
Skupne varnostne zahteve za radijsko opremo - 2. del: Radijska oprema za obdelavo podatkov, in sicer radijska oprema, povezana z internetom, radijska oprema za varstvo otrok, radijska oprema za igrače in nosljiva radijska oprema

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

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

Exigences de sécurité communes applicables aux équipements radioélectriques qui traitent des données, à savoir les équipements radioélectriques connectés à l'internet, les équipements radioélectriques destinés à la garde denfants, les jouets dotés d'une

Ta slovenski standard je istoveten z: prEN 18031-2

ICS:

33.060.01	Radijske komunikacije na splošno	Radiocommunications in general
-----------	----------------------------------	--------------------------------

oSIST prEN 18031-2:2023

en,fr,de

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 18031-2

August 2023

ICS

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 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'une

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 draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN and CENELEC 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation. Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is a draft European Standard. It is distributed as a draft and shall not be referred to as a standard.

subject to change without notice.



16	Contents	Page
17		
18	European foreword	4
19	Introduction	5
20	1 Scope	6
21	2 Normative references	6
22	3 Terms and definitions	6
23	4 Application of this standard	10
24	5 Requirements	12
25	5.1 [ACM] Access control mechanism	12
26	5.1.1 [ACM-1] Applicability of access control mechanisms	12
27	5.1.2 [ACM-2] Appropriate access control mechanisms	16
28	5.1.3 [ACM-3] Default access control for children in toys	19
29	5.1.4 [ACM-4] Default access control to children’s privacy assets for toys and childcare equipment	23
30	5.1.5 [ACM-5] Parental/Guardian access controls for children in toys	27
31	5.1.6 [ACM-6] Parental/Guardian access controls for children’s privacy assets in toys	31
32	5.2 [AUM] Authentication mechanism	35
33	5.2.1 [AUM-1] Applicability of authentication mechanisms for external interfaces	35
34	5.2.2 [AUM-2] Appropriate authentication mechanisms for external interfaces	42
35	5.2.3 [AUM-3] Authenticator validation	46
36	5.2.4 [AUM-4] Changing authenticators	49
37	5.2.5 [AUM-5] Preventing static and default values	52
38	5.2.6 [AUM-6] Brute force protection	56
39	5.3 [SUM] Secure update mechanism	59
40	5.3.1 [SUM-1] Applicability of update mechanisms	59
41	5.3.2 [SUM-2] Secure updates	62
42	5.3.3 [SUM-3] Automated updates	66
43	5.4 [SSM] Secure storage Mechanism	69
44	5.4.1 [SSM-1] Applicability of secure storage mechanisms	69
45	5.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms	72
46	5.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms	75
47	5.5 [SCM] Secure communication mechanism	78
48	5.5.1 [SCM-1] Applicability of secure communication mechanisms	78
49	5.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	82
50	5.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms	85
51	5.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms	89
52	5.6 [LGM] Logging Mechanism	93
53	5.6.1 [LGM-1] Applicability of logging mechanisms	93
54	5.6.2 [LGM-2] Appropriate Logging mechanisms	96
55	5.6.3 [LGM-3] Appropriate Logging mechanisms – Minimum number of events	100
56	5.6.4 [LGM-4] Appropriate Logging mechanisms – Time related information	103
57	5.7 [DLM] Deletion mechanism	106

61	5.7.1	[DLM-1] Applicability of and appropriate deletion mechanisms.....	106
62	5.8	[UNM] User notification mechanism.....	110
63	5.8.1	[UNM-1] Applicability of user notification mechanisms	110
64	5.8.2	[UNM-2] Content of user notification	115
65	5.9	[CCK] Confidential cryptographic keys.....	117
66	5.9.1	[CCK-1] Appropriate Confidential cryptographic keys (CCKs).....	117
67	5.9.2	[CCK-2] Confidential cryptographic key generation mechanisms.....	120
68	5.9.3	[CCK-3] No hard-coded confidential cryptographic keys.....	122
69	5.9.4	[CCK-4] Preventing static default values for confidential cryptographic keys	124
70	5.10	[GEC] General equipment capabilities	128
71	5.10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities.....	128
72			
73	5.10.2	[GEC-2] Limit exposure of services via related network interfaces	130
74	5.10.3	[GEC-3] Configuration of optional services and the related exposed network interfaces.....	133
75			
76	5.10.4	[GEC-4] Documentation of exposed services via network interfaces	135
77	5.10.5	[GEC-5] No unnecessary external interfaces.....	137
78	5.10.6	[GEC-6] Documentation of external sensing capabilities.....	139
79	5.10.7	[GEC-7] Input validation.....	141
80	5.11	[CRY] Cryptography	145
81	5.11.1	[CRY-1] Best practice Cryptography	145
82		Annex A (informative) Rationale	150
83	A.1	General	150
84	A.2	Rationale.....	150
85	A.2.1	Family of standards	150
86	A.2.2	Security by design.....	150
87	A.2.3	Assets	151
88	A.2.4	Mechanisms	151
89	A.2.5	Assessment criteria	151
90	A.2.5.1	Decision trees.....	152
91	A.2.5.2	Technical documentation	152
92	A.2.5.3	Security testing.....	154
93	A.2.6	Security parameters	154
94		Annex ZA (informative)	155
95		Table ZA.1 — Correspondence between this European Standard and Directive 2014/53/EU	
96		[OJ L 153]	155
97		Bibliography	156

