

SLOVENSKI STANDARD oSIST prEN 18031-3:2023

01-november-2023

Skupne varnostne zahteve za radijsko opremo - 3. del: Z internetom povezana radijska oprema, ki obdeluje virtualni denar ali denarno vrednost

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

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

Exigences de sécurité communes applicables aux équipements radioélectriques connectés à linternet qui traitent une monnaie virtuelle ou de la valeur monétaire

Ta slovenski standard je istoveten z: prEN 18031-3

ICS:

33.060.01 Radijske komunikacije na

splošno

Radiocommunications in

general

oSIST prEN 18031-3:2023

en,fr,de

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

<u>oSIST prEN 18031-3:2023</u>

https://standards.iteh.ai/catalog/standards/sist/f2e1060d-ad6d-459a-8a07-1c7e3113d070/osist-pren-18031-3-2023

EUROPEAN STANDARD NORME EUROPÉENNE EUROPÄISCHE NORM

DRAFT prEN 18031-3

August 2023

ICS

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 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 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 not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.





16	Cont	ents	Page
17			
18	Europ	ean foreword4	4
19	Introd	uction5	5
20	1	Scope	6
21	2	Normative references	
22	3	Terms and definitions	
23	4	Application of this standard10	
24	5	Requirements	
25	5.1	[ACM] Access control mechanism	
26	5.1.1	[ACM-1] Applicability of access control mechanisms	
27	5.1.2	[ACM-2] Appropriate access control mechanisms	
28	5.2	[AUM] Authentication mechanism	
29	5.2.1	[AUM-1] Applicability of authentication mechanisms for external interfaces	
30 31	5.2.2 5.2.3	[AUM-3] Authenticator validation29	
32	5.2.3 5.2.4	[AUM-4] Changing authenticators	
33	5.2.5	[AUM-5] Preventing static and default values35	<u>.</u>
34	5.2.6	[AUM-6] Brute force protection))
35	5.3	[SUM] Secure update mechanism43	
36	5.3.1	[SUM-1] Applicability of update mechanisms43	
37	5.3.2	[SUM-2] Secure updates46	
38	5.3.3	[SUM-3] Automated updates	
39	5.4	[SSM] Secure storage Mechanism53	
40	5.4.1	[SSM-1] Applicability of secure storage mechanisms53	
41	5.4.2	[SSM-2] Appropriate integrity protection for secure storage mechanisms	
42	5.4.3	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms59	
43	5.5	[SCM] Secure communication mechanism62	
44	5.5.1	[SCM-1] Applicability of secure communication mechanisms62	2
45	5.5.2	[SCM-2] Appropriate integrity and authenticity protection for secure communication	n
46		mechanisms66	
47	5.5.3	[SCM-3] Appropriate confidentiality protection for secure communication	
48		mechanisms69	
49	5.5.4	[SCM-4] Appropriate replay protection for secure communication mechanisms73	
50	5.6	[LGM] Logging Mechanism	
51	5.6.1	[LGM-1] Applicability of logging mechanisms	
52	5.6.2	[LGM-2] Appropriate Logging mechanisms80	
53	5.6.3	[LGM-3] Appropriate Logging mechanisms – Minimum number of events84	
54	5.6.4	[LGM-4] Appropriate Logging mechanisms – Time related information87	
55	5.7	[CCK] Confidential cryptographic keys	
56	5.7.1	[CCK-1] Appropriate Confidential cryptographic keys (CCKs)	
57	5.7.2	[CCK-2] Confidential cryptographic key generation mechanisms	
58 59	5.7.3 5.7.4	[CCK-3] No hard-coded confidential cryptographic keys95 [CCK-4] Preventing static default values for confidential cryptographic keys97	
39	5./.4	[CCK-4] Freventing static default values for confidential cryptographic Reys97	<i>(</i>

[GEC] General equipment capabilities100

5.8

60

61	5.8.1	[GEC-1] Up-to-date software and hardware with no publicly known exploit	able
62		vulnerabilities	100
63	5.8.2	[GEC-2] Limit exposure of services via related network interfaces	103
64	5.8.3	[GEC-3] Configuration of optional services and the related exposed network	vork
65		interfaces	
66	5.8.4	[GEC-4] Documentation of exposed services via network interfaces	108
67	5.8.5	[GEC-5] No unnecessary external interfaces	109
68	5.8.6	[GEC-7] Input validation	112
69	5.9	[CRY] Cryptography	
70	5.9.1	[CRY-1] Best practice Cryptography	116
71	Annex	x A (informative) Rationale	121
72	A.1	General	121
73	A.2	Rationale	121
74	A.2.1	Family of standards	
75	A.2.2	Security by design	
76	A.2.3	Assets	121
77	A.2.4	Mechanisms	122
78	A.2.5	Assessment criteria	122
79	A.2.5. 1	1 Decision trees	123
80	A.2.5.2	2 Technical documentation	123
81	A.2.5.3	3 Security testing	125
82	A.2.6	Security parameters	125
83	Annex	x ZA [D][E][F] (informative)	126
84 85	Table	ZA.1 — Correspondence between this European Standard and Directive 2014/53 [OJ L 153]	
86	Biblio	graphy Document Preview	127
87			
88			
00			

