E DIN EN 40000-10:2026-12 (D/E)

Erscheinungsdatum: 2026-11-06

Grundlegende Anforderungen an die Cybersicherheit für Produkte - Teil 10: Produkte mit digitalen Elementen, die in Identitätsmanagementsystemen und Software und Hardware für die Verwaltung des privilegierten Zugangs verwendet werden, einschließlich Authentifizierungs- und Zugangskontrollleser, einschließlich biometrischer Leser; Deutsche und Englische Fassung prEN 40000-10:2026

Essential cybersecurity requirements for products - Part 10: Products with digital elements used in identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers; German and English version prEN 40000-10:2026

Inhalt

Seite

Europäisches Vorwort 9

Einleitung 10

1 Anwendungsbereich 11

2 Normative Verweisungen 14

3 Begriffe, Symbole und Abkürzungen 14
3.1 Begriffe 14
3.2 Symbole und Abkürzungen 20

4 Produktkontext 22
4.1 Produktfunktionen 22
4.2 Produktarchitektur 22
4.3 Betriebsumgebung 23
4.3.1 Einleitung 23
4.3.2 Allgemeine Beschreibung 23
4.3.3 Konnektivitätsaspekte 24
4.4 Verteilung der Sicherheitsfunktionen 24
4.5 Nutzer 24
4.6 Anwendungsfälle und Sicherheitsprofile 25

5 Anforderungen an Produkte 28
5.1 Einführung – Technische Leitlinien und Sicherheitsanalyse 28
5.1.1 Allgemeines 28
5.1.2 Anforderung [REQ-TGSA-001] 29
5.1.3 Anforderung [REQ-TGSA-002] 29
5.1.4 Anforderung [REQ-TGSA-003] 29
5.1.5 Anforderung [REQ-TGSA-004] 30
5.1.6 Anforderung [REQ-TGSA-005] 30
5.1.7 Anforderung [REQ-TGSA-006] 33
5.2 Unbekannte ausnutzbare Schwachstellen 33
5.2.1 Anforderung [REQ-KEV-001] 33
5.2.2 Anforderung [REQ-KEV-002] 33
5.2.3 Anforderung [REQ-KEV-003] 34
5.2.4 Anforderung [REQ-KEV-004] 34
5.2.5 Anforderung [REQ-KEV-005] 34
5.2.6 Anforderung [REQ-KEV-006] 35
5.2.7 Anforderung [REQ-KEV-007] 35
5.2.8 Anforderung an die grundlegenden Sicherheitsprofile [REQ-KEV-008] 35
5.2.9 Zusätzliche Anforderung an substanzielle Sicherheitsprofile [REQ-KEV-009] 36

5.2.10 Zusätzliche Anforderung an die hohen Sicherheitsprofile [REQ-KEV-010] ... 36
5.2.11 Zusätzliche Anforderung an die hohen Sicherheitsprofile [REQ-KEV-011] ... 36
5.3 Sicherheit durch Gestaltung ... 36
5.3.1 Anforderung [REQ-SBD-001] ... 36
5.3.2 Anforderung [REQ-SBD-002] ... 37
5.3.3 Anforderung [REQ-SBD-003] ... 37
5.3.4 Anforderung [REQ-SBD-004] ... 37
5.3.5 Anforderung [REQ-SBD-005] ... 38
5.4 Sichere Aktualisierungen – Anforderung [REQ-SU-001] ... 38
5.5 Authentifizierung und Zugangskontrolle ... 38
5.5.1 Anforderung [REQ-AC-001] ... 38
5.5.2 Anforderung [REQ-AC-002] ... 38
5.6 Integrität und Vertraulichkeit ... 39
5.6.1 Anforderung [REQ-CON-001] ... 39
5.6.2 Anforderung [REQ-CON-002] ... 39
5.6.3 Anforderung [REQ-CON-003] ... 39
5.7 Datenminimierung ... 40
5.7.1 Anforderung [REQ-DM-001] ... 40
5.7.2 Anforderung [REQ-DM-002] ... 40
5.7.3 Anforderung [REQ-DM-003] ... 40
5.8 Verfügbarkeitsschutz ... 40
5.8.1 Anforderung [REQ-AP-001] ... 40
5.8.2 Anforderung [REQ-AP-002] ... 41
5.8.3 Anforderung [REQ-AP-003] ... 41
5.9 Minimierung von Auswirkungen ... 41
5.9.1 Anforderung [REQ-IM-001] ... 41
5.9.2 Anforderung [REQ-IM-002] ... 41
5.10 Minimierung der Angriffsflächen ... 42
5.10.1 Anforderung [REQ-MAS-001] ... 42
5.10.2 Anforderung [REQ-MAS-002] ... 42
5.10.3 Anforderung [REQ-MAS-003] ... 42
5.10.4 Anforderung [REQ-MAS-004] ... 43
5.10.5 Anforderung [REQ-MAS-005] ... 43
5.11 Mechanismen zum Eindämmen der Ausnutzung ... 43
5.11.1 Anforderung [REQ-EMM-001] ... 43
5.11.2 Anforderung [REQ-EMM-002] ... 43
5.12 Protokollierung und Überwachung ... 44
5.12.1 Anforderung [REQ-LOG-001] ... 44
5.12.2 Anforderung [REQ-LOG-002] ... 44
5.13 Datenlöschung und -transparenz ... 44
5.13.1 Anforderung [REQ-DRT-001] ... 44
5.13.2 Anforderung [REQ-DRT-002] ... 45
5.13.3 Anforderung [REQ-DRT-003] ... 45
5.13.4 Anforderung [REQ-DRT-004] ... 45
5.14 Umgang mit Schwachstellen ... 46
5.14.1 Anforderung [REQ-VH-001] ... 46
5.14.2 Anforderung [REQ-VH-002] ... 46
5.14.3 Anforderung [REQ-VH-003] ... 46
5.14.4 Anforderung [REQ-VH-004] ... 47
5.14.5 Anforderung [REQ-VH-005] ... 47
5.14.6 Anforderung [REQ-VH-006] ... 47
5.14.7 Anforderung [REQ-VH-007] ... 47

