

RAADIOSEADMETE ÜHISED TURVANÕUDED. OSA 3:  
INTERNETIGA ÜHENDATUD RAADIOSEADMED, MIS  
TÖÖTLEVAD VIRTUAALRAHA VÕI RAHALIST  
VÄÄRTUST

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

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

<p>See Eesti standard EVS-EN 18031-3:2024 sisaldab Euroopa standardi EN 18031-3:2024 ingliskeelset teksti.</p> <p>Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.</p> <p>Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 14.08.2024.</p> <p>Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.</p>	<p>This Estonian standard EVS-EN 18031-3:2024 consists of the English text of the European standard EN 18031-3:2024.</p> <p>This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.</p> <p>Date of Availability of the European standard is 14.08.2024.</p> <p>The standard is available from the Estonian Centre for Standardisation and Accreditation.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile [standardiosakond@evs.ee](mailto:standardiosakond@evs.ee).

ICS 33.060.20

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele. Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis- ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto:info@evs.ee)

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation and Accreditation: Homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

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**

**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>
<b>6.1 [ACM] Access control mechanism</b> .....	<b>16</b>
<b>6.1.1 [ACM-1] Applicability of access control mechanisms</b> .....	<b>16</b>
<b>6.1.2 [ACM-2] Appropriate access control mechanisms</b> .....	<b>21</b>
<b>6.2 [AUM] Authentication mechanism</b> .....	<b>25</b>
<b>6.2.1 [AUM-1] Applicability of authentication mechanisms</b> .....	<b>25</b>
<b>6.2.2 [AUM-2] Appropriate authentication mechanisms</b> .....	<b>36</b>
<b>6.2.3 [AUM-3] Authenticator validation</b> .....	<b>42</b>
<b>6.2.4 [AUM-4] Changing authenticators</b> .....	<b>46</b>
<b>6.2.5 [AUM-5] Password strength</b> .....	<b>49</b>
<b>6.2.6 [AUM-6] Brute force protection</b> .....	<b>57</b>
<b>6.3 [SUM] Secure update mechanism</b> .....	<b>61</b>
<b>6.3.1 [SUM-1] Applicability of update mechanisms</b> .....	<b>61</b>
<b>6.3.2 [SUM-2] Secure updates</b> .....	<b>64</b>
<b>6.3.3 [SUM-3] Automated updates</b> .....	<b>68</b>
<b>6.4 [SSM] Secure storage mechanism</b> .....	<b>72</b>
<b>6.4.1 [SSM-1] Applicability of secure storage mechanisms</b> .....	<b>72</b>
<b>6.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms</b> .....	<b>76</b>
<b>6.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms</b> .....	<b>81</b>
<b>6.5 [SCM] Secure communication mechanism</b> .....	<b>86</b>
<b>6.5.1 [SCM-1] Applicability of secure communication mechanisms</b> .....	<b>86</b>
<b>6.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms</b> .....	<b>91</b>
<b>6.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms</b> .....	<b>97</b>
<b>6.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms</b> ...	<b>102</b>
<b>6.6 [LGM] Logging Mechanism</b> .....	<b>107</b>
<b>6.6.1 [LGM-1] Applicability of logging mechanisms</b> .....	<b>107</b>
<b>6.6.2 [LGM-2] Persistent storage of log data</b> .....	<b>110</b>
<b>6.6.3 [LGM-3] Minimum number of persistently stored events</b> .....	<b>113</b>
<b>6.6.4 [LGM-4] Time-related information of persistently stored log data</b> .....	<b>116</b>
<b>6.7 [CCK] Confidential cryptographic keys</b> .....	<b>119</b>
<b>6.7.1 [CCK-1] Appropriate CCKs</b> .....	<b>119</b>
<b>6.7.2 [CCK-2] CCK generation mechanisms</b> .....	<b>123</b>
<b>6.7.3 [CCK-3] Preventing static default values for preinstalled CCKs</b> .....	<b>127</b>
<b>6.8 [GEC] General equipment capabilities</b> .....	<b>131</b>

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
	<b>Annex A (informative) Rationale .....</b>	<b>162</b>
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
	<b>Annex B (informative) Mapping with EN IEC 62443-4-2:2019.....</b>	<b>173</b>
B.1	General .....	173
B.2	Mapping.....	173
	<b>Annex C (informative) Mapping with ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements) .....</b>	<b>176</b>
C.1	General .....	176
C.2	Mapping.....	176
	<b>Annex D (informative) Mapping with Security Evaluation Standard for IoT Platforms (SESIP) .....</b>	<b>180</b>
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**

Preview document is a preview generated by EVS

## 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.

## 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.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp/>
- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp/>

### 3.1

#### access control mechanism

equipment functionality to grant, restrict or deny access to specific equipment's *resources*

Note 1 to entry: Access to specific equipment's resources can amongst others be:

- reading specific data; or
- writing specific data to equipment's persistent storage; or
- performing a specific equipment functionality such as recording audio.

### 3.2

#### authentication

provision of assurance that an *entity* is who or what it claims to be

Note 1 to entry: An entity can amongst others claim to be:

- a specific human, owner of a user account, device, or service; or
- a member of specific groups such as an authorized group to access a specific equipment's resource; or
- authorized by another entity to access a specific equipment's resource.

### 3.3

#### authentication mechanism

equipment functionality to verify that an *entity* is who or what it claims to be

Note 1 to entry: Typically, the verification is based on examining evidence from one or more elements of the categories:

- knowledge; and
- possession; and