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

Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value

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
6.2 [AUM] Authentication mechanism 25
6.2.1 [AUM-1] Applicability of authentication mechanisms 25
6.2.2 [AUM-2] Appropriate authentication mechanisms 36
6.2.3 [AUM-3] Authenticator validation 42
6.2.4 [AUM-4] Changing authenticators 46
6.2.5 [AUM-5] Password strength 49
6.2.6 [AUM-6] Brute force protection 57
6.3 [SUM] Secure update mechanism 61
6.3.1 [SUM-1] Applicability of update mechanisms 61
6.3.2 [SUM-2] Secure updates 64
6.3.3 [SUM-3] Automated updates 68
6.4 [SSM] Secure storage mechanism 72
6.4.1 [SSM-1] Applicability of secure storage mechanisms 72
6.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms 76
6.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms 81
6.5 [SCM] Secure communication mechanism 86
6.5.1 [SCM-1] Applicability of secure communication mechanisms 86
6.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms 91
6.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms 97
6.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms 102
6.6 [LGM] Logging Mechanism 107
6.6.1 [LGM-1] Applicability of logging mechanisms 107
6.6.2 [LGM-2] Persistent storage of log data 110
6.6.3 [LGM-3] Minimum number of persistently stored events 113
6.6.4 [LGM-4] Time-related information of persistently stored dog data 116
6.7 [CCK] Confidential cryptographic keys 119
6.7.1 [CCK-1] Appropriate CCKs 119
6.7.2 [CCK-2] CCK generation mechanisms 123
6.7.3 [CCK-3] Preventing static default values for preinstalled CCKs 127
6.8 [GEC] General equipment capabilities 131
6.8.1 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities 131

6.8.2 [GEC-2] Limit exposure of services via related network interfaces 135
6.8.3 [GEC-3] Configuration of optional services and the related exposed network interfaces 139
6.8.4 [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces 143
6.8.5 [GEC-5] No unnecessary external interfaces 146
6.8.6 [GEC-6] Input validation 148
6.8.7 [GEC-7] 153
6.8.8 [GEC-8] Equipment Integrity 153
6.9 [CRY] Cryptography 157
6.9.1 [CRY-1] Best practice cryptography 157

Annex A (informative) Rationale 162

A.1 General 162
A.2 Rationale 162
A.2.1 Family of standards 162
A.2.2 Security by design 162
A.2.3 Threat modelling and security risk assessment 163
A.2.4 Functional sufficiency assessment 164
A.2.5 Implementation categories 164
A.2.6 Assets 165
A.2.7 Mechanisms 166
A.2.8 Assessment criteria 167
A.2.8.1 Decision trees 167
A.2.8.2 Technical documentation 167
A.2.8.3 Security testing 168
A.2.9 Interfaces 169
A.2.9.1 Example: Laptop with a built-in keyboard 170
A.2.9.2 Example: Equipment with a USB-keyboard 170
A.2.9.3 Example: User interface over a network 171
A.2.9.4 Example: USB-printer 171
A.2.9.5 Example: Network printer 171

Annex B (informative) Mapping with ENIEC 62443-4-2:2019 173

B.1 General 173
B.2 Mapping 173

Annex C (informative) Mapping with ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements) 176

C.1 General 176
C.2 Mapping 176

Annex D (informative) Mapping with Security Evaluation Standard for IoT Platforms (SESIP) 180

D.1 General 180
D.2 Mapping 180

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 183

Bibliography 184