6 Konformitätsbewertung anhand der normativen Anforderungen ... 48
6.1 Einleitung ... 48
6.2 Konformitätsbewertung anhand der normativen Anforderungen ... 52
6.2.1 Anforderungen an technische Leitlinien (5.1) ... 52
6.2.2 Sicherheitsanalyse und Anforderungen an die Sicherheitsprofilstufe (5.2) ... 64

6.2.3 Anforderungen an „Sicherheit durch Gestaltung“ (5.3) ... 70
6.2.4 Anforderungen an die Cybersicherheitsanalyse (5.4) ... 89
6.2.5 Anforderungen an das Schwachstellenmanagement (5.5) ... 95
6.2.6 Anforderungen an das Sicherheitsprofil (5.6) ... 102

Anhang A (informativ) Hardwareprodukte ... 107

Anhang B (informativ) Softwareprodukte ... 110

Anhang C (informativ) Kontrollsystem für den physischen Zugang ... 113
C.1 Allgemeine Architektur eines PACS ... 113
C.2 Ausführliche Beschreibung der Teilsysteme, die Produkte enthalten ... 113
C.2.1 Öffnungs- und Verriegelungsvorrichtungen einschließlich Online-/Offline-Schlösser ... 113
C.2.2 Lesemodule ... 113
C.2.3 lokale Verarbeitungseinheit ... 114
C.2.4 Tür- und E/A-Module ... 114
C.2.5 Zentrale Zugangsverwaltung ... 115
C.2.6 Benutzungsschnittstellen ... 115

Anhang D (informativ) Identitätsmanagementsystem ... 116
D.1 Allgemeine Architektur eines IDMS ... 116
D.2 Ausführliche Beschreibung der Teilsysteme, die Produkte enthalten ... 116
D.2.1 Identitätsrepositorys und Verzeichnisdienste ... 116
D.2.2 Komponenten für die Identitätsregistrierung und -bereitstellung ... 117
D.2.3 Authentifizierungsdienste ... 117
D.2.4 Dienste zur Autorisierungs- und Richtlinienverwaltung ... 117
D.2.5 Komponenten in den Bereichen Governance, Audit und Compliance ... 118
D.2.6 Benutzungsschnittstellen und Selbstbedienungstools ... 118

Anhang E (normativ) Bedrohungsstufen und Schweregrade der Sicherheitsanalyse ... 119

Anhang F (informativ) Sicherheitsproblemdefinition ... 121
F.1 Synthese ... 121
F.2 Begründung ... 121
F.3 Beschreibung der technischen Betriebsumgebung ... 121
F.4 Zu schützende Vermögenswerte ... 121
F.5 Bedrohungen ... 121
F.6 Sicherheitsfunktionen ... 121
F.7 Bedrohungsabdeckung ... 121

