E DIN EN 40000-11:2026-12 (D/E)

Erscheinungsdatum: 2026-11-20

Grundlegende Anforderungen an die Cybersicherheit für Produkte - Teil 11: Hardware-Geräte mit Sicherheitsboxen, die eine physische Hardware-Umhüllung enthalten und für die Bereitstellung von Sicherheitsfunktionen, wie sichere Speicherung und kryptografische Operationen in einer offenen Umgebung ausgelegt sind; Deutsche und Englische Fassung prEN 40000-11:2026

Essential cybersecurity requirements for products - Part 11: Hardware Devices with Security Boxes incorporating a hardware physical envelope and designed to provide security functions such as secure storage and cryptographic operations in an open environment; German and English version prEN 40000-11:2026

Inhalt

Seite

Europäisches Vorwort 8

Einleitung 9

1 Anwendungsbereich 10

2 Normative Verweisungen 10

3 Begriffe und Abkürzungen 10

4 Produktkontext 17
4.1 Produktkomponenten und -architektur 17
4.1.1 Überblick 17
4.1.2 Sichere Umhüllung 18
4.1.3 Hardwarekomponenten 20
4.1.4 Firmware 22
4.1.5 Sicherheitsfunktionen 24
4.1.6 Schnittstellen und Konnektivität 26
4.1.7 Externe Dienste und unterstützende Systeme 27
4.1.8 Architektonische Variabilität 28
4.2 Betriebsumgebung 28
4.2.1 Physische Umgebung 28
4.2.2 Logische und physische Konnektivität 30
4.3 Verteilung der Sicherheitsfunktionen 30
4.3.1 HWSB-Integration 30
4.3.2 Zielvorgaben für die Umgebung 30
4.4 Nutzer 33
4.5 Beispiel für einen HWSB-Anwendungsfall 33
4.5.1 Allzweck-HSM 33
4.5.2 Zahlungsterminal/Interaktionsstelle (POI) 34
4.5.3 Fahrtenschreibersysteme 34
4.5.4 Eingebettete/OEM-Systeme 35
4.5.5 Sonstige HWSB-Anwendungsfälle 36

5 Anforderungen 36
5.1 Überblick 36
5.2 Technische Anforderungen 37
5.2.1 Nutzerauthentifizierung (REQ-USER-AUTH-XXX) 37
5.2.2 Ereignisautorisierung (REQ-AUTHORIZATION-XXX) 42
5.2.3 Geräteauthentisierung (REQ-DEVICE-AUTH-XXX) 44
5.2.4 Import sensibler Daten (REQ-SD-IMPORT-XXX) 48
5.2.5 Sichere Kommunikation (REQ-SEC-COM-XXX) 49

5.2.6 Sichere Firmware-Aktualisierung (REQ-COP-SECUP-XXX) ... 53
5.2.7 Integrität gespeicherter Daten (REQ-SDI-XXX) ... 56
5.2.8 Vertraulichkeit gespeicherter Daten (REQ-SDC-HWSB-XXX) ... 57
5.2.9 Integrität der Codeausführung (REQ-CEI-XXX) ... 58
5.2.10 Sicheres Audit (REQ-LOG-XXX) ... 63
5.2.11 Gesicherte Kryptographie (REQ-CRY-XXX) ... 68
5.2.12 Physischer Schutz (REQ-PHY-XXX) ... 76
5.2.13 Konfiguration mit „Sicherheit durch Voreinstellung“ (REQ-COP-SECDEF-XXX) ... 81
5.2.14 Sichere Datensicherung und -wiederherstellung (REQ-BACKUP-XXX) ... 83
5.2.15 Minimierung verarbeiteter Daten (REQ-DATAMIN-XXX) ... 86
5.2.16 Schutz von Restinformationen (REQ-DPR-XXX) ... 87
5.2.17 Minimierung der Auswirkungen von Angriffen (REQ-AIM-XXX) ... 89
5.2.18 Minimierung der Angriffsfläche (REQ-AS-MINIMIZE-XXX) ... 89
5.3 Vertrauenswürdigkeitsanforderungen ... 90
5.3.1 Prozess zum Umgang mit Schwachstellen (REQ-ASS-VUL-HAND) ... 90
5.3.2 Ausnutzbare Schwachstellen (REQ-ASS-VUL-EXP) ... 91
5.3.3 Software-Stückliste (REQ-ASS-SBOM) ... 91
5.3.4 Auswahlleitlinien ... 92

6 Konformitätsbewertungn/Tests (normativ) ... 92
6.1 Methodik zur Bewertung ... 92
6.2 Bewertungsformat ... 92
6.2.1 Allgemeines ... 92
6.2.2 Bewertungsgrundlage ... 92
6.2.3 Bewertungsziel ... 92
6.2.4 Vorbereitung der Bewertung ... 93
6.2.5 Bewertungstätigkeiten ... 93
6.2.6 Entscheidung der Bewertung ... 93
6.2.7 Bewertungsnachweis ... 93
6.3 Bewertung der Produktanforderungen ... 94
6.3.1 Bewertung – Authentifizierung des Bedieners ... 94
6.3.2 Bewertung – Ereignisautorisierung ... 96
6.3.3 Bewertung – Geräteauthentisierung ... 97
6.3.4 Bewertung – Import sensibler Daten ... 98
6.3.5 Bewertung – Sichere Kommunikation ... 100
6.3.6 Bewertung – Sichere Firmware-Aktualisierungen ... 101
6.3.7 Bewertung – Integrität gespeicherter Daten ... 103
6.3.8 Bewertung – Vertraulichkeit gespeicherter Daten ... 104
6.3.9 Bewertung – Integrität der Codeausführung ... 105
6.3.10 Bewertung – Sicheres Audit ... 107
6.3.11 Bewertung – Gesicherte Kryptographie ... 108
6.3.12 Bewertung – Physischer Schutz ... 110
6.3.13 Bewertung – Konfiguration mit „Sicherheit durch Voreinstellung“ ... 112
6.3.14 Bewertung – Sichere Datensicherung (Backup) und Wiederherstellung ... 113
6.3.15 Bewertung – Minimierung verarbeiteter Daten ... 114
6.3.16 Bewertung – Schutz von Restinformationen ... 116
6.3.17 Bewertung – Minimierung der Auswirkungen von Angriffen ... 117
6.3.18 Bewertung – Minimierung der Angriffsfläche ... 118
6.3.19 Bewertung – Vertrauenswürdigkeitsanforderungen ... 119

