhalten, müssen diese für den normalen Gebrauch gesperrt werden, z. B. durch Aktivierung von Mechanismen, die den Klartext kryptografischer Schlüssel löschen oder nutzlos machen (d. h. Schutz vor unbefugtem Zugriff). Stufe 3 der physikalischen Sicherheitsanforderungen nach FIPS Pub 140-2, 4.5.1, muss mindestens erfüllt werden.

#### **5.1.8 Firmware-Updates**

Firmware-Updates sind verschlüsselt nach 5.1.7 an die Auswerte und/oder Eingabeeinheit zu übertragen. Firmware-Updates müssen durch einen Berechtigungscode eingeleitet werden. Die Anzahl der Installationsversuche eines Firmware-Updates pro Stunde muss den Anforderungen der Tabelle 1 genügen. Ein Firmware-Update darf nicht einen Öffnungscode ändern oder löschen.

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

Jedes Gerät zwischen Eingabe- und Auswerteeinheit darf nicht HSS sicherheitsrelevante Informationen 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 nutzbaren Codes für mechanische Schlösser der Klasse A ist nur dann als ausreichend einzustufen, wenn der Manipulationswiderstand nach Tabelle 1 mittels manueller Prüfung 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 Öffnungscode 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 eines der Codierarten muss die Sicherheitsanforderungen dieser Norm erfüllen. Bei einer zweiten vorhandenen Codierart, die nicht komplett die Anforderungen dieser Norm erfüllt, kann 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** Alle HSS-Eingabeeinheiten der Klassen C und D und bei verteilten Eingabeeinheiten (bezieht sich auch auf vertrauenswürdige (abgesicherte) und ausschließlich für den Verwendungszweck vorgesehene Eingabeeinheiten nach 5.1.7.2.3) aller Klassen, die in einem verteilten System benutzt werden, darf der Winkelbereich, in dem die Codeinformation optisch beobachtet werden kann, nicht größer als 30° sein, gemessen von der Mittellinie aus 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:

Es darf nicht möglich sein, unverschlüsselte sicherheitsrelevante Informationen mit von einem beliebigen Bauteil eines verteilten Systems ausgesendeten Signalen zu korrelieren. In Verbindung mit kompromittierender Strahlung ist dem Übertragungssystem aufgrund der Strahlungskopplung und/oder drahtloser Übertragungen besonderes Augenmerk zu schenken.

## 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 auch gesichert bleiben.

Nach erfolgter Prüfung nach 8.2.5.4 müssen netzbetriebene HSS bei einem bis zu 12 h dauernden Ausfall der Netzversorgung gesichert werden 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 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 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 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 16 h bei –10 °C im Normalzustand befinden.

