DIN EN 18031-3:2026-02 (D)

Gemeinsame Sicherheitsanforderungen für Funkanlagen - Teil 3: Internetfähige Funkanlagen, die virtuelles Geld oder Geldwerte verarbeiten; Deutsche Fassung EN 18031-3:2024

Inhalt

Seite

Europäisches Vorwort ... 8
Einleitung ... 9
1 Anwendungsbereich ... 10
2 Normative Verweisungen ... 10
3 Begriffe ... 10
4 Abkürzungen ... 15
5 Anwendung dieses Dokuments ... 17
6 Anforderungen ... 20
6.1 [ACM] Zugangssteuerungsmechanismus (en: Access Control Mechanism) ... 20
6.1.1 [ACM-1] Anwendbarkeit von Zugangssteuerungsmechanismen ... 20
6.1.2 [ACM-2] Angemessene Zugangssteuerungsmechanismen ... 25
6.2 [AUM] Authentisierungsmechanismus (en: Authentication Mechanism) ... 30
6.2.1 [AUM-1] Anwendbarkeit von Authentisierungsmechanismen ... 30
6.2.2 [AUM-2] Angemessene Authentisierungsmechanismen ... 42
6.2.3 [AUM-3] Authentifikator-Validierung ... 49
6.2.4 [AUM-4] Änderung von Authentifikatoren ... 53
6.2.5 [AUM-5] Passwortstärke ... 56
6.2.6 [AUM-6] Schutz vor Brute-Force-Angriffen ... 64
6.3 [SUM] Sicherer Aktualisierungsmechanismus (en: Secure Update Mechanism) ... 68
6.3.1 [SUM-1] Anwendbarkeit von Aktualisierungsmechanismen ... 68
6.3.2 [SUM-2] Sichere Aktualisierungen ... 72
6.3.3 [SUM-3] Automatisierte Aktualisierungen ... 76
6.4 [SSM] Sicherer Speichermechanismus (en: Secure Storage Mechanism) ... 81
6.4.1 [SSM-1] Anwendbarkeit von sicheren Speichermechanismen ... 81
6.4.2 [SSM-2] Angemessener Integritätsschutz für sichere Speichermechanismen ... 85
6.4.3 [SSM-3] Angemessener Vertraulichkeitsschutz für sichere Speichermechanismen ... 90
6.5 [SCM] Sicherer Kommunikationsmechanismus (en: Secure Communication Mechanism) ... 96
6.5.1 [SCM-1] Anwendbarkeit von sicheren Kommunikationsmechanismen ... 96
6.5.2 [SCM-2] Angemessener Integritäts- und Authentizitätsschutz für sichere Kommunikationsmechanismen ... 100
6.5.3 [SCM-3] Angemessener Vertraulichkeitsschutz für sichere Kommunikationsmechanismen ... 107
6.5.4 [SCM-4] Angemessener Wiederholungsschutz für sichere Kommunikationsmechanismen ... 112
6.6 [LGM] Protokollierungsmechanismus (en: Logging Mechanism) ... 118
6.6.1 [LGM-1] Anwendbarkeit von Protokollierungsmechanismen ... 118
6.6.2 [LGM-2] Dauerhafte Speicherung von Protokolldaten ... 122
6.6.3 [LGM-3] Mindestanzahl an dauerhaft gespeicherten Ereignissen ... 125
6.6.4 [LGM-4] Zeitbezogene Informationen der dauerhaft gespeicherten Protokolldaten ... 127
6.7 [CCK] Vertrauliche kryptographische Schlüssel (en: Confidential Cryptographic Keys) ... 131
6.7.1 [CCK-1] Angemessene CCKs ... 131
6.7.2 [CCK-2] Mechanismen zur Erzeugung des CCK ... 135
6.7.3 [CCK-3] Verhinderung von statischen Vorgabewerten für vorinstallierte CCKs ... 140

6.8 [GEC] Allgemeine Anlagenfähigkeiten (en: General Equipment Capabilities) 144
6.8.1 [GEC-1] Aktuelle Software und Hardware ohne öffentlich bekannte ausnutzbare Schwachstellen 144
6.8.2 [GEC-2] Begrenzung der Offenlegung von Diensten über entsprechende Netzwerkschnittstellen 149
6.8.3 [GEC-3] Konfiguration von optionalen Diensten und zugehörigen offengelegten Netzwerkschnittstellen 152
6.8.4 [GEC-4] Dokumentation von zugänglichen Netzwerkschnittstellen und über Netzwerkschnittstellen zugänglichen Diensten 156
6.8.5 [GEC-5] Keine unnötigen externen Schnittstellen 159
6.8.6 [GEC-6] Eingabevalidierung 162
6.8.7 [GEC-7] 167
6.8.8 [GEC-8] Anlagenintegrität 167
6.9 [CRY] Kryptographie (en: Cryptography) 171
6.9.1 [CRY-1] Bewährte Verfahrensweisen für Kryptographie 171