Anhang G (normativ) Produktschnittstellen ... 122

Anhang H (informativ) Kommunikationsprotokolle für das Produkt ... 126

Anhang I (normativ) Methodik zur Bewertung von Angriffen ... 127

Anhang J (informativ) Vorgeschlagene Dokumentstruktur für kryptographische Spezifikationen ... 130
J.1 Allgemeine Beschreibung des Produkts ... 130
J.2 Schlüsselarchitektur ... 130
J.3 Liste der kryptographischen Abhängigkeiten ... 130
J.4 Zuordnung zwischen den Sicherheitsfunktionen und den kryptographischen Mechanismen ... 130
J.5 Einblick in die kryptographischen Mechanismen ... 130

Anhang K (normativ) Kryptographie ... 132
K.1 Kryptographie auf dem neuesten Stand der Technik (CRY-SOTA) ... 132
K.1.1 Anforderung ... 132
K.1.2 Bewertungskriterien ... 132
K.2 Krypto-Agilität ... 135
K.2.1 Anforderung ... 135
K.2.2 Bewertungskriterien ... 136

Anhang L (normativ) Risikoregister ... 137

Anhang R (normativ) Zusätzliche Bestimmungen für Produkte, die auf Lösungen zur Fernverarbeitung von Daten (RDPS) basieren 150
R.1 Anwendungsbereich und Anwendbarkeit 150
R.2 RDPS als Erweiterung der Produktgrenzen 150
R.3 Bedrohungsmodell 152
R.3.1 Allgemeines 152
R.3.2 Vermögenswerte 152
R.3.3 Bedrohungskatalog 153
R.3.4 Zuordnung Vermögenswerte ↔ Bedrohungen 154
R.4 Sicherheitsanforderungen 155
R.4.1 Allgemeines 155
R.4.2 Anforderungen an die lokale Produktseite 156
R.4.3 Anforderungen an die RDPS-Seite 161
R.4.4 Zuordnung Bedrohungen ↔ Anforderungen 167
R.4.5 Zuordnung der Anforderungen aus Anhang I der CRA zu denen aus Anhang R 168
R.5 Sicherheitsmaßnahmen und Leitlinien zur Risikominderung für RDPS-Anforderungen (informativ) 170
R.5.1 Allgemeines 170
R.5.2 Maßnahmenkatalog für REQ-RDPS-L-001 171
R.5.3 Maßnahmenkatalog für REQ-RDPS-L-002 171
R.6 Konformitätsbewertung 171
R.6.1 Allgemeines 171
R.6.2 Konformitätsbewertung für REQ-RDPS-L-001 172
R.6.3 Konformitätsbewertung für REQ-RDPS-R-001 173
R.6.4 Konformitätsbewertung für REQ-RDPS-R-004 175

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) 178

Literaturhinweise 180

Bilder

Bild R.1 — RDPS als Erweiterung der Produktgrenzen (Anwendungsbereich von Anhang R: RDPS-Schnittstelle + RDPS) 151

Tabellen

Tabelle 1 48

Tabelle 2 51

Tabelle A.1 — Liste der Hardwareprodukte nach Zweckbestimmung und vernünftigerweise vorhersehbarer Verwendung 107

Tabelle B.1 — Liste der Softwareprodukte nach Zweckbestimmung und vernünftigerweise vorhersehbarer Verwendung 110

Tabelle E.1 — Bedrohungsstufen der Sicherheitsanalyse 119

Tabelle E.2 — In der Sicherheitsanalyse berücksichtigte Schweregrade 119

Tabelle E.3 — Matrix zwischen Bedrohungen, Schweregraden und erforderlichem Sicherheitsprofil **120**

Tabelle G.1 — Repräsentative Schnittstellen nach Zweckbestimmung und Konformitätsanforderungen **122**

Tabelle H.1 — Repräsentative Protokolle je nach Zweckbestimmung und Konformitätsanforderungen **126**

Tabelle I.1 — Bewertungsfaktoren und -punkte für das Angriffspotential **127**

Tabelle I.2 — Gesamtpunktzahl für Angriffspotential und Widerstandsfähigkeit **129**

Tabelle J.1 — Liste der kryptographischen Abhängigkeiten **130**

Tabelle J.2 — Zuordnung der kryptographischen Mechanismen zu den Sicherheitsfunktionen **130**

Tabelle L.1 — Vermögenswerte **137**

Tabelle L.2 — Risiken **138**

Tabelle L.3 — Bedrohungen **139**

Tabelle R.1 — Zuordnung Bedrohungen ↔ Vermögenswerte **154**

Tabelle R.2 —Zuordnung Bedrohungen ↔ Anforderungen **167**

Tabelle R.3 ..... **168**

Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang I der Cyberresilienz-Verordnung **178**