

DIN EN 17646

ICS 13.310

**Wertbehälter –
Klassifizierung von Hochsicherheitsschlössern nach ihrem
Widerstandswert gegen unbefugtes Öffnen –
Verteilte Systeme;
Deutsche Fassung EN 17646:2022**

Secure storage units –
Classification for high security locks according to their resistance to unauthorized opening –
Distributed systems;
German version EN 17646:2022

Unités de stockage en lieu sûr –
Classification des serrures haute sécurité en fonction de leur résistance à l'effraction –
Systèmes répartis;
Version allemande EN 17646:2022

Gesamtumfang 31 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

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

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

Deutsche Fassung

Wertbehältnisse —
Klassifizierung von Hochsicherheitsschlössern nach ihrem
Widerstandswert gegen unbefugtes Öffnen —
Verteilte Systeme

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

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

Diese Europäische Norm wurde vom CEN am 27. Juni 2022 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



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

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Symbole und Abkürzungen	8
5 Klassifizierung	8
6 Anforderungen	9
6.1 Allgemeines	9
6.1.1 Allgemeines	9
6.1.2 Aufbau	9
6.2 Systemverwaltung	10
6.2.1 Verwaltungsvorgänge	10
6.2.2 Bestätigung von ferngesteuert eingeleiteten sicherheitsrelevanten Bedienvorgängen .	11
6.2.3 Informationsverarbeitendes System als zentrale Bedien-/Verwaltungsinstanz	11
6.2.4 Authentifizierung von Komponenten	12
6.2.5 Software und Firmware	12
6.2.6 Administrationsschnittstellen	14
6.2.7 Authentifizierung von Benutzern	14
6.2.8 Anzeige des Verriegelungszustandes	16
6.2.9 Aufzeichnung von Ereignissen	16
6.2.10 Datenverkehr im gesicherten Zustand	18
6.2.11 Erkennung von Manipulationen	18
6.2.12 Anzeige der Sperrzeiten	19
6.2.13 Widerstand gegen Ausspähen	19
6.3 Informationssicherheit	20
6.3.1 Allgemeine Schutzziele	20
6.3.2 Anforderungen an die Kryptographie	20
6.3.3 Weitere Maßnahmen zur Informationssicherheit	23
6.4 Sicherheitsanforderungen	24
6.4.1 Negative Einflüsse durch die Stromversorgung	24
6.4.2 Widerstand gegen elektrische und elektromagnetische Einflüsse	24
6.4.3 Widerstand gegen physikalische Umwelteinflüsse	24
6.4.4 Temperaturwiderstand	24
6.4.5 Zuverlässigkeit	24
6.5 Fremdkomponenten	24
6.5.1 Verwendung von Fremdkomponenten	24
6.5.2 Zusätzliche Komponenten	25
7 Technische Dokumentation	25
7.1 Allgemeines	25
7.2 Benötigte technische Dokumentation	25
7.3 Betriebshinweise	26
8 Prüfmuster	27
9 Kennzeichnung	27

Anhang A (normativ) Bestimmung des Einbruchwiderstandes aufgrund von konstruktiven Anforderungen 28

A.1 Allgemeines 28

A.2 Elektronisches HSS als Teil eines Verteilten Systems.....28

Literaturhinweise.....29

Europäisches Vorwort

Dieses Dokument (EN 17646:2022) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat von BSI gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2023, und etwaige entgegenstehende nationale Normen müssen bis Februar 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

1 Anwendungsbereich

Dieses Dokument gilt für Verteilte Systeme (VS), d.h. für Hochsicherheitsschlösser mit Komponenten, die über ein drahtgebundenes oder drahtloses Übertragungssystem verbunden sind, um festgelegte Bedienvorgänge unter Nutzung unterschiedlicher, individuell festgelegter Zugriffsmöglichkeiten auszuführen.

Produkte, die auf Basis dieses Dokuments geprüft werden, entsprechen dem zum Zeitpunkt der Prüfung allgemein anerkannten Stand der Technik. Aufgrund der kurzen Innovationszyklen im Bereich elektronischer und insbesondere informationstechnischer Anwendungen sollten auch die zum Zeitpunkt der Produktentwicklung aktuellen technischen Möglichkeiten bei der Realisierung berücksichtigt werden.

Verteilte Systeme können u.a. zur Betätigung von Hochsicherheitsschlössern (HSS) von Wertbehältnissen (Wertschutzschränke und Wertschutzräume) eingesetzt werden.

Hochsicherheitsschlösser (HSS) werden in einem VS als Sperreinheit eingesetzt.

Dieses Dokument gilt nicht für autonom betriebene HSS, die nicht Teil eines Verteilten Systems sind. Für diese autonomen HSS ist nur die EN 1300 anwendbar.

Da sich sowohl die Forschung im Bereich der Kryptographie und relevanter Angriffe als auch in Bezug genommene Normen sehr schnell entwickeln, erfolgt eine Überarbeitung dieses Dokuments alle drei Jahre.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 1300, *Wertbehältnisse — Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen*

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 ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001)*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach EN 1300 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

— ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1

abgesetzte Eingabeeinheit

aEE

zusätzliche Komponente, die die Eingabe von Informationen von einer entfernten Stelle ermöglicht und die für eine ausschließliche Verwendung in einem Verteilten System vorgesehen ist

Anmerkung 1 zum Begriff: Eingabeeinheiten (EE) werden in der EN 1300 definiert.

