

|            |                                                                                                                                                                                     |                                                |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| <b>STN</b> | <b>Spoločné bezpečnostné požiadavky pre rádiové zariadenia</b><br><b>Časť 3: Rádiové zariadenia pripojené na internet, ktoré spracúvajú virtuálne peniaze alebo peňažnú hodnotu</b> | <b>STN</b><br><b>EN 18031-3</b><br><br>97 4191 |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|

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

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 18031-3:2024

139451



EUROPEAN STANDARD

EN 18031-3

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2024

ICS 33.060.20

English version

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

Exigences de sécurité communes applicables aux équipements radioélectriques - Partie 3 : Équipements radioélectriques connectés à l'internet qui traitent une monnaie virtuelle ou de la valeur monétaire

Gemeinsame Sicherheitsanforderungen für mit dem Internet verbundene Funkanlagen, die für die Datenverarbeitung im Zusammenhang mit virtuellen Währungen oder monetären Werten eingesetzt werden

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 18031-3:2024 (E)****Contents**

Page

|                                                                                                           |           |
|-----------------------------------------------------------------------------------------------------------|-----------|
| <b>European foreword .....</b>                                                                            | <b>5</b>  |
| <b>Introduction .....</b>                                                                                 | <b>6</b>  |
| <b>1 Scope.....</b>                                                                                       | <b>7</b>  |
| <b>2 Normative references.....</b>                                                                        | <b>7</b>  |
| <b>3 Terms and definitions .....</b>                                                                      | <b>7</b>  |
| <b>4 Abbreviations.....</b>                                                                               | <b>12</b> |
| <b>5 Application of this document.....</b>                                                                | <b>13</b> |
| <b>6 Requirements.....</b>                                                                                | <b>16</b> |
| 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 log 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 .....                                                                                                                 | 167 |
| A.2.8   | Assessment criteria .....                                                                                                        | 167 |
| A.2.8.1 | Decision trees.....                                                                                                              | 167 |
| A.2.8.2 | Technical documentation.....                                                                                                     | 168 |
| A.2.8.3 | Security testing.....                                                                                                            | 169 |
| 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.....                                                                                                    | 172 |
|         | Annex B (informative) Mapping with EN IEC 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 |

**EN 18031-3:2024 (E)**

|                               |                                                                                                                                                                                                                                                                                                                                             |            |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>D.2</b>                    | <b>Mapping.....</b>                                                                                                                                                                                                                                                                                                                         | <b>180</b> |
| <b>Annex ZA (informative)</b> | <b>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 .....</b> | <b>183</b> |
| <b>Bibliography .....</b>     |                                                                                                                                                                                                                                                                                                                                             | <b>184</b> |

## European foreword

This document (EN 18031-3:2024) 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 18031-3:2024 (E)****Introduction**

Vigilance is required from manufacturers to improve the overall resilience against cybersecurity threats caused by the increased connectivity of radio equipment [34] 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 financial 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 internet connected radio equipment [35]. That equipment enables the holder or user to transfer money, monetary value or virtual currency [35] (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**