### 5.2.8.2 Trockene Wärme

Das elektronische HSS muss sich nach einer Prüfung nach 8.2.7.2, über 16 h bei +55 °C, im Normalzustand 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 Codierungsart |                                | Maximale Anzahl der Öffnungsversuche je Stunde für jede Codierungsart | Widerstand gegen Manipulation M | Widerstand gegen zerstörende Angriffe D |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------|--------------------------------|-----------------------------------------------------------------------|---------------------------------|-----------------------------------------|
|                                                                                                                                                                                                                                                                                                    |                                                                     |                                                                                | materieller Code                                         | mnemonischer Code <sup>b</sup> | beliebig                                                              | Mindestwiderstandseinheit RU    | Mindestwiderstandseinheit RU            |
| <b>A</b>                                                                                                                                                                                                                                                                                           |                                                                     |                                                                                |                                                          |                                |                                                                       |                                 |                                         |
| elektronisch                                                                                                                                                                                                                                                                                       | keine                                                               | keine <sup>c</sup>                                                             | 25 000                                                   | 80 000                         | 300                                                                   | 30                              | 80                                      |
| mechanisch                                                                                                                                                                                                                                                                                         | entfällt                                                            | entfällt                                                                       | 25 000                                                   | 80 000                         | entfällt                                                              | 30                              | 80                                      |
| <b>B</b>                                                                                                                                                                                                                                                                                           |                                                                     |                                                                                |                                                          |                                |                                                                       |                                 |                                         |
| elektronisch                                                                                                                                                                                                                                                                                       | 10 (bei 3 Öffnungscodes)                                            | keine <sup>c</sup>                                                             | 100 000                                                  | 100 000                        | 100                                                                   | 60                              | 135                                     |
| mechanisch                                                                                                                                                                                                                                                                                         | entfällt                                                            | entfällt                                                                       | 100 000                                                  | 100 000                        | entfällt                                                              | 60                              | 135                                     |
| <b>C</b>                                                                                                                                                                                                                                                                                           |                                                                     |                                                                                |                                                          |                                |                                                                       |                                 |                                         |
| elektronisch                                                                                                                                                                                                                                                                                       | 50                                                                  | 3                                                                              | 1 000 000                                                | 1 000 000                      | 30                                                                    | 100                             | 250                                     |
| mechanisch                                                                                                                                                                                                                                                                                         | entfällt                                                            | entfällt                                                                       | 1 000 000                                                | 1 000 000                      | entfällt                                                              | 100                             | 250                                     |
| <b>D</b>                                                                                                                                                                                                                                                                                           |                                                                     |                                                                                |                                                          |                                |                                                                       |                                 |                                         |
| elektronisch                                                                                                                                                                                                                                                                                       | 500                                                                 | 5                                                                              | 3 000 000                                                | 3 000 000                      | 10                                                                    | 620                             | 500                                     |
| mechanisch                                                                                                                                                                                                                                                                                         | entfällt                                                            | entfällt                                                                       | 3 000 000                                                | 3 000 000                      | 10 <sup>a</sup>                                                       | 620                             | 500                                     |
| <sup>a</sup> Ausgenommen Schlüsselschlösser.<br><sup>b</sup> Die Mindestanzahl der geforderten Zeichen ist bei elektronischen Schlössern mit mnemonischen Codes sechs (6).<br><sup>c</sup> Bei verteilten System der Klasse A und B muss mindestens das letzte Firmware-Update gespeichert werden. |                                                                     |                                                                                |                                                          |                                |                                                                       |                                 |                                         |

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

| Störfestigkeit gegen hochfrequente elektromagnetische Felder<br>(Prüfverfahren EN 61000-4-3)                                    |                             |                 |                             |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------|-----------------------------|
| HSS-Klasse                                                                                                                      | Schlosszustand <sup>a</sup> |                 |                             |
| A bis B                                                                                                                         | FS <sup>b</sup>             |                 |                             |
| C bis D                                                                                                                         | O <sup>b</sup>              |                 |                             |
| Prüfschärfegrad                                                                                                                 | 4 <sup>c</sup>              |                 |                             |
| Störfestigkeit gegen elektrostatische Entladung und hochenergetische Stoßspannungen                                             |                             |                 |                             |
| HSS Klasse                                                                                                                      | Prüfmethode                 | Prüfschärfegrad | Schlosszustand <sup>a</sup> |
| A bis D                                                                                                                         | EN 61000-4-2                | 4               | O <sup>b</sup>              |
| A bis D                                                                                                                         | EN 61000-4-5                | 4               | FS <sup>b</sup>             |
| <sup>a</sup> N = Normalzustand    O = funktionsfähig    FS = Sicherheit bei Ausfall                                             |                             |                 |                             |
| <sup>b</sup> Bezeichnet den Zustand, in dem das HSS im schlimmsten Fall während und nach der Prüfung sein sollte.               |                             |                 |                             |
| <sup>c</sup> Frequenzbereich 80 MHz bis 2,7 GHz. Vorderseite, 2 Polarisationen, AM-Modulationsverfahren (80%, 1kHz sinusförmig) |                             |                 |                             |

**Tabelle 3 — Physikalische Umweltbedingungen**

| Vibrationswiderstand<br>(Prüfverfahren EN 60068-2-6, Dauerbeanspruchung mit gleitender Frequenz) |                            |                       |        |
|--------------------------------------------------------------------------------------------------|----------------------------|-----------------------|--------|
| HSS-Klasse                                                                                       | Beschleunigung<br><i>g</i> | Frequenzbereich<br>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 Normalzustand 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 Normalzustand 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 während des Sperrens des Riegelkopfes oder einer anderen Blockiereinheit;
- 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, Zahlenknopfgerätschaften 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 vier 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;
- ein 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 **tief**er 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 muss: 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).

