

DIN EN 17646

ICS 13.310

Einsprüche bis 2021-04-12

Entwurf

**Wertbehältnisse –
Klassifizierung von Hochsicherheitsschlössern nach ihrem
Widerstandswert gegen unbefugtes Öffnen –
Verteilte Systeme;
Deutsche und Englische Fassung prEN 17646:2021**

Secure storage units –

Classification for high security locks according to their resistance to unauthorized opening –

Distributed systems;

German and English version prEN 17646:2021

Unités de stockage en lieu sûr –

Classification des serrures haute sécurité en fonction de leur résistance à l'effraction –

Systèmes répartis;

Version allemande et anglaise prEN 17646:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-02-12 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

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

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

Gesamtumfang 59 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Dieses Dokument (prEN 17646:2021) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat von BSI (Vereinigtes Königreich) gehalten wird.

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

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

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

<i>Titel de:</i>	Wertbehältnisse — Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen — Verteilte Systeme
<i>Titel en:</i>	Secure storage units — Classification for high security locks according to their resistance to unauthorized opening — Distributed systems
<i>Titel fr:</i>	Unités de stockage en lieu sûr — Classification des serrures haute sécurité en fonction de leur résistance à l'effraction — Systèmes répartis

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 remote 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	18
6.2.13 Widerstand gegen Ausspähen	18
6.3 Informationssicherheit	20
6.3.1 Allgemeine Schutzziele	20
6.3.2 Anforderungen an die Kryptografie	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 (prEN 17646:2021) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat von BSI gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

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 werden auch die zum Zeitpunkt der Produktentwicklung aktuellen technischen Möglichkeiten bei der Realisierung berücksichtigt.

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 dieser Norm 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*

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:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

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
Authentifizierungsfaktor
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, die 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 DS 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, 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, kryptografische 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 nicht im geöffneten Zustand spurlos 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 Authentifizierungsfaktoren

Anmerkung 1 zum Begriff: Beispiele von Authentifizierungsfaktoren sind in der dazugehörigen Definition angegeben.

4 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
EMA:	Einbruchmeldeanlage
ENISA:	European Union Agency for Network and Information Security
FK:	Fremdkomponente
HSS:	Hochsicherheitsschloss
IvS:	Informationsverarbeitendes System
KW:	Kommunikationsweg
NIST:	Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways
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 genehmigten verteilten System bestimmt die Komponente mit der niedrigsten Klasse bezogen auf die SE, AE, EE und aEE die Klasse des gesamten verteilten Systems.

6 Anforderungen

6.1 Allgemeines

6.1.1 Allgemeines

Für HSS, die in einem VS nach diesem Dokument benutzt werden, sind im Allgemeinen die Anforderungen der EN 1300 maßgebend. Die Klassifizierungsstufe, die nach der EN 1300 von einem HSS erreicht wird, bestimmt die maximal mögliche Klasse von dieser Norm (siehe Tabelle 1).

Tabelle 1 — Verbindung zwischen EN 1300 und diesem Dokument

Klassen von diesem Dokument	Die Anforderungen der folgenden Klassen nach EN 1300 müssen erfüllt werden
A (DS)	A, B, C oder D
B (DS)	B, C oder D
C (DS)	C oder D
D (DS)	D

