E DIN EN 18031-3:2024-06 (D/E)

Erscheinungsdatum: 2024-05-24

Gemeinsame Sicherheitsanforderungen für Funkgeräte - Teil 3: Internetfähige Funkgeräte, die virtuelles Geld oder Geldwerte verarbeiten; Deutsche und Englische Fassung prEN 18031-3:2023

Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value; German and English version prEN 18031-3:2023

Inhalt

Seite

Europäisches Vorwort 7

Einleitung 8

1 Anwendungsbereich 9

2 Normative Verweisungen 9

3 Begriffe 9

4 Anwendung dieser Norm 13

5 Anforderungen 16
5.1 [ACM] Zugangssteuerungsmechanismus (en: Access Control Mechanism) 16
5.1.1 [ACM-1] Anwendbarkeit von Zugangssteuerungsmechanismen 16
5.1.2 [ACM-2] Angemessene Zugangssteuerungsmechanismen 20
5.2 [AUM] Authentisierungsmechanismus (en: Authentication Mechanism) 23
5.2.1 [AUM-1] Anwendbarkeit von Authentisierungsmechanismen für externe Schnittstellen 24
5.2.2 [AUM-2] Angemessene Authentisierungsmechanismen für externe Schnittstellen 31
5.2.3 [AUM-3] Authentifikator-Validierung 35
5.2.4 [AUM-4] Änderung von Authentifikatoren 38
5.2.5 [AUM-5] Verhinderung von statischen und Vorgabewerten 41
5.2.6 [AUM-6] Schutz vor Brute-Force-Angriffen 45
5.3 [SUM] Sicherer Aktualisierungmechanismus (en: Secure Update Mechanism) 49
5.3.1 [SUM-1] Anwendbarkeit von Aktualisierungsmechanismen 49
5.3.2 [SUM-2] Sichere Aktualisierungen 53
5.3.3 [SUM-3] Automatisierte Aktualisierungen 57
5.4 [SSM] Sicherer Speichermechanismus (en: Secure Storage Mechanism) 60
5.4.1 [SSM-1] Anwendbarkeit von sicheren Speichermechanismen 60
5.4.2 [SSM-2] Angemessener Integritätsschutz für sichere Speichermechanismen 64
5.4.3 [SSM-3] Angemessener Vertraulichkeitsschutz für sichere Speichermechanismen 67
5.5 [SCM] Sicherer Kommunikationsmechanismus (en: Secure Communication Mechanism) 69
5.5.1 [SCM-1] Anwendbarkeit von sicheren Kommunikationsmechanismen 69
5.5.2 [SCM-2] Angemessener Integritäts- und Authentizitätsschutz für sichere Kommunikationsmechanismen 74
5.5.3 [SCM-3] Angemessener Vertraulichkeitsschutz für sichere Kommunikationsmechanismen 77
5.5.4 [SCM-4] Angemessener Wiederholungsschutz für sichere Kommunikationsmechanismen 81
5.6 [LGM] Protokollierungsmechanismus (en: Logging Mechanism) 85
5.6.1 [LGM-1] Anwendbarkeit von Protokollierungsmechanismen 85
5.6.2 [LGM-2] Angemessene Protokollierungsmechanismen 89
5.6.3 [LGM-3] Angemessene Protokollierungsmechanismen – Mindestanzahl von Ereignissen 93
5.6.4 [LGM-4] Angemessene Protokollierungsmechanismen – Zeitbezogene Informationen 96
5.7 [CCK] Vertrauliche kryptographische Schlüssel (en: Confidential Cryptographic Keys) 99

