DIN EN 18031-1:2025-05 (E)

Common security requirements for radio equipment - Part 1: Internet connected radio equipment

Contents

Page

European foreword 4

Introduction 5

1 Scope 6

2 Normative references 6

3 Terms and definitions 6

4 Abbreviations 11

5 Application of this document 12

6 Requirements 15
6.1 [ACM] Access control mechanism 15
6.1.1 [ACM-1] Applicability of access control mechanisms 15
6.1.2 [ACM-2] Appropriate access control mechanisms 20
6.2 [AUM] Authentication mechanism 25
6.2.1 [AUM-1] Applicability of authentication mechanisms 25
6.2.2 [AUM-2] Appropriate authentication mechanisms 34
6.2.3 [AUM-3] Authenticator validation 37
6.2.4 [AUM-4] Changing authenticators 41
6.2.5 [AUM-5] Password strength 44
6.2.6 [AUM-6] Brute force protection 52
6.3 [SUM] Secure update mechanism 56
6.3.1 [SUM-1] Applicability of update mechanisms 56
6.3.2 [SUM-2] Secure updates 59
6.3.3 [SUM-3] Automated updates 64
6.4 [SSM] Secure storage mechanism 68
6.4.1 [SSM-1] Applicability of secure storage mechanisms 68
6.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms 72
6.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms 77
6.5 [SCM] Secure communication mechanism 82
6.5.1 [SCM-1] Applicability of secure communication mechanisms 82
6.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms 88
6.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms ...94
6.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms 99
6.6 [RLM] Resilience mechanism 105
6.6.1 [RLM-1] Applicability and appropriateness of resilience mechanisms 105
6.7 [NMM] Network monitoring mechanism 109
6.7.1 [NMM-1] Applicability and appropriateness of network monitoring mechanisms. 109 6.8 [TCM] Traffic control mechanism 113
6.8.1 [TCM-1] Applicability of and appropriate traffic control mechanisms 113
6.9 [CCK] Confidential cryptographic keys 117
6.9.1 [CCK-1] Appropriate CCKs 117
6.9.2 [CCK-2] CCK generation mechanisms 121
6.9.3 [CCK-3] Preventing static default values for preinstalled CCKs 125
6.10 [GEC] General equipment capabilities 129

6.10.1 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities ... 129
6.10.2 [GEC-2] Limit exposure of services via related network interfaces ... 134
6.10.3 [GEC-3] Configuration of optional services and the related exposed network interfaces 138
6.10.4 [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces ... 141
6.10.5 [GEC-5] No unnecessary external interfaces ... 144
6.10.6 [GEC-6] Input validation ... 147
6.11 [CRY] Cryptography ... 152
6.11.1 [CRY-1] Best practice cryptography ... 152

Annex A (informative) Rationale ... 157

A.1 General ... 157
A.2 Rationale ... 157
A.2.1 Family of standards ... 157
A.2.2 Security by design ... 157
A.2.3 Threat modelling and security risk assessment ... 158
A.2.4 Functional sufficiency assessment ... 159
A.2.5 Implementation categories ... 159
A.2.6 Assets ... 160
A.2.7 Mechanisms ... 161
A.2.8 Assessment criteria ... 162
A.2.9 Interfaces ... 165

Annex B (informative) Mapping with EN IEC 62443-4-2: 2019 ... 168

B.1 General ... 168
B.2 Mapping ... 168

Annex C (informative) Mapping with ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements) ... 171

C.1 General ... 171
C.2 Mapping ... 171

Annex D (informative) Mapping with Security Evaluation Standard for IoT Platforms (SESIP) ... 175

D.1 General ... 175
D.2 Mapping ... 175

Annex ZA (informative) Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered ... 178

Bibliography ... 179