

STN	Spoločné bezpečnostné požiadavky pre rádiové zariadenia Časť 1: Rádiové zariadenia pripojené k internetu	STN EN 18031-1 97 4191
------------	---	--

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 11/24

Obsahuje: EN 18031-1:2024

139453



EUROPEAN STANDARD

EN 18031-1

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2024

ICS 35.030

English version

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

Exigences de sécurité communes applicables aux
équipements radioélectriques - Partie 1 : Équipements
radioélectriques connectés à l'internet

Gemeinsame Sicherheitsanforderungen für
Funkanlagen - Teil 1: Funkanlagen mit
Internetanschluss

This European Standard was approved by CEN on 1 August 2024.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



**CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels**

EN 18031-1:2024 (E)

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

EN 18031-1:2024 (E)**European foreword**

This document (EN 18031-1:2024) has been prepared by Technical Committee CEN/CENELEC JTC 13 “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2025, and conflicting national standards shall be withdrawn at the latest by February 2025.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a standardization request addressed to CEN-CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZA, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Introduction

Vigilance is required from manufacturers to improve the overall resilience against cybersecurity threats caused by the increased connectivity of radio equipment [33] and the growing ability of malicious threat actors to cause harm to users, organizations, and society.

The security requirements presented in this baseline standard are developed to improve the ability of radio equipment to protect its security assets and network assets against common cybersecurity threats and to mitigate publicly known exploitable vulnerabilities.

It is important to note that to achieve the overall cybersecurity of radio equipment, defence in depth best practices will be needed by both the manufacturer and user. In particular, no single measure will suffice to achieve the given objectives, indeed achieving even a single security objective will usually require a suite of mechanisms and measures. Throughout this document, the guidance material includes lists of examples. These examples given are only indicative possibilities, as there are other possibilities that are not listed, and even using the examples given will not be sufficient unless the mechanisms and measures chosen are implemented in a coordinated fashion.

EN 18031-1:2024 (E)**1 Scope**

This document specifies common security requirements and related assessment criteria for internet-connected radio equipment [34] (hereinafter referred to as "equipment").

2 Normative references

There are no normative references in this document.

koniec náhľadu – text ďalej pokračuje v platenej verzii STN