89

European foreword

- 91 This document (prEN 18031-3:2023) has been prepared by Technical Committee CEN/CENELEC JTC
- 92 13/WG 8 "Special Working Group RED Standardization Request", the secretariat of which is held by NEN.
- 93 This document is currently submitted to the CEN Enquiry.
- This document has been prepared under a mandate given to CEN/CENELEC by the European Commission
- 95 and the European Free Trade Association and supports essential requirements of EU Directive(s) /
- 96 Regulation(s).

90

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

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

oSIST prEN 18031-3:2023

https://standards.iteh.ai/catalog/standards/sist/f2e1060d-ad6d-459a-8a07-1c7e3113d070/osist-pren-18031-3-2022

Introduction

99

It is important to note that in order to achieve the overall cybersecurity of radio equipment, defence in
depth best practices will be needed. In particular, no one 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 lists
must be read only as indicative possibilities: 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.

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

oSIST prEN 18031-3:2023

https://standards.iteh.ai/catalog/standards/sist/f2e1060d-ad6d-459a-8a07-1c7e3113d070/osist-pren-18031-3-2027

107	1 Scope		
108 109 110 111 112	Common security requirements for internet connected radio equipment that equipment enables the holder or user to transfer money, monetary value or virtual currency. This document provides technical specifications for radio equipment processing virtual money or monetary value, which apply to electrical or electronic products that are capable to communicate over the internet, regardless of whether these products communicate directly or via any other equipment.		
113	2 Normative references		
114	There are no normative references in this document.		
115	3 Terms and definitions		
116	For the purposes of this document, the following terms and definitions.		
117	ISO and IEC maintain terminological databases for use in standardization at the following addresses:		
118	 IEC Electropedia: available at https://www.electropedia.org/ 		
119	 — ISO Online browsing platform: available at https://www.iso.org/obp/ 		
120 121 122	3.1 access control mechanism equipment functionality to grant, restrict or deny access to specific equipment's resources		
123	Note 1 to entry: Access to specific equipment's resources can amongst others be:		
124	— reading specific data; or https://standards.iteh.ai		
125	 writing specific data to equipment's persistent storage; or 		
126	 performing a specific equipment functionality such as recording audio. 		
127 128 129	3.2 authentication and an entity is who or what it claims to be		
130 131 132	3.3 authentication mechanism equipment functionality to verify that an entity is who or what it claims to be		
133	Note 1 to entry: An entity can amongst others claim to be:		
134	- a specific human, owner of a user account, device, or service; or		
135	- a member of specific groups such as an authorized group to access a specific equipment's resource; or		
136	- authorized by another entity to access a specific equipment's resource.		
137 138	Note 2 to entry: Typically, the verification is based on examining evidence from one or more elements of the categories:		
139	- knowledge; and		
140	- possession; and		
141	- inherence.		

142 143	3.4 authenticator
144	means used to validate the claim of an <i>entity</i>
145	EXAMPLE: A password or token may be used as an authenticator.
146 147	3.5 best practice
148	measures that have been shown to provide appropriate security for the corresponding use case
149 150	3.6 brute force attack
151	method based on trial-and-error to guess the right authenticator
152	3.7
153 154	communication mechanism equipment functionality that allows communication via a device interface
155	3.8
156	confidential security parameters
157 158	secret security related information whose modification or disclosure can compromise the security of an asset
159	3.9
160	denial of service (DoS)
161 162	prevention or interruption of authorized access to an equipment resource or the delaying of equipment operations and functions
163	[SOURCE: IEC 62443-1-1:2019, 3.2.42] modified
164	3.10 Document Preview
165	entity
166	user, device or service <u>oSIST prEN 18031-3:2023</u>
167	:// <mark>3.11</mark> lards.iteh.ai/catalog/standards/sist/f2e1060d-ad6d-459a-8a07-1c7e3113d070/osist-pren-18031-3-20
168	equipment
169	radio equipment
170 171	electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radio determination, or an electrical or electronic product which must be
172	completed with an accessory, such as an antenna, to intentionally emit and/or receive radio waves for
173	the purpose of radio communication and/or radio determination
174	[SOURCE: Directive 2014/53/EU, article 2.1(1)]
175	3.12
176	external interface
177	interface on the equipment that is accessible from outside the equipment