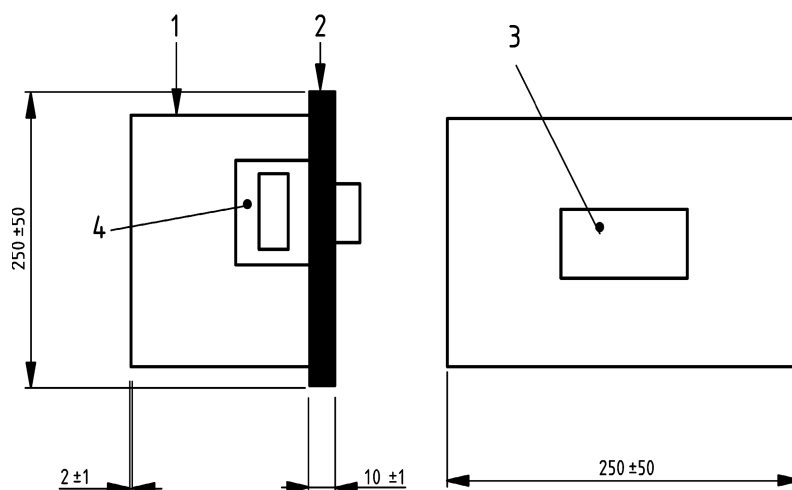
Zugriff auf das Prüfmuster darf nur in Übereinstimmung mit der Technischen Dokumentation nach Abschnitt 6 möglich sein. Handelt es sich bei dem Prüfmuster um ein elektronisches HSS, muss die Abdeckung aus Stahlblech gefertigt werden und mit der Montageplatte allseitig verschraubt werden, wobei der Schraubenabstand 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 Schlossgehäuse oder dessen Abdeckplatte gerichtet sind mit dem Ziel, Teile des Gehäuses oder der Abdeckplatte 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 bestimmen:

- die Kombinationsscheiben, mit Ausnahme der Scheibe, die als letzte eingestellt wird, werden auf ihre Öffnungszahlen eingestellt,
- die letzte Kombinationsscheibe wird dann auf die Prüfwahl eingestellt, dabei beginnt die Öffnungszahl minus 5 Teilstriche,
- es ist zu prüfen, ob das Schloss entsperrt werden kann. Wenn das Schloss entsperrt werden kann, ist die kleinste Öffnungszahl  $N_{\min}$  und die größte Öffnungszahl  $N_{\max}$ , aufzuzeichnen,
- die Prüfwahl wird um 0,25 Teilstriche erhöht,
- 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  $5 \pm 0,1$  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 Anhangs B erfüllen, dürfen nicht auf ihren Widerstand gegen Manipulation geprüft werden.

Mechanische HSS der Klasse B, 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.

Bei elektronischen HSS aller Klassen und 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 Anhangs 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.

#### **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 oder 25 aus 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         | <p>Handelsübliche Werkzeuge und Geräte, die von jedermann im Werkzeughandel erworben werden können. Diese Werkzeuge sind klein genug, dass sie unauffällig mit sich geführt werden können.</p> <p>Es sind keine besonderen Fertigkeiten erforderlich, um sie wirkungsvoll einzusetzen, sie benötigen keinen Stromanschluss und ihr Gebrauch verursacht keinen Lärm, der Aufmerksamkeit erregt.</p>               | Schraubendreher                                        | Spannungsmessgerät                                        |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Kombizange                                             | Strommessgerät                                            |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Zange                                                  | LötKolben                                                 |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Pinzetten                                              | Kabel                                                     |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Feilen                                                 | Phasenmessgerät                                           |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Durchtreiber                                           | PC                                                        |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Hammer                                                 | Batterien                                                 |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Messmittel                                             | Stromversorgungen                                         |
| 2.     | Werkzeuge zum Öffnen von HSS                     | 15        | <p>Allgemeine Werkzeuge und Instrumente zum Öffnen von HSS, die nur bei speziellen Firmen gekauft werden können, und nur an ausgewiesene Schlosser/Schlüsseldienste abgegeben werden oder speziell konstruiert, hergestellt oder verändert werden.</p> <p>Der wirkungsvolle Einsatz dieser Werkzeuge erfordert besondere Fertigkeiten und eine detaillierte Kenntnis des HSS und der Sperrverfahren für HSS.</p> | Allgemeine Picking Werkzeuge                           | Spektrumanalysator                                        |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Schlossersatzteile                                     | Oszilloskop                                               |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Schlüsselrohlinge (ungeschnitten)                      | Gerät zur Schallverstärkung                               |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Spezialschlüssel                                       | optische/faseroptische Sonden                             |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Gerät zur Schallverstärkung                            | Empfangs-/Auswertegeräte für elektromagnetische Strahlung |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | optische/faseroptische Sonden                          | automatische Öffnungsvorrichtungen                        |
|        |                                                  |           |                                                                                                                                                                                                                                                                                                                                                                                                                  | Maschinen zum automatischen Einstellen des Zahlencodes |                                                           |