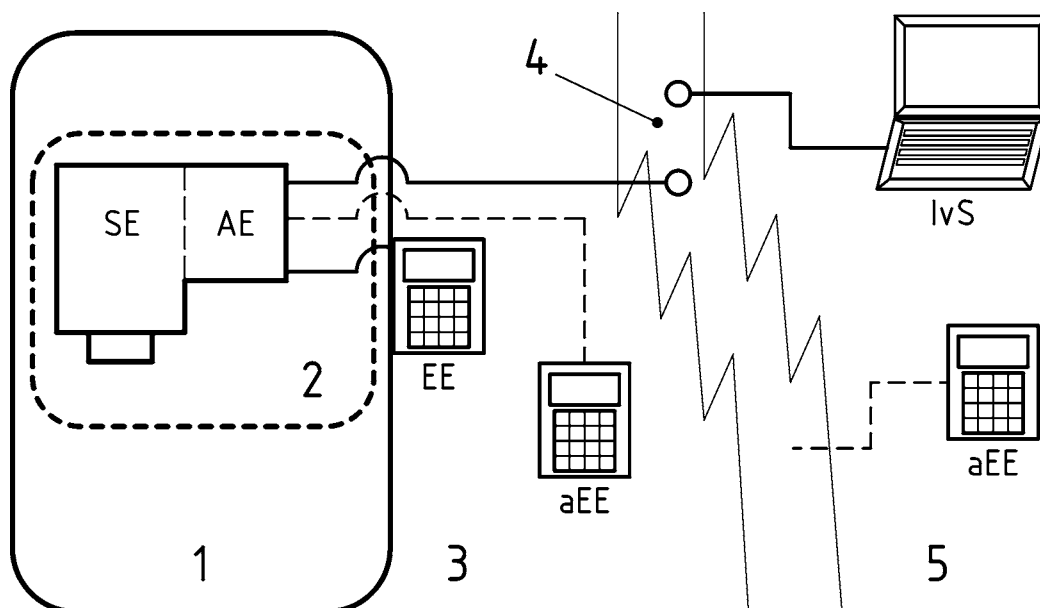
Im Fall von widersprüchlichen Anforderungen zwischen der EN 1300 und diesem Dokument ist dieses Dokument maßgebend. Soweit möglich und zutreffend wird auf entsprechende Kapitel der EN 1300 verwiesen.

Dieses Dokument legt Anforderungen an eigenständige Komponenten (siehe 6.2 bis 6.4) sowie Fremdkomponenten (siehe 6.5) fest. Soweit möglich und zutreffend wird auf entsprechende Kapitel der EN 1300 verwiesen.

Dieses Dokument verweist auf den Stand der Technik. Mit Stand der Technik ist eine Methode gemeint, die von anerkannten Organisationen wie der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI), der französischen Nationalen Agentur für Sicherheit der Informationssysteme (ANSSI) oder dem Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways validiert ist.

6.1.2 Aufbau

Beim VS wird von einer Grundstruktur, bestehend aus Auswerteeinheit (AE) und Sperreinheit (SE), einer Eingabeeinheit (EE) sowie den Kommunikationswegen (KW), die über öffentliche oder lokale Netze laufen können und ggf. einem Informationsverarbeitenden System (IvS) oder einer abgesetzten Eingabeeinheit (aEE) oder beidem ausgegangen. Die genannten Elemente können auch mehrfach im System vorkommen. Die Struktur ist nicht detailliert vorgegeben, orientiert sich jedoch an der Darstellung in Bild 1.



Legende

- 1 Wertbehälter
- 2 Zugriffsgeschützter Bereich
- 3 Lokaler Bereich
- 4 Netzwerk
- 5 Abgesetzter Bereich

Bild 1 — Prinzip eines verteilten Systems

Eigenständige Komponenten mit Ausnahme der EE, der aEE sowie des IvS müssen im zugriffsgeschützten Bereich des VS angeordnet sein.

Die Anordnung der Komponenten muss so erfolgen, dass ein nicht autorisierter Zugriff auf diese Komponenten erkennbar ist (z.B. durch Zerstörung einer Plombe). Dies gilt auch wenn der gesicherte Bereich ordnungsgemäß geöffnet ist.

6.2 Systemverwaltung

6.2.1 Verwaltungsvorgänge

Die das VS betreffenden Konfigurationstätigkeiten und Servicearbeiten, die z. B.