5.7.1 [CCK-1] Angemessene vertrauliche kryptographische Schlüssel (CCKs) 99
5.7.2 [CCK-2] Mechanismen zur Erzeugung vertraulicher kryptographischer Schlüssel 102
5.7.3 [CCK-3] Keine fest einprogrammierten vertraulichen kryptographischen Schlüssel 105
5.7.4 [CCK-4] Verhinderung von statischen Vorgabewerten für vertrauliche kryptographische Schlüssel 107
5.8 [GEC] Allgemeine Gerätefähigkeiten (en: General Equipment Capabilities) 111
5.8.1 [GEC-1] Aktuelle Software und Hardware ohne öffentlich bekannte ausnutzbare Schwachstellen 111
5.8.2 [GEC-2] Begrenzung der Offenlegung von Diensten über entsprechende Netzwerkschnittstellen 114
5.8.3 [GEC-3] Konfiguration von optionalen Diensten und zugehörigen offengelegten Netzwerkschnittstellen 116
5.8.4 [GEC-4] Dokumentation von über Netzwerkschnittstellen zugänglichen Diensten 119
5.8.5 [GEC-5] Keine unnötigen externen Schnittstellen 120
5.8.6 [GEC-7] Eingabevalidierung 123
5.9 [CRY] Kryptographie (en: Cryptography) 128
5.9.1 [CRY-1] Bewährte Verfahrensweisen für Kryptographie 128

Anhang A (informativ) Begründung 133
A.1 Allgemeines 133
A.2 Begründung 133
A.2.1 Normenfamilie 133
A.2.2 Sicherheit durch Gestaltung (en: Security by Design) 133
A.2.3 Werte 134
A.2.4 Mechanismen 134
A.2.5 Beurteilungskriterien 135
A.2.6 Sicherheitsparameter 137

Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und der Delegierten Verordnung (EU) 2022/30 zur Ergänzung der Verordnung 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 Verordnung in Bezug genommen 138

Literaturhinweise 139

Bilder

Bild 1 — Entscheidungsbaum für Anforderung ACM-1 18

Bild 2 — Entscheidungsbaum für Anforderung ACM-2 22

Bild 3 — Entscheidungsbaum für Anforderung AUM-1-1 27

Bild 4 — Entscheidungsbaum für Anforderung AUM-1-2 30

Bild 5 — Entscheidungsbaum für Anforderung AUM-2 33

Bild 6 — Entscheidungsbaum für Anforderung AUM-3 36

Bild 7 — Entscheidungsbaum für Anforderung AUM-4 40

Bild 8 — Entscheidungsbaum für Anforderung AUM-5 44

Bild 9 — Entscheidungsbaum für Anforderung AUM-6 48

Bild 10 — Entscheidungsbaum für Anforderung SUM-1 52

Bild 11 — Entscheidungsbaum für Anforderung SUM-2 55

Bild 12 — Entscheidungsbaum für Anforderung SUM-3 59

Bild 13 — Entscheidungsbaum für Anforderung SSM-1 62

Bild 14 — Entscheidungsbaum für Anforderung SSM-2 66

Bild 15 — Entscheidungsbaum für Anforderung SSM-3 68

Bild 16 — Entscheidungsbaum für Anforderung SCM-1 72

Bild 17 — Entscheidungsbaum für Anforderung SCM-2 76

Bild 18 — Entscheidungsbaum für Anforderung SCM-3 80

Bild 19 — Entscheidungsbaum für Anforderung SCM-4 84

Bild 20 — Entscheidungsbaum für Anforderung LGM-1 88

Bild 21 — Entscheidungsbaum für Anforderung LGM-2 92

Bild 22 — Entscheidungsbaum für Anforderung LGM-3 95

Bild 23 — Entscheidungsbaum für Anforderung LGM-4 98

Bild 24 — Entscheidungsbaum für Anforderung CCK-4 109

Bild 25 — Entscheidungsbaum für Anforderung GEC-7 126

Bild 26 — Entscheidungsbaum für Anforderung CRY-1 131

Bild A.1 — Beispiel für einen Entscheidungsbaum 135

Tabellen

Tabelle 1 — 14

Tabelle A.1 — 134

Tabelle A.2 — 136

Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und der Richtlinie 2014/53/EU [Amtsblatt L 153] 138