|    |                                                                                    |    |                                                                                                                                                                                                                                                                                                                                                                                                                  |                                   |                                                              |
|----|------------------------------------------------------------------------------------|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|--------------------------------------------------------------|
| 3. | Spezifische HSS-Öffnungswerkzeuge für die Verwendung am einem einzelnen Schlusstyp | 25 | Jedes spezifische HSS-Werkzeug und Instrument zum Öffnen von HSS, das nur bei speziellen Firmen gekauft werden kann, und nur an ausgewiesene Schlosser/Schlüsseldienste abgegeben werden oder speziell konstruiert, hergestellt oder verändert werden.<br><br>Der wirkungsvolle Einsatz dieser Werkzeuge erfordert besondere Fertigkeiten und eine detaillierte Kenntnis des HSS und der Sperrverfahren für HSS. | HSS spezifische Picking Werkzeuge | HSS spezifisch konstruierte elektronische Analysiereinheiten |
|    |                                                                                    |    |                                                                                                                                                                                                                                                                                                                                                                                                                  | HSS spezifische Decodierer        |                                                              |

### 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 (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 oder 15 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.

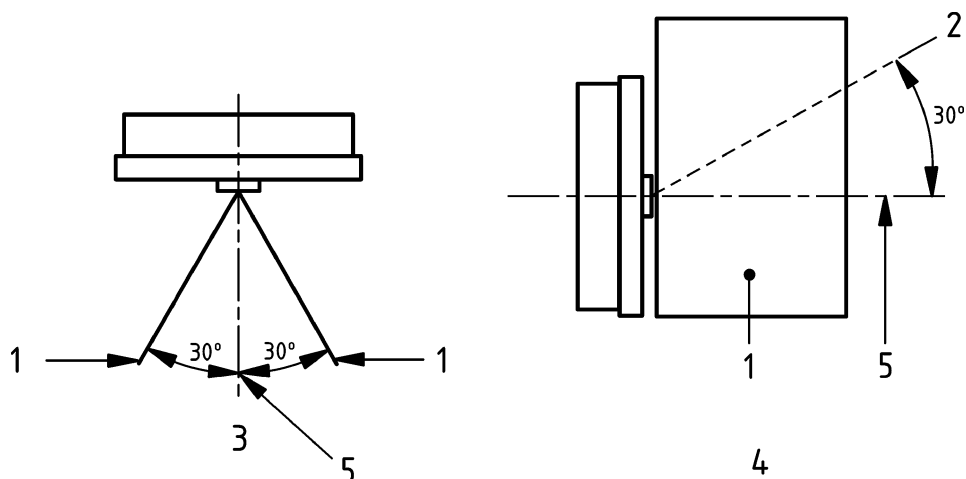
**8.2.4.2.3 Zwei Schirme**, mit denen ein begrenzter Ausspäh-Winkel bestimmt werden kann.

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° vor dem Prüfmuster positioniert. Während die Codes eingegeben werden, ist festzustellen und aufzuzeichnen, ob Eingabeinformationen in einem vertikalen Winkel von 30° von der Mittellinie des Prüfmusters 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**