- Initialisierung;
- Konfiguration (z. B. Einbinden neuer Komponenten);
- Einrichtung eines Zeitfensters;
- Öffnungsverzögerung einstellen;
- Nutzerverwaltung;
- Nutzerrechteverwaltung;
- Backup erstellen (und ggf. wiederherstellen);

— ggf. Reset der Hardware

dürfen ausschließlich durch autorisierte Benutzer (nach 6.2.7) durchgeführt werden.

Stellt ein HSS darüber hinaus noch produktspezifische Funktionen zur Verfügung, durch die auf Daten an einem beliebigen Ort des VS zugegriffen werden kann, dürfen diese Funktionen ebenfalls nur von autorisierten Benutzern (nach 6.2.7) ausgeführt werden.

Alle vorgenannten Konfigurationen und Servicearbeiten sowie alle zusätzlichen produktspezifischen Funktionen müssen einen Überwachungseintrag gemäß den Anforderungen in 6.2.9 erzeugen.

Im gesamten System ist die Eingabe von Codes nur über speziell dafür konstruierte und geschützte Komponenten zulässig (EE oder aEE nach 6.2.11).

6.2.2 Bestätigung von remote eingeleiteten sicherheitsrelevanten Bedienvorgängen

Die folgenden sicherheitsrelevanten Bedienvorgänge müssen (wenn diese aus der Ferne eingeleitet werden) durch eine willentliche Handlung eines autorisierten Nutzers an der EE bestätigt werden:

- Kopplung von Komponenten;
- Entsperren des HSS;
- Hardwarekonfiguration bei Erstinbetriebnahme;
- Änderung der Hardware nach der Erstinbetriebnahme;
- Reset des Systems auf den Auslieferungszustand.

Bei den folgenden sicherheitsrelevanten Bedienvorgängen ist es ausreichend, wenn die willentliche Handlung eines autorisierten Benutzers an einem Schloss für dieses Schloss sowie für weitere Schlösser der gleichen oder einer niedrigeren Klasse vorgenommen wird:

- Änderung des Nutzercodes;
- Aktivierung neuer Nutzer.

Die willentliche Handlung muss einen Überwachungseintrag nach 6.2.9 erzeugen.

Die vorgenannten Anforderungen und die daraus resultierende willentliche Handlung muss in den Betriebshinweisen dokumentiert werden.

Bei der Installation von Software/Firmware Updates sind die Anforderungen nach 6.2.5.3 maßgebend.

6.2.3 Informationsverarbeitendes System als zentrale Bedien-/Verwaltungsinstanz

Grundsätzlich können ein oder mehrere IvS zur Übernahme von Bedien- und Verwaltungsvorgängen im VS verwendet werden. Dies kann z. B. sinnvoll sein bei der Verwaltung einer großen Anzahl von Wertschutzschränken mit einer geringen Anzahl von aEE oder der Steuerung des VS von einem zentralen Punkt aus. Das IvS muss in diesem Fall die folgenden Anforderungen erfüllen:

Zur Verarbeitung oder Speicherung von Informationen müssen kryptographische Algorithmen, wie in 6.3.1 und 6.3.2 beschrieben, eingesetzt werden.

Benutzer müssen nach den Anforderungen von 6.2.7 authentifiziert werden.

Der Einsatz und die Verwaltung der Software ist nach den Anforderungen nach 6.2.5 zu erfolgen.

Die Eingabe von Codes an einem IvS darf ausschließlich von autorisierten Benutzern erfolgen und ist nur in Verbindung mit einer aEE möglich.

Das IvS muss einer autorisierten Person (z. B. einem autorisierten Benutzer) die Möglichkeit bieten, eine Vertretung für das gesamte VS-Netzwerk zu erstellen.

ANMERKUNG Die Vertretung im Netzwerk bezieht sich auf alle eigenständigen Komponenten vom VS.

Der Hersteller muss in der technischen Dokumentation die Umsetzung aller Anforderungen beschreiben.