98

99

prEN 18031-2:2023 (E)**100 European foreword**

101 This document (prEN 18031-2:2023) has been prepared by Technical Committee CEN/CENELEC JTC
102 13/WG 8 “Special Working Group RED Standardization Request”, the secretariat of which is held by NEN.

103 This document is currently submitted to the CEN Enquiry.

104 This document has been prepared under a mandate given to CEN/CENELEC by the European Commission
105 and the European Free Trade Association and supports essential requirements of EU Directive(s) /
106 Regulation(s).

107 For relationship with EU Directive(s) / Regulation(s), see informative Annex ZA, which is an integral part
108 of this document.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN 18031-2:2023](https://standards.iteh.ai/catalog/standards/sist/5a44ec14-755e-4b14-8135-27d62ca8aa5e/osist-pren-18031-2-2023)

<https://standards.iteh.ai/catalog/standards/sist/5a44ec14-755e-4b14-8135-27d62ca8aa5e/osist-pren-18031-2-2023>

109 **Introduction**

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

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN 18031-2:2023](https://standards.iteh.ai/catalog/standards/sist/5a44ec14-755e-4b14-8135-27d62ca8aa5e/osist-pren-18031-2-2023)

<https://standards.iteh.ai/catalog/standards/sist/5a44ec14-755e-4b14-8135-27d62ca8aa5e/osist-pren-18031-2-2023>

prEN 18031-2:2023 (E)**1 Scope**

Common security requirements for radio equipment processing personal data or traffic data or location data being either internet connected radio equipment, radio equipment designed or intended exclusively for childcare; toys and wearable radio equipment. The standard provides technical specifications for radio equipment processing personal data, traffic data or location data, which concerns electrical or electronic products that are capable to communicate over the internet, regardless of whether these products communicate directly or via any other equipment, childcare, toys or wearable radio equipment.

The scope does not apply to 5G network equipment used by providers of public electronic communications networks and publicly available electronic communications services within the meaning of in Directive (EU) 2018/1972 of the European Parliament and of the Council as defined in that Regulation.

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.

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

- 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

Note1 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

3.3 authentication mechanism
equipment functionality to verify 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.

152 Note 2 to entry: Typically, the verification is based on examining evidence from one or more elements of the
153 categories:

154 — knowledge; and

155 — possession; and

156 — inherence.

157 **3.4**

158 **authenticator**

159 means used to validate the claim of an *entity*

160 EXAMPLE: A password or token may be used as an authenticator.

161 **3.5**

162 **best practice**

163 measures that have been shown to provide appropriate security for the corresponding use case

164 **3.6**

165 **brute force attack**

166 method based on trial-and-error to guess the right *authenticator*

167 **3.7**

168 **communication mechanism**

169 *equipment* functionality that allows communication via a device *interface*

170 **3.8**

171 **confidential security parameters**

172 secret security related information whose modification or disclosure can compromise the security of an
173 asset

174 **3.9**

175 **denial of service (DoS)**

176 prevention or interruption of authorized access to an equipment resource or the delaying of equipment
177 operations and functions

178 [SOURCE : IEC 62443-1-1 :2019, 3.2.42] modified

179 **3.10**

180 **entity**

181 user, device or service

182 **3.11**

183 **equipment**

184 **radio equipment**

185 electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose
186 of radio communication and/or radio determination, or an electrical or electronic product which must be
187 completed with an accessory, such as an antenna, to intentionally emit and/or receive radio waves for
188 the purpose of radio communication and/or radio determination

189 [SOURCE: Directive 2014/53/EU, article 2.1(1)]

190 **3.12**

191 **external interface**

192 *interface* on the *equipment* that is accessible from outside the *equipment*

prEN 18031-2:2023 (E)

193 **3.13**
 194 **factory default state**
 195 defined state where the configuration settings and configuration of the equipment is set to initial values
 196 typically set when it leaves the manufacturing factory

197 Note 1 to entry: a factory default state may include security updates, installed after the equipment being placed on
 198 the market.

