SLOVENSKI STANDARD
SIST ENV 1300:1999

01-julij-1999

Varnostne shranjevalne enote – Klasifikacija visoko varnostnih ključavnic po odpornosti proti nepooblaščenemu odpiranju

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

Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen

Unités de stockage en lieux surs - Classification des serrures haute sécurité en fonction de leur résistance a l'effraction

Ta slovenski standard je istoveten z: **ENV 1300:1999**

ICS:

13.310	Varstvo pred kriminalom	Protection against crime
35.220.99	Druge naprave za shranjevanje podatkov	Other data storage devices

SIST ENV 1300:1999 **de**

EUROPÄISCHE VORNORM
EUROPEAN PRESTANDARD
PRÉNORME EUROPÉENNE

ENV 1300

Februar 1999

ICS 13.310

Deskriptoren: Geldschrank, Lagermöbel, Magazinierung, Sicherung, Einbruchhemmung, Sicherheitsschlenk, Code, Anforderung, Bezeichnung, Klassifikation, Prüfung, Kennzeichnung

Deutsche Fassung

Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen

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

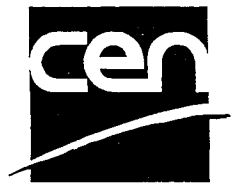
Unités de stockage en lieux sûrs - Classification des serrures haute sécurité en fonction de leur résistance à l'effraction

Diese Europäische Vornorm (ENV) wurde vom CEN am 17.Januar 1999 als eine künftige Norm zur vorläufigen Anwendung angenommen.

Die Gültigkeitsdauer dieser ENV ist zunächst auf drei Jahre begrenzt. Nach zwei Jahren werden die Mitglieder des CEN gebeten, ihre Stellungnahmen abzugeben, insbesondere über die Frage, ob die ENV in eine Europäische Norm umgewandelt werden kann.

Die CEN Mitglieder sind verpflichtet, das Vorhandensein dieser ENV in der gleichen Weise wie bei einer EN anzukündigen und die ENV auf nationaler Ebene unverzüglich in geeigneter Weise verfügbar zu machen. Es ist zulässig, entgegenstehende nationale Normen bis zur Entscheidung über eine mögliche Umwandlung der ENV in eine EN (parallel zur ENV) beizubehalten.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, der Tschechischen Republik und dem Vereinigten Königreich.



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

Zentralsekretariat: rue de Stassart, 36 B-1050 Brüssel

Inhalt **Seite**

Vorwort

Diese Europäische Vornorm wurde vom Technischen Komitee CEN/TC 263 "Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern" erarbeitet, dessen Sekretariat vom BSI gehalten wird.

Diese Europäische Norm wurde von einer Arbeitsgruppe (3) des CEN/TC 263 im Rahmen einer Normenreihe zu Wertbehältnissen erarbeitet. Weitere Normen dieser Reihe tragen folgende Titel oder befinden sich noch in Vorbereitung:

EN 1047-1 Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand. Teil 1: Datensicherungsschränke

prEN 1047-2 Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand. Teil 1: Datensicherungsräume

EN 1143-1 Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl - Teil 1: Geldschränke, Tresorraumtüren und Tresorräume

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

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu

übernehmen: Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, die Tschechische Republik und das Vereinigte Königreich.

1. Anwendungsbereich

Diese Europäische Norm legt die Anforderungen an Hochsicherheitsschlösser hinsichtlich ihrer Zuverlässigkeit und ihres Widerstandswertes gegen zerstörende Angriffe und gegen unbefugtes Öffnen sowie die Prüfverfahren fest. Außerdem wird ein Schema zur Klassifizierung von Hochsicherheitsschlössern gemäß ihrem Sicherheitswert gegeben.

Sie gilt für mechanische und elektronische Hochsicherheitsschlösser. Sie gilt nicht für Sonderoptionen, die die Gesamtsicherheit eines Systems erhöhen können, wie

1) Mastercode zur Verhinderung einer Codeänderung und/oder der Freigabe / Sperrung eines Parallelcodes.
2) Zeitcode zur Freigabe einer Zeitschloßfunktion
3) Einbau von Bauteilen oder Funktionen einer Alarmanlage
4) Funktionen zur Fernsteuerung und -überwachung
5) Widerstand gegen Angriffe mit Säuren
6) Widerstand gegen Röntgendurchstrahlung
7) Widerstand gegen Angriffe mit Sprengstoffen

2. Normative Verweisungen

Diese Europäische Vornorm enthält durch datierte oder undatierte Verweisungen Festlegungen aus anderen Publikationen. Diese normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert und die Publikationen sind nachstehend aufgeführt. Bei starren Verweisungen gehören spätere Änderungen oder Überarbeitungen dieser Publikationen nur zu dieser Europäischen Vornorm, falls sie durch Änderung oder Überarbeitung eingearbeitet sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation.