6.2.4 Authentifizierung von Komponenten

Alle eigenständigen Komponenten (siehe 3.6) eines VS müssen in der Lage sein, sich miteinander zu authentifizieren. Der Austausch der für die Authentifizierung benötigten Informationen muss die Kryptographie-Anforderungen der Abschnitte 6.36.3.1 und 6.3.2 erfüllen.

Das Authentifizierungsverfahren muss mittels Methoden implementiert werden, die dem Stand der Technik entsprechen.

Zur Kommunikation zwischen zwei Komponenten ist es notwendig, dass diese sich erfolgreich authentifiziert haben und für den Datenaustausch autorisiert sind.

Wenn das Authentifizierungsverfahren durch einen Benutzer verwaltet werden kann (z. B. (Re-) Initialisierung, Modifizierung oder das Resetten der Authentifizierung einer Komponente), darf dies nur von einem autorisierten Benutzer möglich sein.

Das Authentifizierungsverfahren ist vom Hersteller zu beschreiben.

ANMERKUNG Die Authentifizierung von Komponenten kann nahe mit dem Schutz der übertragenen Daten verwandt sein (z. B. durch Verschlüsselung). Allerdings ist das Schutzziel der Authentifizierung fundamental verschieden. Während die Verschlüsselung der Daten die Vertraulichkeit dieser sicherstellt, stellt eine positive Authentifizierung die Echtheit der Komponente sicher. Es ist auch möglich, weitere Sicherheitsvorteile durch die Kombination von Authentifizierung und Verschlüsselungsfunktionen zu erlangen. Dies kann z. B. durch Signieren, Integritäts- und Fälschungsschutz der übermittelten Daten erfolgen. Zusätzlich können die Firmware und Software bzgl. Authentizität und Integrität verifiziert und das sichere Booten unterstützt werden.

6.2.5 Software und Firmware

6.2.5.1 Allgemeines

Die sichere Systemkonfiguration von VS-Komponenten hat in Bezug auf die Informationssicherheit eine besondere Bedeutung. Deshalb ist es wichtig, dass diese vor ihrer Verwendung vom Hersteller auf Fehler und Schwachstellen geprüft wird.

Die Konfiguration und die zugrundeliegende Software von IP-gestützten VS-Komponenten darf in einem „System Vulnerability Scan“ keine Schwachstellen laut der Common Vulnerabilities and Exposures-Datenbank (CVE – cve.mitre.org) aufweisen.

6.2.5.2 Bezug von Software und Firmware

Der Bezug von Software/Firmware darf ausschließlich aus einer Quelle erfolgen, welche im unmittelbaren Einflussbereich des Herstellers liegt.

Wird die Software/Firmware über öffentliche Netze übertragen, ist diese mit dem aktuellen Stand der Technik entsprechenden Sicherungs- und Prüfmechanismen verschlüsselt zu übertragen und auf Integrität zu prüfen. Zusätzlich kann die Software signiert übertragen werden.

6.2.5.3 Software- und Firmware-Updates

Die Software/Firmware von VS-Komponenten muss aktualisierbar sein (nicht gefordert für Fremdkomponenten, siehe 3.7).

Es muss VS-weit mindestens ein Mechanismus vorhanden sein, über welchen auf Updates geprüft und automatisch oder manuell die Software/Firmware der einzelnen Komponenten aktualisiert werden kann.

Stehen Updates zur Verfügung, müssen dem Betreiber des VS solange eine oder mehrere Meldungen angezeigt werden, bis diese berücksichtigt wurden. Die Art und Weise einer Meldung muss der Hersteller in der technischen Dokumentation beschreiben.

ANMERKUNG 1 Eine Update-Meldung kann z.B. zentral bei einem autorisierten Benutzer (z. B. einem Administrator) eingehen oder auch dezentral an jeder vom Update betroffenen Komponente erfolgen.