178 179 180 181	3.13 factory default state defined state where the configuration settings and configuration of the equipment is set to initial values typically set when it leaves the manufacturing factory
182 183	Note 1 to entry: a factory default state may include security updates, installed after the equipment being placed on the market.
184 185 186	3.14 financial asset - financial functions,
187	- financial functions configuration used by the equipment
188	- financial data stored, transmitted or otherwise processed by the equipment or
189 190	- sensitive security parameter stored at the equipment for access to financial functions, financial functions configuration and financial data
191 192 193 194	3.15 financial data data that represents, provides information about, or is processed for transferring money, monetary assets or virtual currencies
195 196 197	3.16 financial function equipment's functionality that can directly affect the financial data
198 199 200	3.17 financial functions configuration data that defines the behaviour of the equipment's financial functions
201 202 203	3.18 oSIST prEN 18031-3:2023 initialization in the ai/catalog/standards/sist/f2e1060d-ad6d-459a-8a07-1c7e3113d070/osist-pren-18031-3-process that configures the network connectivity of the <i>equipment</i> for operation
204 205	Note 1 to entry: Initialization may provide the possibility to configure authentication features for a user or for network access
206 207 208	3.19 interface shared boundary across which <i>entities</i> exchange information
209 210 211 212	3.20 legacy equipment, software/hardware component, cryptography or communication protocol that cannot be protected against current cybersecurity threats without mitigating measures
213 214 215	3.21 log data record(s) of certain events (of processes) on a computing equipment

216217218	3.22 machine interface external interface between the equipment and a service or device		
219 220	3.23 network interface		
221	external interface enabling the equipment to have or provide access to a network		
222 223	Note 1 to entry: Examples for network interfaces are a LAN port (wired) or a wireless network interface enabling WLAN or Bluetooth communication, e.g., using a 2.4 GHz antenna.		
224	3.24		
225226227	operational state state in which the <i>equipment</i> is functioning normally providing its intended use and within its intended operational environment of use		
228 229 230	3.25 optional services services which are not necessary to setup the <i>equipment</i> , and which are not part of the basic functionality		
231	but are still relevant for the intended use of the equipment and are delivered as part of the factory default.		
232 233	Example: an SSH service on the equipment is not required for basic functionality of the equipment, but it may b used to allow a remote access to the equipment		
234	3.26		
235	password		
236 237	sequence of characters (letters, numbers, or other symbols) used to authenticate an <i>entity</i> Note: personal identification numbers (PINs) are also considered a form of password		
238	3.27 (https://standards.iten.ai)		
239 240	public security parameters security related public information whose modification can compromise the security of an asset		
241	3.28 oSIST prEN 18031-3:2023		
242	resilient iteh ai/catalog/standards/sist/f2e1060d-ad6d-459a-8a07-1c7e3113d070/osist-prep-18031-3-20/		
243 244	able to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.		
245	[SOURCE: NIST Glossary: https://csrc.nist.gov/glossary/term/cyber_resiliency]		
246	3.29		
247	risk		
248	combination of the probability of occurrence of harm and the severity of that harm		
249	[SOURCE: ISO/IEC Guide 51:2014]		
250	3.30		
251	security asset		
252	equipment's security functionality that can directly affect the equipment's integrity, or security relevant		
253 254	configuration used by the <i>equipment</i> , or <i>sensitive security parameter</i> for <i>equipment's</i> integrity used by the <i>equipment</i>		
255	3.31		
256	security relevant configuration		
257	data that affects the behaviour of the <i>equipment's</i> security functionality		

חדת	2 2 2
258	3.32

- 259 **sensitive security parameters**
- 260 confidential security parameter for an asset or public security parameter for an asset
- 261 **3.33**

263

266

269

272

278

279

280 281

282

283284

285

- 262 **security update**
 - software update that addresses security vulnerabilities through code patches or other mitigations
- 264 **3.34**
- 265 **storage mechanism**
 - *equipment* functionality that allows to store information
- 267 **3.35**
- 268 update mechanism
 - equipment functionality that allows to change equipment's software
- **270 3.36**
- 271 user interface
 - external interface between the equipment and a user
- 273 **3.37**
- 274 vulnerability
- weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the *equipment*, network, application, or protocol involved.
- 277 [SOURCE: (ITSEC) (definition given by ENISA, "computer system" has been replaced by "equipment")]

This standard uses the concept of mechanism to instruct the user of this standard when to apply certain security measures. Mechanisms address the applicability and appropriateness through a set of requirements including assessment criteria. The pass/fail decision is made for each of the items specified, for example when checking the applicability of a requirement on external interfaces, then the decision whether the requirement and all further requirements need to be fulfilled is determined for each external 3-2023 interface independently.