Anhang A (normativ) Sicherheitsprofil ... 122
A.1 Einleitung ... 122
A.2 Auswählen des Vertrauenswürdigkeitsprofils und der Anforderungsmodule auf der Grundlage von IPRFU ... 123
A.3 Vertrauenswürdigkeitsprofil ... 127
A.4 Anforderungsmodule ... 128

Anhang B (informativ) Sicherheitsanalyse ... 134
B.1 Überblick ... 134

B.2 IPRFU **134**
B.2.1 Zweckbestimmung **134**
B.2.2 Vernünftigerweise vorhersehbare Verwendung **135**
B.2.3 Zuordnung von IPRFU zu HWSB während der Sicherheitsanalyse **135**
B.3 Analyse **136**
B.3.1 Sicherheitszielsetzungen und Vermögenswerte **136**
B.3.2 Bedrohungen **136**
B.3.3 Zuordnung von Bedrohungen zu Zielen und Vermögenswerten **138**
B.3.4 Zuordnung von Sicherheitsmaßnahmen zu Bedrohungen **140**

Anhang C (informativ) Weitere relevante Branchen **145**

Anhang K (normativ) Kryptographie **146**
K.1 Kryptographie auf dem neuesten Stand der Technik (CRY-SOTA) **146**
K.1.1 Anforderung **146**
K.1.2 Bewertungskriterien **146**
K.2 Krypto-Agilität **149**
K.2.1 Anforderung **149**
K.2.2 Bewertungskriterien **150**

Anhang R (normativ) Zusätzliche Bestimmungen für Produkte, die auf Lösungen zur Fernverarbeitung von Daten (RDPS) basieren **151**
R.1 Anwendungsbereich und Anwendbarkeit **151**
R.2 RDPS als Erweiterung der Produktgrenzen **151**
R.3 Bedrohungsmodell **153**
R.3.1 Allgemeines **153**
R.3.2 Vermögenswerte **153**
R.3.3 Bedrohungskatalog **154**
R.3.4 Zuordnung Vermögenswerte ↔ Bedrohungen **155**
R.4 Sicherheitsanforderungen **156**
R.4.1 Allgemeines **156**
R.4.2 Anforderungen an die lokale Produktseite **157**
R.4.3 Anforderungen an die RDPS-Seite **162**
R.4.4 Zuordnung Bedrohungen ↔ Anforderungen **168**
R.4.5 Zuordnung der Anforderungen aus Anhang I der CRA zu denen aus Anhang R **169**
R.5 Sicherheitsmaßnahmen und Leitlinien zur Risikominderung für RDPS-Anforderungen (informativ) **171**
R.5.1 Allgemeines **171**
R.5.2 Maßnahmenkatalog für REQ-RDPS-L-001 ..... **172**
R.5.3 Maßnahmenkatalog für REQ-RDPS-L-002 ..... **172**
R.6 Konformitätsbewertung **172**
R.6.1 Allgemeines **172**
R.6.2 Konformitätsbewertung für REQ-RDPS-L-001 ..... **173**
R.6.3 Konformitätsbewertung für REQ-RDPS-R-001 ..... **174**
R.6.4 Konformitätsbewertung für REQ-RDPS-R-004 ..... **176**

Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Cybersicherheitsanforderungen und der abzudeckenden Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) **179**

Literaturhinweise **182**

Bilder

Bild 1 — Generische Architektur der HWSB-Produkte **18**

Bild 2 — Mehrschichtige Sicherheitsumhüllung 19

Bild 3 — Verteilte sichere Umhüllung mit Schutzinseln 20

Tabellen

Tabelle A.1 — Regelbasiertes Sicherheitsprofil — Auswahloptionen 123

Tabelle A.2 — Regelbasiertes Sicherheitsprofil — Auswahloptionen 125

Tabelle A.3 — Vorlagenbasiertes Sicherheitsprofil — Auswahloptionen 125

Tabelle A.4 — Sicherheitsprofil — Vertrauenswürdigkeitsprofile 127

Tabelle A.5 — Anforderungsmodule — Anwendbarkeitsmatrix 130

Tabelle B.1 — Zuordnung von Bedrohungen zu Zielen und Vermögenswerten 138

Tabelle B.2 — Zuordnung von Sicherheitsmaßnahmen zu Bedrohungen 141

Tabelle R.1 — Zuordnung Bedrohungen ↔ Vermögenswerte 155

Tabelle R.2 — Zuordnung Bedrohungen ↔ Anforderungen 168

Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang I der Cyberresilienz-Verordnung 179