IEC 68-2-6:1995	Umweltprüfungen - Teil 2: Prüfung Fc: Schwingen (sinusförmig)
EN 50130-4:1995	Alarmsysteme - Teil 4: Elektromagnetische Verträglichkeit - Produktfamiliennorm: Anforderungen an die Störfestigkeit von

	Anlageteilen für Brand- und Einbruchmeldeanlagen sowie Personen-Hilferufanlagen
IEC 1000-4-2:1995	Elektromagnetische Verträglichkeit (EMV) - Teil 4: Prüf- und Meßverfahren Hauptabschnitt 2: Prüfung der Störfestigkeit gegen Entladung statischer Elektrizität
IEC 1000-4-3:1995	Elektromagnetische Verträglichkeit (EMV) - Teil 4: Prüf- und Meßverfahren Hauptaschnitt 3: Störfestigkeit gegen hochfrequente elektromagnetische Felder
IEC 1000-4-4:1995	Elektromagnetische Verträglichkeit (EMV) - Teil 4: Prüf- und Meßverfahren Hauptabschnitt 4: Prüfung der Störfestigkeit gegen schnelle transiente elektrische Störgrößen / Burst
IEC 1000-4-5:1995	Elektromagnetische Verträglichkeit (EMV) - Teil 4: Prüf- und Meßverfahren Hauptabschnitt 5: Prüfung der Störfestigkeit gegen Stoßspannungen
IEC 1000-4-6:1995	Elektromagnetische Verträglichkeit (EMV) - Teil 4: Prüf- und Meßverfahren Hauptabschnitt 6: Störfestigkeit gegen leitungsgeführte Störgrößen, induziert durch hochfrequente Felder
IEC 1000-4-11:1994	Elektromagnetische Verträglichkeit (EMV) - Teil 4: Prüf- und Meßverfahren Hauptabschnitt 11: Prüfung der Störfestigkeit gegen Spannungseinbrüche, Kurzzeitunterbrechungen und Spannungsschwankungen
EN 1143-1:1996	Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandswertes gegen Einbruchdiebstahl - Teil 1: Geldschränke, Tresorraumtüren und Tresorräume
EN 50081-1:1992	Elektromagnetische Verträglichkeit (EMV) - Fachgrundnorm Störaussendung - Teil 1: Wohnbereich, Geschäfts- und Gewerbebereiche sowie Kleinbetriebe
ISO 6988:1985	Metallische und andere anorganische Überzüge - Schwefeldioxyd-Prüfung mit allgemeiner Feuchtigkeitskondensation

3. Definitionen

Für die Anwendung dieser Norm gelten folgende Definitionen:

3.1 Hochsicherheitsschloß: Unabhängige Einheit, die gewöhnlich an Türen von Wertbehältnissen angebracht ist. In diese Einheit kann die Eingabe eines Codes erfolgen, der dann mit einem gespeicherten Code verglichen wird. 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 Hochsicherheitsschloß ermöglicht, den Sicherheitszustand des Schlosses zu ändern.

3.2.1 Öffnungscode: Identifikationsinformation, die ein Entsperren des Hochsicherheitsschlosses gestattet.

3.2.2 Berechtigungscode: Identifikationsinformation, die einen Zugang zur Verarbeitungseinheit gestattet. Der Berechtigungscode kann auch der Öffnungscode sein.

3.2.3 Überfallcode: Parallelcode, der zusätzliche Funktionen aktiviert.

3.3 Codierarten: Alle 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 sich aus charakteristischen physischen Merkmalen des Menschen ergibt.

3.4 Verarbeitungseinheit: Teileinheit, die auswertet, ob der eingegebene Code richtig ist und die Bewegung einer Sperreinheit freigibt oder sie verhindert.

3.5 Sperreinheit: Teil eines Hochsicherheitsschlosses, das die Bewegung der Blockier-einheit freigibt oder sie verhindert.

3.6 Codeträger: Gegenstand, dessen physische Form oder physikalische Eigenschaften den Eingabecode bestimmen, z.B. ein Schlüssel.