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

286 **Table 1**

Clause #	Title		Description on how to apply the standard	
5.x	XX	X Mechanism	Mechanism for each specific item (e.g., external interface or security asset)	
5.x.1	XX	X-1 Applicability of mechanisms	Applicability of the mechanism	
5.x.1.1	Red	quirement	For each specific item determine and assess	
5.x.1.2 Rationale		tionale	if the mechanism is required. Note: A mechanism might combine applicability and appropriateness in a single	
5.x.1.3	Guidance			
5.x.1.4	Ass	sessment criteria	requirement.	
5.x.1.4.1		Assessment objective		
5.x.1.4.2		Required information		

Clause #	Tit	le	Description on how to apply the standard
5.x.1.4.3		Conceptual assessment	
5.x.1.4.4		Functional completeness assessment	
5.x.1.4.5		Functional sufficiency assessment	
5.x.2	XX	X-2 Appropriate mechanisms	Appropriateness of the mechanism
5.x.2.1	Re	quirement	For each specific item for which the
5.x.2.2	Ra	tionale	mechanism is required as determined by XXX-1, determine and assess if the
5.x.2.3	Gu	idance	mechanism is implemented sufficiently.
5.x.2.4	Ass	sessment criteria	Note: A mechanism might have multiple
5.x.2.4.1		Assessment objective	appropriateness sub-clauses to focus on specific properties.
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 Toh Stand		For each specific item for which the
5.x.y.2	Rationale		mechanism is required as determined by XXX-1, determine and assess if the
5.x.y.3	Guidance Mttps://Standar		supporting requirement needs to be
5.x.y.4	Assessment criteria		implemented (there might be specific conditions, for instance if the equipment is a
5.x.y.4.1		Assessment objective	toy) and if it needs to be implemented,
5.x.y.4.2		Required information IST prEN 18031-	whether it is implemented sufficiently.
5.x.y.4.3	eh.ai	Conceptual assessment 060d-ad6d-45	9a-8a07-1c7e3113d070/osist-pren-18031-3-20
5.x.y.4.4		Functional completeness assessment	
5.x.y.4.5		Functional sufficiency assessment	

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

Conceptual assessment

289

290

291

292

293

294295

296297

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

Functional completeness assessment

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

Functional sufficiency assessment

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

298 299	Each of the assessments is further divided into the following sub-clauses which might use a decision tree to guide the assessment:
300	Assessment purpose
301	— Preconditions
302	 Assessment units
303	 Assignment of verdict
304 305	Required information lists the information that is to be provided through technical documentation. The standard does not require each required information element to be provided as a separate document.
306	5 Requirements
307	5.1 [ACM] Access control mechanism
308	5.1.1 [ACM-1] Applicability of access control mechanisms
309	5.1.1.1 Requirement
310 311	The equipment shall use access control mechanisms to manage entities access to security assets and financial assets, unless for security or financial assets where:
312	 its full public accessibility is "equipment's reasonably foreseeable and intended use"; or
313 314	 the "foreseeable and intended operational environment of use" ensures that its accessibility is limited to authorized entities.
315	5.1.1.2 Rationale Document Preview
316 317	Security and financial assets are exposed to unauthorized access attempts. Access control mechanisms limit the ability of any unauthorized entity to access these assets.
318	5.1.1.3 tan Guidance ai/catalog/standards/sist/f2e1060d-ad6d-459a-8a07-1c7e3113d070/osist-pren-18031-3-
319 320 321 322 323	The requirement does not demand access control mechanisms on assets that it does not cover (for example, the dispense button on a coffee machine). Further it does not demand access control mechanisms for assets that are in principle covered, but where the reasonably foreseeable and intended use is to be generally accessible by the public or where the foreseeable and intended operational environment of use ensures that only authorized access is possible.
324 325	Note that radio interfaces might be accessible even if the equipment is in a trusted environment, for instance a wireless network is often accessible from outside a user's home.
326 327 328	For example, depending on the equipment's technical properties, foreseeable and intended use and foreseeable and intended operational environment of use access control mechanisms might not be necessary for relevant assets where:
329 330 331	 all entities with access to the equipment (the equipment is intended to be operated in an area which has physical access control) are authorized to access these assets (for example, the WPS button on a home router);

the equipment's functionality only provides information (on assets) that is intended to be publicly accessible (for instance broadcasting Bluetooth advertising beacons).

332333