Anhang A (informativ) Begründung 177
A.1 Allgemeines 177
A.2 Begründung 177
A.2.1 Normenfamilie 177
A.2.2 Sicherheit durch Gestaltung (en: Security by design) 177
A.2.3 Bedrohungsmodellierung und Sicherheitsrisikobeurteilung 178
A.2.4 Beurteilung der funktionalen Suffizienz 179
A.2.5 Umsetzungskategorien 180
A.2.6 Werte 180
A.2.7 Mechanismen 182
A.2.8 Beurteilungskriterien 183
A.2.9 Schnittstellen 185

Anhang B (informativ) Abbildung auf EN IEC 62443-4-2:2019 189
B.1 Allgemeines 189
B.2 Abbildung 189

Anhang C (informativ) Abbildung auf ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements) 192
C.1 Allgemeines 192
C.2 Abbildung 192

Anhang D (informativ) Abbildung auf Sicherheitsbewertungsstandard für IoT-Plattformen (SESIP, en: Security Evaluation Standard for IoT Platforms) 197
D.1 Allgemeines 197
D.2 Abbildung 197

Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und der Delegierten Verordnung (EU) 2022/30 zur Ergänzung der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der grundlegenden Anforderungen, wie in Artikel 3(3), Punkt (d), Punkt (e) und Punkt (f) dieser abzudeckenden Richtlinie in Bezug genommen 200

Literaturhinweise 201

Bilder

Bild 1 — Entscheidungsbaum für Anforderung ACM-1 23

Bild 2 — Entscheidungsbaum für Anforderung ACM-2 28

Bild 3 — Entscheidungsbaum für Anforderung AUM-1-1 33

Bild 4 — Entscheidungsbaum für Anforderung AUM-1-2 37

Bild 5 — Entscheidungsbaum für Anforderung AUM-1-3 40

Bild 6 — Entscheidungsbaum für Anforderung AUM-2-1 45

Bild 7 — Entscheidungsbaum für Anforderung AUM-2-2 47

Bild 8 — Entscheidungsbaum für Anforderung AUM-3 50

Bild 9 — Entscheidungsbaum für Anforderung AUM-4 55

Bild 10 — Entscheidungsbaum für Anforderung AUM-5-1 59

Bild 11 — Entscheidungsbaum für Anforderung AUM-5-2 62

Bild 12 — Entscheidungsbaum für Anforderung AUM-6 66

Bild 13 — Entscheidungsbaum für Anforderung SUM-1 71

Bild 14 — Entscheidungsbaum für Anforderung SUM-2 74

Bild 15 — Entscheidungsbaum für Anforderung SUM-3 79

Bild 16 — Entscheidungsbaum für Anforderung SSM-1 83

Bild 17 — Entscheidungsbaum für Anforderung SSM-2 88

Bild 18 — Entscheidungsbaum für Anforderung SSM-3 93

Bild 19 — Entscheidungsbaum für Anforderung SCM-1 99

Bild 20 — Entscheidungsbaum für Anforderung SCM-2 104

Bild 21 — Entscheidungsbaum für Anforderung SCM-3 110

Bild 22 — Entscheidungsbaum für Anforderung SCM-4 116

Bild 23 — Entscheidungsbaum für Anforderung LGM-1 120

Bild 24 — Entscheidungsbaum für Anforderung LGM-2 123

Bild 25 — Entscheidungsbaum für Anforderung LGM-3 126

Bild 26 — Entscheidungsbaum für Anforderung LGM-4 129

Bild 27 — Entscheidungsbaum für Anforderung CCK-1 133

Bild 28 — Entscheidungsbaum für Anforderung CCK-2 138

Bild 29 — Entscheidungsbaum für Anforderung CCK-3 142

Bild 30 — Entscheidungsbaum für Anforderung GEC-1 146

Bild 31 — Entscheidungsbaum für Anforderung GEC-2 151

Bild 32 — Entscheidungsbaum für Anforderung GEC-3 154

Bild 33 — Entscheidungsbaum für Anforderung GEC-4 158

Bild 34 — Entscheidungsbaum für Anforderung GEC-5 161

Bild 35 — Entscheidungsbaum für Anforderung GEC-6 165

Bild 36 — Entscheidungsbaum für Anforderung GEC-8 170

Bild 37 — Entscheidungsbaum für Anforderung CRY-1 174

Bild A.1 — Finanzieller Wert der Anlage 181

Bild A.2 — Sicherheitswert der Anlage 181

Bild A.3 — Beispiel für einen Entscheidungsbaum 183

Bild A.4 — Beispiel: Nachweis durch Entscheidungsbaum 185

Bild A.5 — Beispiel: Laptop mit einer eingebauten Tastatur 186

Bild A.6 — Beispiel: Anlage mit einer USB-Tastatur 187

Bild A.7 — Beispiel: Benutzungsschnittstelle über das Netzwerk 187

Bild A.8 — Beispiel: USB-Drucker 187

Bild A.9 — Beispiel: Netzwerkdrucker 188

Tabellen

Tabelle 1 — Struktur der Anforderungen 17

Tabelle A.1 — STRIDE 178

Tabelle A.2 — Sicherheitsanforderungen, Fähigkeiten, Eindämmungstechniken und Gestaltungsgrundsätze 179

Tabelle A.3 — Werte und grundlegende Anforderungen 180

Tabelle A.4 — Schnittstellen 186

Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und der Richtlinie 2014/53/EU [Amtsblatt L 153] 200