3.2

Auslieferungszustand

Zustand eines VS oder eines Bestandteils eines VS, bevor die erste kundenspezifische Modifikation vorgenommen wurde, mit Ausnahme von Software/Firmware-Updates, die in Kraft bleiben können

3.3

Authentizität

Eigenschaft, die gewährleistet, dass z. B. ein Kommunikationspartner derjenige ist, der er vorgibt zu sein; bei authentischen Informationen ist sichergestellt, dass diese von der angegebenen Quelle erstellt wurden

3.4

Authentisierungsfaktor

Berechtigungsnachweisart (Faktoren, die auf Wissen (z. B. Passwort), Besitz (z. B. eine Karte) oder Inhärenz (z. B. biometrische Merkmale) beruhen), die eine Verifizierung vornimmt, dass eine Entität, die einen Zugang erhalten möchte, diejenige ist, die sie vorgibt

3.5

autorisierter Benutzer

Person, die sich durch Eingabe einer erforderlichen Information für eine bestimmte Aktion als berechtigt ausweist

3.6

eigenständige Komponente

Komponente eines VS, die aktiv Einfluss auf die Datenverarbeitung sowie auf den Sicherheitszustand vom VS hat und die absolut notwendig für die bestimmungsgemäße Verwendung eines VS ist

3.7

Fremdkomponente

FK

Komponente eines VS, die nicht speziell für das VS hergestellt wurde, aber in einem VS als Funktionseinheit eingesetzt wird

Anmerkung 1 zum Begriff: Öffentliche Teile des Übertragungsweges oder eingesetzte Office-Computer können beispielsweise als Fremdkomponente eingesetzt werden.

3.8

informationsverarbeitendes System

IvS

System zur Verarbeitung, Verwaltung und/oder Speicherung von Informationen

Anmerkung 1 zum Begriff: Um das Risiko des unberechtigten Zugriffs auf sicherheitsrelevante Informationen durch Dritte zu reduzieren, wird dringend empfohlen, ein IvS ausschließlich im unmittelbaren Einflussbereich des Betreibers einzusetzen.

3.9

Kommunikationsweg

KW

Übertragungsweg zum Informationsaustausch zwischen der abgesetzten Eingabeeinheit und der Auswerteeinrichtung einschließlich zwischengelagerter informationsverarbeitender Systeme

3.10

Authentifizierung von Komponenten

Kopplung zweier Kommunikationspartner unter Zuhilfenahme eindeutiger Identifikationsmerkmale

3.11

sicherheitsrelevante Information

Code (z. B. Öffnungs-, Berechtigungs-, Überfall-, Parallelcodes, kryptographische Schlüssel), Authentifizierungsinformation (z. B. Passwörter), Daten zu Software-/Firmware-Updates

3.12

Sperreinheit

SE

Komponente, die mittelbar oder unmittelbar die physikalische Sperre (Verriegelung) weiterer Einheiten, z. B. einer Tür oder eines Riegelwerks, ermöglicht

3.13

Überwachungseintrag

gespeicherte Information zu einem definierten Ereignis innerhalb des VS mit Angabe von:

- auslösendem Ereignis;
- Uhrzeit/Datum des Ereignisses;
- auslösender Benutzer/auslösende Komponente.

3.14

Verteiltes System

VS

als Einheit funktionierende örtlich getrennte Komponenten, die auf die systematische Umsetzung eines einheitlichen Ziels ausgerichtet sind

Anmerkung 1 zum Begriff: Der Informationsaustausch zwischen den Komponenten kann drahtgebunden oder drahtlos erfolgen.

3.15

willentliche Handlung

bewusste Aktion einer Person zur Bestätigung einer Statusänderung

Anmerkung 1 zum Begriff: Eine willentliche Handlung kann z. B. das Drücken eines Bedienknopfes, die Eingabe eines (Bestätigungs-)Codes oder das Drehen eines Handgriffes sein.

3.16

zugriffsgeschützter Bereich

Bereich eines Wertbehältnisses, der durch die physikalischen Eigenschaften des Produktes nicht im geschlossenen Zustand und im geöffneten Zustand nicht spurenlos zugänglich ist

Anmerkung 1 zum Begriff: Dies kann z. B. das Innere einer Wertbehältnistür sein, die auch bei offener Tür durch eine mechanische Abdeckung geschützt ist.

3.17

Zwei-Faktor-Authentifizierung

Art der Authentifizierung von Benutzern, eines Services oder einer Komponente mittels zwei unterschiedlichen Authentisierungsfaktoren

Anmerkung 1 zum Begriff: Beispiele von Authentisierungsfaktoren werden in deren Definition aufgeführt.

4 Symbole und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Symbole und Abkürzungen.

AE:	Auswerteeinheit
aEE:	abgesetzte Eingabeeinheit
ANSSI:	Agence nationale de la sécurité des systèmes d'information (National Cybersecurity Agency of France)
BSI (DE):	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
EE:	Eingabeeinheit
ENISA:	European Union Agency for Network and Information Security
FK:	Fremdkomponente
HSS:	Hochsicherheitsschloss
IvS:	Informationsverarbeitendes System
KW:	Kommunikationsweg
NIST:	National Institute of Standards and Technology
SE:	Sperreinheit
VS:	Verteiltes System

5 Klassifizierung

Verteilte Systeme werden in die vier Klassen A(DS), B(DS), C(DS) und D(DS) eingeteilt. Für VS der Klasse A(DS) gelten die geringsten, für solche der Klasse D(DS) die höchsten Anforderungen.

Bei einem zugelassenen Verteilten System bestimmt die Komponente mit der niedrigsten Klasse bezogen auf die SE, AE, EE und aEE die Klasse des gesamten Verteilten Systems.