Updates aus der Ferne müssen verschlüsselt (nach 6.3.1 und 6.3.2) übertragen und können zusätzlich signiert werden. Dabei ist ein asymmetrisches Verschlüsselungsverfahren mit individuellen Schlüsselpaaren für jeden Kommunikationspartner (innerhalb des VS) zu bevorzugen.

Werden lediglich symmetrische Verschlüsselungsverfahren eingesetzt, so ist sicherzustellen, dass von jeweils zwei Kommunikationsteilnehmern ein individueller Schlüssel verwendet wird. Dieser Schlüssel muss systemweit einzigartig sein und muss sicher an beide Kommunikationspartner übermittelt werden (nach 6.3.2.5).

Der Hersteller muss in der technischen Dokumentation beschreiben, welches Verfahren er zur Absicherung der Updates verwendet und wie die Schlüssel hierzu an die beteiligten Kommunikationsteilnehmer übermittelt werden.

ANMERKUNG 2 Der Einsatz von asymmetrischen Verschlüsselungsverfahren wird bspw. beim Einsatz von Public-Key-Infrastrukturen berücksichtigt.

Jede Einspielung eines Updates, egal ob für ein einzelnes Schloss oder für das komplette VS, muss durch die Eingabe/Übertragung eines Berechtigungscode (z. B. Eingabe an EE oder aEE) oder Passworts (z. B. Eingabe am IvS) eingeleitet werden. Zusätzlich muss die Installation durch die Eingabe eines Berechtigungscode an mindestens einer lokalen Eingabeeinheit bestätigt werden. Die Anzahl möglicher Falscheingaben dieser Berechtigungscode, die in unmittelbarer Folge vom VS verarbeitet werden, ist nach 6.2.7.6 zu beschränken. Updates dürfen keine Codes oder Passwörter löschen oder ändern.

Updates dürfen in einem separaten Vorgang die Änderungen von Codes oder Passwörtern durchsetzen.

Vor der Aktivierung von Updates muss deren Authentizität und Integrität bestätigt werden (z. B. mittels Hashverfahren oder Signiermechanismen).

BEISPIEL Die Bestätigung der Aktivierung kann z.B. durch Eingabe eines speziellen Codes oder – nach entsprechender Abfrage oder entsprechendem Hinweis – durch erneute Eingabe des zuvor genutzten Codes erfolgen.

Jeder Eingriff in die Firmware/Software muss einen Überwachungseintrag nach 6.2.9 auslösen.

Der Hersteller muss alle erforderlichen Maßnahmen zur Durchführung eines Updates in den Betriebshinweisen aufführen.

Updates müssen durch eine eindeutige Versionsnummer gekennzeichnet werden und eindeutig identifizierbar sein.

6.2.6 Administrationsschnittstellen

Sind vor Ort Administrationsschnittstellen verfügbar, muss der Datenaustausch über eine dedizierte, unmittelbare und leitungsgebundene Kommunikationsverbindung erfolgen. Die übertragenen Daten müssen sicher nach 6.3.1 und 6.3.2 übermittelt werden.

Falls die übertragenen Daten nicht verschlüsselt übermittelt werden, darf jede Administrationsschnittstelle nur nach vorheriger Aktivierung an der EE durch einen autorisierten Benutzer verwendbar sein. Die Aktivierung der Administrationsschnittstelle sowie die Konfigurationstätigkeiten und Servicearbeiten nach 6.2.1 müssen entsprechende Einträge nach 6.2.9 im Ereignisspeicher erzeugen. Eine automatische Deaktivierung der Administrationsschnittstellen muss nach spätestens 10 min Inaktivität erfolgen.

Der Datenaustausch sollte immer durch den Einsatz von aktuellen Kommunikationsprotokollen erfolgen, die über Mechanismen zur Authentisierung, Integritätssicherung und Verschlüsselung der übertragenen Daten verfügen.