199 **3.14**
 200 **initialization**
 201 process that configures the network connectivity of the *equipment* for operation

202 Note 1 to entry: Initialization may provide the possibility to configure authentication features for a user or for
 203 network access

204 **3.15**
 205 **interface**
 206 shared boundary across which *entities* exchange information

207 **3.16**
 208 **legacy**
 209 *equipment*, software/hardware component, cryptography or communication protocol that cannot be
 210 protected against current cybersecurity threats without mitigating measures

211 **3.17**
 212 **log data**
 213 record(s) of certain events (of processes) on a computing *equipment*

214 **3.18**
 215 **machine interface**
 216 *external interface* between the *equipment* and a service or device

217 **3.19**
 218 **network interface**
 219 *external interface* enabling the *equipment* to have or provide access to a network

220 Note 1 to entry: Examples for network interfaces are a LAN port (wired) or a wireless network interface enabling
 221 WLAN or Bluetooth communication, e.g., using a 2.4 GHz antenna.

222 **3.20**
 223 **operational state**
 224 state in which the *equipment* is functioning normally providing its intended use and within its intended
 225 operational environment of use

226 **3.21**
 227 **optional services**
 228 services which are not necessary to setup the *equipment*, and which are not part of the basic functionality
 229 but are still relevant for the intended use of the *equipment* and are delivered as part of the factory default.
 230 Example: an SSH service on the equipment is not required for basic functionality of the equipment, but it may be
 231 used to allow a remote access to the equipment

- 232 **3.22**
 233 **password**
 234 sequence of characters (letters, numbers, or other symbols) used to authenticate an *entity*
 235 Note 1 to entry: personal identification numbers (PINs) are also considered a form of password
- 236 **3.23**
 237 **personal information**
 238 personal data, traffic data or location data
- 239 **3.24**
 240 **privacy asset**
 241 *privacy functions*, or *privacy functions* configuration used by the *equipment*, or *personal information*
 242 stored, communicated or otherwise processed by the *equipment*, or *sensitive security parameter* stored at
 243 the *equipment* for access to personal information or *privacy functions*
- 244 **3.25**
 245 **privacy function**
 246 *equipment's* functionality that can directly affect the privacy of users or subscribers
- 247 **3.26**
 248 **privacy functions configuration**
 249 data that defines the behaviour of the *equipment's privacy functions*
- 250 **3.27**
 251 **public security parameters**
 252 security related public information whose modification can compromise the security of an asset
- 253 **3.28**
 254 **resilient**
 255 able to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or
 256 compromises on systems that use or are enabled by cyber resources.
- 257 [SOURCE: NIST Glossary: https://csrc.nist.gov/glossary/term/cyber_resiliency]
<https://standards.iteh.ai/catalog/standards/sist/3a44ec14-755e-4614-8155-27d62ca3aa3e/osist-pren-18031-2-2023>
- 258 **3.29**
 259 **risk**
 260 combination of the probability of occurrence of harm and the severity of that harm
- 261 [SOURCE: ISO/IEC Guide 51:2014]
- 262 **3.30**
 263 **security asset**
 264 *equipment's* security functionality that can directly affect the *equipment's* integrity, or *security relevant*
 265 *configuration* used by the *equipment*, or *sensitive security parameter* for *equipment's* integrity used by the
 266 *equipment*
- 267 **3.31**
 268 **security relevant configuration**
 269 data that affects the behaviour of the *equipment's* security functionality
- 270 **3.32**
 271 **sensitive security parameters**
 272 *confidential security parameter* for an asset or *public security parameter* for an asset

prEN 18031-2:2023 (E)

- 273 **3.33**
 274 **security update**
 275 software update that addresses security vulnerabilities through code patches or other mitigations
- 276 **3.34**
 277 **storage mechanism**
 278 *equipment* functionality that allows to store information
- 279 **3.35**
 280 **update mechanism**
 281 *equipment* functionality that allows to change *equipment's* software
- 282 **3.36**
 283 **user interface**
 284 *external interface* between the *equipment* and a user
- 285 **3.37**
 286 **vulnerability**
 287 weakness, design, or implementation error that can lead to an unexpected, undesirable event
 288 compromising the security of the *equipment*, network, application, or protocol involved.
- 289 [SOURCE: (ITSEC) (definition given by ENISA, "computer system" has been replaced by "equipment")]

4 Application of this document

291 This document uses the concept of mechanism to instruct the user of this standard when to apply certain
 292 security measures. Mechanisms address the applicability and appropriateness through a set of
 293 requirements including assessment criteria. The pass/fail decision is made for each of the items specified,
 294 for example when checking the applicability of a requirement on external interfaces, then the decision
 295 whether the requirement and all further requirements need to be fulfilled is determined for each external
 296 interface independently.