3.7 Mechanisches Hochsicherheitsschloß: Hochsicherheitsschloß, das nur durch mechanische Elemente gesichert wird.

3.8 Elektronisches Hochsicherheitsschloß: Hochsicherheitsschloß, das teilweise oder vollständig durch elektrische oder elektronische Elemente gesichert wird.

3.9 Blockiereinheit: Teil eines Hochsicherheitsschlosses, das sich nach Eingabe des richtigen Öffnungscodes bewegt oder bewegt werden kann, um entweder eine Tür zu sichern oder die Bewegung eines Riegelwerks zu verhindern. Ein Beispiel für eine Blockiereinheit ist der Riegel eines mechanischen Schlosses.

3.10 Zerstörender Angriff: Angriff, der an einem Hochsicherheitsschloß Schäden verursacht, die irreversibel sind und vor dem rechtmäßigen Benutzer nicht verborgen werden können.

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

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

ANMERKUNG: Nach einer Manipulation kann ein Hochsicherheitsschloß funktionsfähig bleiben, obwohl sein Sicherheitswert dauerhaft beeinträchtigt sein kann.

3.13 Ausspähen: Angriff, der auf eine Feststellung des richtigen Codes abzielt, ohne daß dabei direkter Zugriff - auch nicht mit einem Werkzeug - auf das Hochsicherheitsschloß besteht.

3.14 Nutzbare Codes: Codes oder Codeträger, die vom Hersteller zugelassen sind und die den Anforderungen dieser Norm entsprechen.

ANMERKUNG: Bei mechanischen Hochsicherheitsschlössern ist im allgemeinen die Anzahl der nutzbaren Codes weit geringer als die Gesamtzahl der Codes, auf die das Hochsicherheitsschloß eingestellt werden kann.

3.15 Überwachung: Ausspähen oder unbefugtes Erkennen der Codeeingabe mit beliebigen Hilfsmitteln einschließlich der Nutzung von Instrumenten.

3.16 Beobachtung: Ausspähen oder unbefugtes Erkennen der Codeeingabe mit den menschlichen Sinnen.

3.17 Verworfen-Zustand: Zustand, bei dem sich die Codierungselemente nicht in der Anordnung befinden, die erforderlich ist, um das Hochsicherheitsschloß 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: Die Tür liegt nicht im Rahmen.

3.20 Geschlossene Tür: Die Tür liegt im Rahmen, der/die Riegel können jetzt ausgefahren werden.

3.21 Verriegelte Tür: Die Riegel sind ausgefahren.

3.22 Gesperrte Tür: Das Riegelwerk kann nicht eingefahren werden, weil es vom Hochsicherheitsschloß blockiert wird.

3.23 Gesicherte Tür: Die Tür ist geschlossen, verriegelt und mit einem Hochsicherheits-schloß , das sich im gesicherten Zustand befindet, gesperrt.

3.24 Hochsicherheitsschloß im gesicherten Zustand: Die Blockiereinheit ist ausgefahren und kann nur nach Eingabe des/der Öffnungscodes wieder eingefahren werden.

3.2.5 **Normalzustand:** Das Hochsicherheitsschloß befindet sich nach einer Prüfung im gesicherten Zustand und alle Schloßfunktionen können ausgeführt werden.

3.26 **Funktionsfähig:** Das Hochsicherheitsschloß befindet sich nach einer Prüfung im gesicherten Zustand und kann mit dem (den) Öffnungscode(s) entsperrt werden, es sind aber nicht alle Schloßfunktionen ausführbar.

3.27 **Sicherheit bei Ausfall:** Das Hochsicherheitsschloß befindet sich nach einer Prüfung im gesicherten Zustand, es kann mit dem (den) Öffnungscode(s) aber nicht mehr entsperrt werden.

4. Klassifizierung

Aufgrund der Sicherheitsanforderungen erfolgt bei Hochsicherheitsschlössern die Klassifizierung in die Schloßklassen A, B, C und D gemäß den Tabellen 1, 2 und 3. Allgemeine Anforderungen (siehe **5.1**) und Zuverlässigkeitsanforderungen (siehe **5.3**) müssen erfüllt sein.

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

5. Anforderungen

5.1 Allgemeine Anforderungen an alle Hochsicherheitsschlösser

5.1.1.1 Der (die) Öffnungscode(s) müssen so lange als allein gültige Codes erhalten bleiben, bis sie absichtlich umgestellt werden. Die Bewertung erfolgt gemäß **8.1.2**.