6.2.7 Authentifizierung von Benutzern

6.2.7.1 Allgemeines

Die Benutzung einer Komponente eines VS kann nur durch autorisierte Benutzer erfolgen. Eine Autorisierung eines Benutzers setzt eine vorherige positive Authentifizierung voraus. Ein Authentisierungsmerkmal muss dabei mindestens die Anforderungen von 6.2.7.3 erfüllen.

Werden Bedien- und Verwaltungsvorgänge direkt an der EE oder aEE initiiert, ist eine Authentisierung nach den Anforderungen der EN 1300 ausreichend (z. B. Authentisierung mittels Code).

Ein Authentisierungsmerkmal muss einem Benutzer individuell zuzuordnen sein.

Authentisierungsmerkmale müssen ausreichend sicher und vertraulich sein. Sie müssen nach dem aktuellen Stand der Technik gestaltet und entsprechen in die Infrastruktur des VS implementiert sein.

6.2.7.2 Zugriff auf sicherheitsrelevante Information

Jeder Remote-Zugriff auf sicherheitsrelevante Informationen muss durch eine Zwei-Faktor-Authentifizierung gesichert sein. Einer der Faktoren muss dabei mindestens die Anforderungen nach 6.2.7.3 erfüllen.

Bei dem Zugriff vor Ort ist eine Authentisierung nach den Anforderungen der EN 1300 ausreichend (z. B. Authentisierung mittels Code).

6.2.7.3 Anforderungen an Passwörter

Passwörter müssen mindestens aus 8 Zeichen bestehen und mindestens zwei der nachfolgenden Zeichenarten enthalten: Kleinbuchstaben, Großbuchstaben, Ziffern oder Sonderzeichen.

Dem Benutzer muss die Möglichkeit zur Verfügung stehen, ein Passwort jederzeit ändern zu können. Darüber hinaus sollte es möglich sein, die Passwörter regelmäßig im VS zu ändern.

Dieses Dokument unterscheidet zwischen Codes und Passwörtern. Für Codes sind die Anforderungen nach EN 1300 maßgebend.

6.2.7.4 Voreingestellte Passwörter/Codes

Werden voreingestellte Passwörter/Codes verwendet (z. B. bei Anlegen von neuen Benutzern oder Rücksetzen von Passwörtern/Codes), müssen diese bei erstmaligem Gebrauch umgehend von den entsprechenden Benutzern abgeändert werden (eine andere Aktion darf dem Benutzer vorher nicht gestattet sein).

Bei neuen Passwörtern/Codes, die während einer Funktion aktiviert werden (nicht in der Produktionsstätte voreingestellt), dürfen diese Passwörter/Codes keinen direkten Bezug zu ihren jeweiligen Benutzern haben (z. B. nicht automatisch den Namen oder das Geburtsdatum des jeweiligen Benutzers verwenden) oder anderweitig leicht erraten werden können (keine trivialen oder wiederholenden Passwörter/Codes).

6.2.7.5 Anzeige von Passwörtern/Codes

Es darf nicht möglich sein, dass über die vom Hersteller konzipierten/entwickelten Komponenten sicherheitsrelevante Informationen (z. B. Passwörter/Codes) gewonnen werden können.

In keiner Komponente des VS dürfen Passwörter/Codes im Klartext angezeigt werden. Ausnahme für Administratoren: Gehört es zu den Aufgaben, Benutzerpasswörter/-codes zu erzeugen oder zurückzusetzen, so darf die neu erzeugte Authentisierungsinformation dem Administrator lediglich einmalig (bei der Erzeugung bzw. Rücksetzung) im Klartext angezeigt werden. Anschließend dürfen die Authentisierungsinformationen ausschließlich verschleiert angezeigt werden.

Zur Hilfe bei der Eingabe eines Passworts/Codes darf lediglich das letzte eingegebene Zeichen für eine Zeitdauer von max. 2 s, spätestens bis zur Eingabe eines weiteren Zeichens angezeigt werden. Anschließend muss das Passwort durch geeignete Zeichen oder Symbole verschleiert (z. B. durch Sternchen, Punkte etc.) oder komplett verborgen werden.

