

E DIN EN 18031-1:2024-06 (D/E)

Erscheinungsdatum: 2024-05-03

Gemeinsame Sicherheitsanforderungen für Funkanlagen - Teil 1: Funkanlagen mit Internetanschluss; Deutsche und Englische Fassung prEN 18031-1:2023

Common security requirements for radio equipment - Part 1: Internet connected radio equipment; German and English version prEN 18031-1:2023

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.....	30
5.2.3 [AUM-3] Authentifikator-Validierung	34
5.2.4 [AUM-4] Änderung von Authentifikatoren.....	37
5.2.5 [AUM-5] Verhinderung von statischen und Vorgabewerten.....	40
5.2.6 [AUM-6] Schutz vor Brute-Force-Angriffen.....	44
5.3 [SUM] Sicherer Aktualisierungsmechanismus (en: Secure Update Mechanism)	48
5.3.1 [SUM-1] Anwendbarkeit von Aktualisierungsmechanismen.....	48
5.3.2 [SUM-2] Sichere Aktualisierungen.....	52
5.3.3 [SUM-3] Automatisierte Aktualisierungen.....	56
5.4 [SSM] Sicherer Speichermechanismus (en: Secure Storage Mechanism)	59
5.4.1 [SSM-1] Anwendbarkeit von sicheren Speichermechanismen.....	59
5.4.2 [SSM-2] Angemessener Integritätsschutz für sichere Speichermechanismen	63
5.4.3 [SSM-3] Angemessener Vertraulichkeitsschutz für sichere Speichermechanismen.....	66
5.5 [SCM] Sicherer Kommunikationsmechanismus (en: Secure Communication Mechanism)	69
5.5.1 [SSM-1] Anwendbarkeit von sicheren Kommunikationsmechanismen.....	69
5.5.2 [SCM-2] Angemessener Integritäts- und Authentizitätsschutz für sichere Kommunikationsmechanismen.....	73
5.5.3 [SCM-3] Angemessener Vertraulichkeitsschutz für sichere Kommunikationsmechanismen.....	77
5.5.4 [SCM-4] Angemessener Wiederholungsschutz für sichere Kommunikationsmechanismen.....	80
5.6 [RLM] Resilienzmechanismus (en: Resilience Mechanism)	84
5.6.1 [RLM-1] Anwendbarkeit von Resilienzmechanismen	84
5.7 [NMM] Netzwerküberwachungsmechanismus (en: Network Monitoring Mechanism)	89
5.7.1 [NMM-1] Anwendbarkeit eines angemessenen Netzwerküberwachungsmechanismus.....	89
5.8 [TCM] Verkehrssteuerungsmechanismus (en: Traffic Control Mechanism).....	93
5.8.1 [TCM-1] Anwendbarkeit eines angemessenen Verkehrssteuerungsmechanismus	93
5.9 [CCK] Vertrauliche kryptographische Schlüssel (en: Confidential Cryptographic Keys).....	96
5.9.1 [CCK-1] Angemessene vertrauliche kryptographische Schlüssel (CCKs).....	96

5.9.2	[CCK-2] Mechanismen zur Erzeugung vertraulicher kryptographischer Schlüssel	99
5.9.3	[CCK-3] Keine fest einprogrammierten vertraulichen kryptographischen Schlüssel	102
5.9.4	[CCK-4] Verhinderung von statischen Vorgabewerten für vertrauliche kryptographische Schlüssel.....	104
5.10	[GEC] Allgemeine Gerätefähigkeiten (en: General Equipment Capabilities)	108
5.10.1	[GEC-1] Aktuelle Software und Hardware ohne öffentlich bekannte ausnutzbare Schwachstellen.....	108
5.10.2	[GEC-2] Begrenzung der Offenlegung von Diensten über entsprechende Netzwerkschnittstellen	111
5.10.3	[GEC-3] Konfiguration von optionalen Diensten und zugehörigen offengelegten Netzwerkschnittstellen	113
5.10.4	[GEC-4] Dokumentation von über Netzwerkschnittstellen zugänglichen Diensten.....	116
5.10.5	[GEC-5] Keine unnötigen externen Schnittstellen	117
5.10.6	[GEC-7] Eingabevalidierung.....	120
5.11	[CRY] Kryptographie (en: Cryptography).....	125
5.11.1	[CRY-1] Bewährte Verfahrensweisen für Kryptographie.....	125
Anhang A (informativ) Begründung		130
A.1	Allgemeines.....	130
A.2	Begründung.....	130
A.2.1	Normenfamilie	130
A.2.2	Sicherheit durch Gestaltung (en: Security by Design).....	130
A.2.3	Werte.....	131
A.2.4	Mechanismen.....	131
A.2.5	Beurteilungskriterien.....	132
A.2.6	Sicherheitsparameter.....	134
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		135
Literaturhinweise.....		136
Bilder		
Bild 1 — Entscheidungsbaum für Anforderung ACM-2		22
Bild 2 — Entscheidungsbaum für Anforderung AUM-1-1		26
Bild 3 — Entscheidungsbaum für Anforderung AUM-1-2		29
Bild 4 — Entscheidungsbaum für Anforderung AUM-2		32
Bild 5 — Entscheidungsbaum für Anforderung AUM-3		35
Bild 6 — Entscheidungsbaum für Anforderung AUM-4		39
Bild 7 — Entscheidungsbaum für Anforderung AUM-5		43
Bild 8 — Entscheidungsbaum für Anforderung AUM-6		47
Bild 9 — Entscheidungsbaum für Anforderung SUM-1.....		51
Bild 10 — Entscheidungsbaum für Anforderung SUM-2		54
Bild 11 — Entscheidungsbaum für Anforderung SUM-3		58

Bild 12 — Entscheidungsbaum für Anforderung SSM-1	61
Bild 13 — Entscheidungsbaum für Anforderung SSM-2	65
Bild 14 — Entscheidungsbaum für Anforderung SSM-3	68
Bild 15 — Entscheidungsbaum für Anforderung SCM-1.....	71
Bild 16 — Entscheidungsbaum für Anforderung SCM-2.....	75
Bild 17 — Entscheidungsbaum für Anforderung SCM-3.....	79
Bild 18 — Entscheidungsbaum für Anforderung SCM-4.....	83
Bild 19 — Entscheidungsbaum für Anforderung RLM-1	87
Bild 20 — Entscheidungsbaum für Anforderung NMM-1.....	91
Bild 21 — Entscheidungsbaum für Anforderung TCM-1.....	94
Bild 22 — Entscheidungsbaum für Anforderung CCK-4	106
Bild 23 — Entscheidungsbaum für Anforderung GEC-7	123
Bild 24 — Entscheidungsbaum für Anforderung CRY-1	128
Bild A.1 — Beispiel für einen Entscheidungsbaum.....	132
Tabellen	
Tabelle 1 —	14
Tabelle A.1 —.....	131
Tabelle A.2 —.....	133
Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und der Richtlinie 2014/53/EU [Amtsblatt L 153]	135