

STN	Spoločné bezpečnostné požiadavky pre rádiové zariadenia Časť 2: Rádiové zariadenia spracúvajúce údaje, menovite rádiové zariadenia pripojené na internet, rádiové zariadenia pre starostlivosť o deti, rádiové zariadenia hračiek a nositeľné rádiové zariadenia	STN EN 18031-2 97 4191
------------	---	--

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

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 18031-2:2024

139452



Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2024

Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

EUROPEAN STANDARD**EN 18031-2****NORME EUROPÉENNE****EUROPÄISCHE NORM**

August 2024

ICS 33.060.20

English version

**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**

Exigences de sécurité communes applicables aux équipements radioélectriques - Partie 2 : Équipements radioélectriques qui traitent des données, à savoir les équipements radioélectriques connectés à l'internet, les équipements radioélectriques destinés à la garde d'enfants, les jouets dotés d'équipements radioélectriques et les équipements radioélectriques portables

Gemeinsame Sicherheitsanforderungen für datenverarbeitende Funkanlagen, namentlich mit dem Internet verbundene Funkanlagen, in der Kinderbetreuung eingesetzte Funkanlagen, in Spielzeug eingesetzte Funkanlagen sowie an einem Teil des menschlichen Körpers oder an Kleidungsstücken getragene Funkanlagen

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.



EN 18031-2:2024 (E)**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

EN 18031-2:2024 (E)

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

European foreword

This document (EN 18031-2:2024) 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.

EN 18031-2:2024 (E)**Introduction**

Vigilance is required from manufacturers to improve the overall resilience against cybersecurity threats caused by the increased connectivity of radio equipment [36] 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 and privacy 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.

1 Scope

This document specifies common security requirements and related assessment criteria for radio equipment [36] processing personal data [40] or traffic data [41] or location data [41] for either internet connected radio equipment [37], radio equipment designed or intended exclusively for childcare [37]; toys [39] and wearable radio equipment [37] (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