Die Eingabe von Passwörtern/Codes muss nach abgeschlossener Eingabe unmittelbar zurückgesetzt werden. Bei einer unvollständigen Eingabe muss diese spätestens 30 s nach Eingabe des letzten Zeichens zurückgesetzt werden.

Es muss verhindert werden, dass die Zeichenfolge von Passwörtern/Codes mittels elektronischen Klartextes o. ä. kopiert werden kann.

6.2.7.6 Begrenzung der Falscheingabe von Passwörtern/Codes

Werden Bedien- und Verwaltungsvorgänge direkt an der EE oder aEE initiiert (nach 6.2.7.1), ist die Falscheingabe von Codes, die von der AE innerhalb eines festgelegten Zeitraums verarbeitet werden, klassenabhängig begrenzt. Die entsprechenden Anforderungen sind in Tabelle 1 aufgelistet.

Tabelle 2 — Begrenzung der Falscheingaben

Klassifizierung nach diesem Dokument	Maximale Anzahl verarbeitbarer Falscheingaben in Folge	Zeitraum
A (DS)	300	1 h
B (DS)	100	1 h
C (DS)	30	1 h
D (DS)	10	1 h

Wenn die Bedien- und Verwaltungsvorgänge an einer anderen eigenständigen Komponente initiiert werden (z. B. bei Verwendung eines IvS) müssen Passwörter benutzt werden. Falscheingaben von Passwörtern sind klassenunabhängig auf 10 Versuche pro Stunde begrenzt.

Für die Verwendung von Passwörtern und Codes gilt grundsätzlich: Wird bei Falscheingabe eines Passworts/Codes eine Fehlermeldung ausgegeben, darf diese keine Rückschlüsse auf Korrektheit, Status oder sonstiger Einzelheiten des entsprechenden Benutzerkontos und/oder der eingegebenen Authentisierungsinformation zulassen.

6.2.8 Anzeige des Verriegelungszustandes

Bei VS aller Klassen sind Maßnahmen vorzusehen, die den Verschlusszustand der SE (gesperrt oder entsperrt) ersichtlich machen.

Der Verschlusszustand muss an der EE angezeigt werden. Die zusätzliche Anzeige des Verschlusszustandes an abgesetzter Stelle ist zulässig.

BEISPIEL Dies können z. B. optische Anzeigen am IvS bzw. aEE sein.

6.2.9 Aufzeichnung von Ereignissen

Ereignisse, die in Zusammenhang mit der Bedienung von verteilten Systemen ausgeführt werden, müssen gemäß den folgenden Vorgaben im Ereignisspeicher abgelegt werden.

Die nachfolgenden Ereignisse müssen im VS gespeichert werden:

- Öffnen und schließen der SE
- alle Konfigurationstätigkeiten und Servicearbeiten (siehe 6.2.1)
- Eingriffe in die Software/Firmware (siehe 6.2.5.3)*
- vom Benutzer veranlasste Änderung kryptografischer Schlüssel (siehe 6.3.2.4)
- vom Benutzer veranlasster Zugriff auf kryptografische Schlüssel (siehe 6.3.2.7)
- Manipulation oder Austausch der EE (siehe 6.2.11)
- Zurücksetzen einer Sperre einer EE (siehe 6.2.11)
- Manipulation der aEE (siehe 6.2.11)
- Wiederinbetriebnahme einer aEE (siehe 6.2.11)

**Bei Aktualisierung von Software/Firmware muss die installierte Version sowie die Angabe, ob die Installation lokal oder aus der Ferne ausgeführt wurde, gespeichert werden.*

Jedes Ereignis muss im Ereignisspeicher mit den folgenden Parametern gespeichert werden:

- Identifikation/Art des Ereignisses
- auslösender Benutzer
- auslösende Funktionseinheit (Komponente, automatisierter Prozess oder ähnliches)