DIN EN 18031-2:2025-03 (E)

Common security requirements for radio equipment - Part 2: Radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

Contents

Page

European foreword 5

Introduction 6

1 Scope 7

2 Normative references 7

3 Terms and definitions 7

4 Abbreviations 12

5 Application of this document 13

6 Requirements 16
6.1 [ACM] Access control mechanism 16
6.1.1 [ACM-1] Applicability of access control mechanisms 16
6.1.2 [ACM-2] Appropriate access control mechanisms 21
6.1.3 [ACM-3] Default access control for children in toys 26
6.1.4 [ACM-4] Default access control to children's privacy assets for toys and childcare equipment 30
6.1.5 [ACM-5] Parental/Guardian access controls for children in toys 36
6.1.6 [ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys 40
6.2 [AUM] Authentication mechanism 45
6.2.1 [AUM-1] Applicability of authentication mechanisms 45
6.2.2 [AUM-2] Appropriate authentication mechanisms 55
6.2.3 [AUM-3] Authenticator validation 61
6.2.4 [AUM-4] Changing authenticators 65
6.2.5 [AUM-5] Password strength 68
6.2.6 [AUM-6] Brute force protection 76
6.3 [SUM] Secure update mechanism 80
6.3.1 [SUM-1] Applicability of update mechanisms 80
6.3.2 [SUM-2] Secure updates 83
6.3.3 [SUM-3] Automated updates 88
6.4 [SSM] Secure storage mechanism 91
6.4.1 [SSM-1] Applicability of secure storage mechanisms 91
6.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms 96
6.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms 101
6.5 [SCM] Secure communication mechanism 106
6.5.1 [SCM-1] Applicability of secure communication mechanisms 106
6.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms 112
6.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms 118
6.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms 123
6.6 [LGM] Logging mechanism 128
6.6.1 [LGM-1] Applicability of logging mechanisms 128
6.6.2 [LGM-2] Persistent storage of log data 131
6.6.3 [LGM-3] Minimum number of persistently stored events 134

6.6.4 [LGM-4] Time-related information of persistently stored log data 137
6.7 [DLM] Deletion mechanism 140
6.7.1 [DLM-1] Applicability of deletion mechanisms 140
6.8 [UNM] User notification mechanism 144
6.8.1 [UNM-1] Applicability of user notification mechanisms 144
6.8.2 [UNM-2] Appropriate user notification content 148
6.9 [CCK] Confidential cryptographic keys 150
6.9.1 [CCK-1] Appropriate CCKs 150
6.9.2 [CCK-2] CCK generation mechanisms 154
6.9.3 [CCK-3] Preventing static default values for preinstalled CCKs 159
6.10 [GEC] General equipment capabilities 163
6.10.1 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities 163
6.10.2 [GEC-2] Limit exposure of services via related network interfaces 168
6.10.3 [GEC-3] Configuration of optional services and the related exposed network interfaces 172
6.10.4 [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces 175
6.10.5 [GEC-5] No unnecessary external interfaces 178
6.10.6 [GEC-6] Input validation 181
6.10.7 [GEC-7] Documentation of external sensing capabilities 186
6.11 [CRY] Cryptography 188
6.11.1 [CRY-1] Best practice cryptography 188

Annex A (informative) Rationale 194

A.1 General 194
A.2 Rationale 194
A.2.1 Family of standards 194
A.2.2 Security by design 194
A.2.3 Threat modelling and security risk assessment 195
A.2.4 Functional sufficiency assessment 196
A.2.5 Implementation categories 196
A.2.6 Assets 197
A.2.7 Mechanisms 199
A.2.8 Assessment criteria 199
A.2.9 Interfaces 202

Annex B (informative) Mapping with EN IEC 62443-4-2: 2019 205

B.1 General 205
B.2 Mapping 205

Annex C (informative) Mapping with ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements) 208

C.1 General 208
C.2 Mapping 208

Annex D (informative) Mapping with Security Evaluation Standard for IoT Platforms (SESIP) 214

D.1 General 214
D.2 Mapping 214

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 217

Bibliography 218