5.1.1.2 Es darf nicht möglich sein, daß durch zusätzliche vom Schloßhersteller eingebaute Vorrichtungen (z.B. Mikroschalter) Informationen über den Code gewonnen werden können. Die Bewertung erfolgt gemäß **8.1.2.**

5.1.1.3 Hochsicherheitsschlösser müssen eine Blockiereinheit enthalten oder die Bewegung einer Blockiereinheit steuern können.

5.1.1.4 Wird die Blockiereinheit nicht manuell bewegt, so muß auf irgendeine Weise angezeigt werden, ob sich das Hochsicherheitsschloß im gesicherten Zustand befindet (gesperrt und verworfen).

5.1.1.5 Es darf nicht möglich sein, einen Öffnungscode zu ändern, ohne einen Autorisierungscode einzugeben. Die Bewertung erfolgt gemäß **8.1.2**.

5.1.2 Hochsicherheitsschlösser der Klasse D

5.1.2.1 Es müssen Mittel zur Verfügung stehen, die den Verschlußzustand des Schlosses, ob gesperrt oder entsperrt, anzeigen.

> ANMERKUNG: Bei Schlüsselschlössern kann dies dadurch erfolgen, daß der Schlüssel nur in gesperrtem Zustand des Schlosses abgezogen werden kann

5.1.2.2 Das Hochsicherheitsschloß muß sich nach dem Sperren im Verworfen-Zustand befinden. Die Bewertung erfolgt gemäß **8.1.2**.

5.1.2.3 Das Hochsicherheitsschloß muß eine Vorrichtung enthalten, die den Verworfen-Zustand anzeigt.

5.1.3 Hochsicherheitsschlösser mit Codeträger

5.1.3.1 Bei Hochsicherheitsschlössern der Klasse A (siehe **Abschnitt 4**) darf der gleiche Code erst dann wiederholt werden, wenn mindestens 80% der nutzbaren Codes schon verwendet wurden. Die Bewertung erfolgt gemäß **8.1.2**.

5.1.3.2 Codes (und gleichschließende Codeträger) müssen nach einem Zufallsverfahren ausgewählt werden. Die Bewertung erfolgt gemäß **8.1.2**.

5.1.3.3 Weder auf dem Codeträger noch auf dem Hochsicherheitsschloß dürfen sich eine Nummer oder eine Kennzeichnung befinden, mit denen sich der Code feststellen läßt. Die Bewertung erfolgt gemäß **8.1.2**.

5.1.4 Codierungsstufen für mechanische Schlüsselschlösser

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

5.1.4.2 Bei nutzbaren Codes dürfen höchstens zwei gleiche Codierungsstufen einander benachbart sein.

5.1.4.3 Bei nutzbaren Codes muß der Unterschied zwischen der höchsten und tiefsten Codierungsstufe größer als 60% des größtmöglichen Stufensprungs des Hochsicherheits-schlosses sein.

5.1.5 Elektronische Hochsicherheitsschlösser

5.1.5.1 Bei elektronischen Hochsicherheitsschlössern mit Parallelcode muß die in Tabelle 1 aufgeführte Anzahl der letzten Öffnungscodes gespeichert werden. Die gespeicherten Daten müssen selbst bei Stromausfall mindestens 1 Jahr erhalten bleiben.

5.1.5.2 Bei elektronischen Hochsicherheitsschlössern in gesichertem Zustand darf ein Datenverkehr mit der Verarbeitungseinheit nur möglich sein zur Eingabe des Öffnungscodes und Anzeige des Schloßzustandes.

5.1.5.3 Bei elektronischen Hochsicherheitsschlössern der Klassen C und D muß die Eingabeeinheit fest an der Tür oder der Türzarge befestigt sein. Es darf nicht möglich sein, die Eingabeeinheit gewaltsam zu entfernen, ohne daß für den Nutzer offensichtliche dauerhafte Spuren oder Beschädigungen entstehen oder es dem Nutzer angezeigt wird. Die Prüfung erfolgt gemäß **8.1.2**.

5.1.5.4 Bei elektronischen Hochsicherheitsschlössern der Klassen B, C und D darf keine Zugriffsmöglichkeit auf sicherheitsempfindliche Teile der Eingabeeinheit bestehen, ohne daß für den Nutzer offensichtliche dauerhafte Spuren oder Beschädigungen entstehen oder es dem Nutzer angezeigt wird. Die Prüfung erfolgt gemäß **8.1.2**.