297 The mechanisms are documented using the following structure and how to apply them:

298 <https://standards.iteh.ai/catalog/standards/sist/5a44155e-4b14-8135-27d62ca8aa5e/osist-pren-18031-2-2023> **Table 1**

Clause #	Title	Description on how to apply the standard
5.x	XXX Mechanism	Mechanism for each specific item (e.g., external interface or security asset)
5.x.1	XXX-1 Applicability of mechanisms	Applicability of the mechanism
5.x.1.1	Requirement	For each specific item determine and assess if the mechanism is required. NOTE A mechanism might combine applicability and appropriateness in a single requirement.
5.x.1.2	Rationale	
5.x.1.3	Guidance	
5.x.1.4	Assessment criteria	
5.x.1.4.1	Assessment objective	
5.x.1.4.2	Required information	
5.x.1.4.3	Conceptual assessment	
5.x.1.4.4	Functional completeness assessment	
5.x.1.4.5	Functional sufficiency assessment	

Clause #	Title	Description on how to apply the standard
5.x.2	XXX-2 Appropriate mechanisms	Appropriateness of the mechanism
5.x.2.1	Requirement	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the mechanism is implemented sufficiently. NOTE A mechanism might have multiple appropriateness sub-clauses to focus on specific properties.
5.x.2.2	Rationale	
5.x.2.3	Guidance	
5.x.2.4	Assessment criteria	
5.x.2.4.1	Assessment objective	
5.x.2.4.2	Required information	
5.x.2.4.3	Conceptual assessment	
5.x.2.4.4	Functional completeness assessment	
5.x.2.4.5	Functional sufficiency assessment	
5.x.y	XXX-# Supporting Requirements	Applicability and appropriateness of supporting requirements for the mechanism
5.x.y.1	Requirement	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the supporting requirement needs to be implemented (there might be specific conditions, for instance if the equipment is a toy) and if it needs to be implemented, whether it is implemented sufficiently.
5.x.y.2	Rationale	
5.x.y.3	Guidance	
5.x.y.4	Assessment criteria	
5.x.y.4.1	Assessment objective	
5.x.y.4.2	Required information	
5.x.y.4.3	Conceptual assessment	
5.x.y.4.4	Functional completeness assessment	
5.x.y.4.5	Functional sufficiency assessment	

299 The assessments are conducted by examining the documented assessment cases, not all assessment cases
300 might be provided for every mechanism:

301 — Conceptual assessment

302 Examine if the provided documentation and rationale adequately provides the required evidence
303 (for example the rationale why a mechanism is not applicable for a specific network interface).

304 — Functional completeness assessment

305 Examine and test if the provided documentation is complete (for example use network scanners
306 to verify that all external interfaces are properly identified, documented and assessed)

307 — Functional sufficiency assessment

308 Examine and test if the implementation is adequate (for example run fuzzing tools on a network
309 interface to check if it is resilient to attacks with malformed data)

prEN 18031-2:2023 (E)

310 Each of the assessments is further divided into the following sub-clauses which might use a decision tree
311 to guide the assessment:

- 312 — Assessment purpose
- 313 — Preconditions
- 314 — Assessment units
- 315 — Assignment of verdict

316 Required information lists the information that is to be provided through technical documentation. The
317 standard does not require each required information element to be provided as a separate document.

318 5 Requirements**319 5.1 [ACM] Access control mechanism****320 5.1.1 [ACM-1] Applicability of access control mechanisms****321 5.1.1.1 Requirement**

322 The equipment shall use access control mechanisms to manage entities access to security assets and
323 privacy assets, unless for security or privacy assets where:

- 324 — its full public accessibility is the “equipment’s reasonably foreseeable and intended use”; or
- 325 — the “foreseeable and intended operational environment of use” ensures that its accessibility is
326 limited to authorized entities.

327 5.1.1.2 Rationale

328 Security and privacy assets exposed to unauthorized access attempts. Access control mechanisms limit
329 the ability of any unauthorized entity to access these assets.

330 5.1.1.3 Guidance

331 The requirement does not demand access control mechanisms on assets that it does not cover (for
332 example, the dispense button on a coffee machine). Further it does not demand access control
333 mechanisms for assets that are in principle covered, but where the reasonably foreseeable and intended
334 use is to be generally accessible by the public or where the foreseeable and intended operational
335 environment of use ensures that only authorized access is possible.

336 However, generally publicly accessibility to privacy assets cannot be considered as reasonably
337 foreseeable use, especially concerning children’s privacy and childcare.

338 Note that radio interfaces might be accessible even if the equipment is in a trusted environment, for
339 instance a wireless network is often accessible from outside a user’s home.

340 For example, depending on the equipment’s technical properties, foreseeable and intended use and
341 foreseeable and intended operational environment of use access control mechanisms might not be
342 necessary for relevant assets where:

- 343 — all entities with access to the equipment (the equipment is intended to be operated in an area
344 which has physical access control) are authorized to access these assets (for example, the WPS
345 button on a home router);