SLOVENSKI STANDARD
oSIST prEN 18031-2:2023

01-november-2023

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 linternet, les équipements radioélectriques destinés à la garde denfants, les jouets dotés dune

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.

Contents

Page

European foreword

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

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 and the European Free Trade Association and supports essential requirements of EU Directive(s) / Regulation(s).

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

Introduction

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.

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.

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

- knowledge; and
- possession; and
- inherence.

3.4
authenticator
means used to validate the claim of an *entity*

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

3.5
best practice
measures that have been shown to provide appropriate security for the corresponding use case

3.6
brute force attack
method based on trial-and-error to guess the right *authenticator*

3.7
communication mechanism
equipment functionality that allows communication via a device *interface*

3.8
confidential security parameters
secret security related information whose modification or disclosure can compromise the security of an asset

3.9
denial of service (DoS)
prevention or interruption of authorized access to an equipment resource or the delaying of equipment operations and functions

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

3.10
entity
user, device or service

3.11
equipment
radio equipment
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 completed with an accessory, such as an antenna, to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radio determination

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

3.12
external interface
interface on the *equipment* that is accessible from outside the *equipment*

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

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

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

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

3.15
interface
shared boundary across which *entities* exchange information

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

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

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

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

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.

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

3.21
optional services
services which are not necessary to setup the *equipment*, and which are not part of the basic functionality but are still relevant for the intended use of the *equipment* and are delivered as part of the factory default.

Example: an SSH service on the equipment is not required for basic functionality of the equipment, but it may be used to allow a remote access to the equipment

3.22
password
sequence of characters (letters, numbers, or other symbols) used to authenticate an *entity*

Note 1 to entry: personal identification numbers (PINs) are also considered a form of password

3.23
personal information
personal data, traffic data or location data

3.24
privacy asset
privacy functions, or *privacy functions* configuration used by the *equipment,* or *personal information* stored, communicated or otherwise processed by the *equipment,* or *sensitive security parameter* stored at the *equipment* for access to personal information or *privacy functions*

3.25
privacy function
equipment's functionality that can directly affect the privacy of users or subscribers

3.26
privacy functions configuration
data that defines the behaviour of the *equipment's privacy functions*

3.27
public security parameters
security related public information whose modification can compromise the security of an asset

3.28
resilient
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.

[SOURCE: NIST Glossary: https://csrc.nist.gov/glossary/term/cyber_resiliency]

3.29
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:2014]

3.30
security asset
equipment's security functionality that can directly affect the *equipment's* integrity, or *security relevant configuration* used by the *equipment,* or *sensitive security parameter* for *equipment's* integrity used by the *equipment*

3.31
security relevant configuration
data that affects the behaviour of the *equipment's* security functionality

3.32
sensitive security parameters
confidential security parameter for an asset or *public security parameter* for an asset

3.33
security update
software update that addresses security vulnerabilities through code patches or other mitigations

3.34
storage mechanism
equipment functionality that allows to store information

3.35
update mechanism
equipment functionality that allows to change *equipment's* software

3.36
user interface
external interface between the *equipment* and a user

3.37
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.

[SOURCE: (ITSEC) (definition given by ENISA, "computer system" has been replaced by "equipment")]

4 Application of this document

This document 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 interface independently.

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

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	

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

— Conceptual assessment

  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)

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

- Assessment purpose
- Preconditions
- Assessment units
- Assignment of verdict

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.

5 Requirements

5.1 [ACM] Access control mechanism

5.1.1 [ACM-1] Applicability of access control mechanisms

5.1.1.1 Requirement

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

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

5.1.1.2 Rationale

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

5.1.1.3 Guidance

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.

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

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.

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:

- 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);