5.1.5.5 Bei elektronischen Hochsicherheitsschlössern der Klassen A und B kann die Eingabeeinheit vom Schloß getrennt sein. Sie sollte dann aber mit einem abgeschirmten Kabel mit einer maximalen Länge von 1 m dauerhaft und sichtbar mit der Tür oder dem Türrahmen verbunden sein. Die Prüfung erfolgt gemäß **8.1.2**.

5.2 Sicherheitsanforderungen

5.2.1 Nutzbare Codes

Die Mindestzahl der nutzbaren Codes für alle Klassen und Arten von Hochsicherheitsschlössern muß den Werten von Tabelle 1 entsprechen. Die Prüfung erfolgt gemäß **8.2.1**.

Mechanische Schlüsselschlösser dürfen von den zusätzlichen Schlüsseln (siehe **7.3**) nicht entsperrt werden.

5.2.2 Hochsicherheitsschlösser mit Parallelschloß

Bei Hochsicherheitsschlössern mit einem Parallelschloß (z.B. ein elektronisches Hochsicherheitsschloß parallel mit einem mechanischen Hochsicherheitsschloß) erfolgt die Klassifizierung nach dem Schloß mit dem geringsten Sicherheitswert.

5.2.3 Widerstand gegen Manipulation

5.2.3.1 Höchstwerte für Öffnungsversuche

Die zulässige maximale Anzahl von Öffnungsversuchen pro Stunde muß den Werten in Tabelle 1 entsprechen.

> ANMERKUNG: Tabelle 1 enthält für mechanische Hochsicherheitsschlösser mit Codeträgern keine Anforderungen an die Anzahl der Öffnungsversuche, weil der Zeitaufwand für die Änderung der Codeträger die Anzahl der Öffnungsversuche ausreichend begrenzt.

5.2.3.2 Manipulation

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

5.2.4 Widerstand gegen zerstörende Angriffe

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

5.2.5 Widerstand gegen Ausspähen

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

5.2.5.2 Bei Hochsicherheitsschlössern der Klassen C und D darf der Winkelbereich, in dem die Codeinformation optisch beobachtet werden kann, nicht größer als 30° sein, gemessen von der Mittellinie aus in der Horizontalebene (d.h. 60° Gesamtwinkel; siehe **8.2.4**).

5.2.6 Widerstand gegen elektrische und elektromagnetische Einflüsse

5.2.6.1 Elektronische Hochsicherheitsschlösser, die aus dem Netz gespeist werden, müssen bei Spannungsschwankungen, Spannungseinbrüchen und Kurzzeitunterbrechungen im Normalzustand bleiben. Die Prüfung erfolgt gemäß **8.2.5.6**.

Befindet sich ein elektronisches Schloß im gesicherten Zustand, so muß es bei einem Ausfall der Versorgungsspannung auch gesichert bleiben (siehe **8.2.5.3**).

Netzbetriebene Hochsicherheitsschlösser müssen bei einem bis zu 12 Stunden dauernden Ausfall der Netzversorgung im gesicherten Zustand bleiben (siehe **8.2.5.4**).

5.2.6.2 Elektronische Hochsicherheitsschlösser müssen bei der Prüfung ihrer Widerstandsfähigkeit gegen elektrostatische Entladung die Anforderungen gemäß Tabelle 2 erfüllen. Während der Prüfung dürfen die Prüfmuster höchstens 5 ms lang in den ungesicherten Zustand gehen. Die Prüfung erfolgt gemäß **8.2.5.7**.

5.2.6.3 Bei der Prüfung der Widerstandsfähigkeit von elektronischen Hochsicherheitsschlössern gegen eingestrahlte elektromagnetische Felder müssen die Anforderungen der Tabelle 2 erfüllt werden. Die Prüfung erfolgt gemäß **8.2.5.9**.

5.2.6.4 Bei der Prüfung der Widerstandsfähigkeit von netzbetriebenen elektronischen Hochsicherheitsschlössern gegen schnelle transiente elektrische Störgrößen (Burst) müssen die Anforderungen der Tabelle 2 erfüllt werden. Während der Prüfung dürfen die Prüfmuster höchstens 5 ms lang in den ungesicherten Zustand gehen. Die Prüfung erfolgt gemäß **8.2.5.8**.