SLOVENSKI STANDARD
SIST EN 18031-2:2024

01-oktober-2024

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 - Partie 2 : 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'équipements radioélectriques et les équipements radioélectriques portables

Ta slovenski standard je istoveten z: **EN 18031-2:2024**

ICS:

33.060.01	Radijske komunikacije na splošno	Radiocommunications in general
35.030	Informacijska varnost	IT Security

SIST EN 18031-2:2024 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 18031-2

August 2024

ICS 33.060.20

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 - Partie 2 : 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'équipements radioélectriques et les équipements radioélectriques portables

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 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.

Contents

Page

European foreword

This document (EN 18031-2:2024) 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 [36] 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 privacy 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 radio equipment [36] processing personal data [40] or traffic data [41] or location data [41] for either internet connected radio equipment [37], radio equipment designed or intended exclusively for childcare [37]; toys [39] and wearable radio equipment [37] (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/

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

— inherence.

3.4
authenticator

something known or possessed, and controlled by an *entity* that is used for *authentication*

Note 1 to entry: Typically, it is a physical device or a password.

EXAMPLE A password or token can be used as an authenticator.

3.5
assessment objective

statement, provided as part of the assessment input, which defines the reasons for performing the assessment

[SOURCE: ISO/IEC 33001:2015, 3.2.6 [29]]

3.6
best practice

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

3.7
brute force attack

attack on a cryptosystem that employs a trial-and-error search of a set of keys, *passwords* or other data

3.8
communication mechanism

equipment functionality that allows communication via a *machine interface*

3.9
confidential cryptographic key

confidential security parameter, excluding *passwords*, which is used in the operation of a cryptographic algorithm or cryptographic protocol

3.10
confidential personal information

personal information whose disclosure can compromise the user's or subscriber's privacy

3.11
confidential privacy function configuration

privacy function configuration whose disclosure can compromise the user's or subscriber's privacy

3.12
confidential security parameter

security parameter whose disclosure can compromise the user's or subscriber's privacy

3.13
denial of service

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

[SOURCE : IEC 62443-1-1 :2019, 3.2.42 [30]] modified

3.14
device

product external to the equipment

3.15
entity

user, *device*, equipment or service

3.16
entropy

measure of the disorder, randomness or variability in a closed system

3.17
external interface

interface of an equipment that is accessible from outside the equipment

Note 1 to entry: Machine, network, and user interfaces are specific types of external interfaces.

3.18
factory default state

defined state where the configuration settings and configuration of the equipment is set to initial values

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

3.19
hard-coded

software development practice of embedding data directly into the source code of a program or other executable object

3.20
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.

3.21
interface

shared boundary across which *entities* exchange information

3.22
justification

documented information providing evidence that a claim is true under the assumption of common expertise

Note 1 to entry: Such evidence can be supported for example by:

- a description of the intended equipment functionality,
- a descriptions of equipment's operational environment of use,
- a description of equipment's technical properties such as security measures
- an analysis of relevant risks related to the operation of the equipment within its reasonably foreseeable use and intended equipment functionality.

3.23
log data

record(s) of certain events (of processes) on a computing equipment

3.24
logging mechanism

equipment functionality to log internal activities

3.25
machine interface

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

3.26
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 short- range wireless communication, e.g., using a 2.4 GHz antenna.

3.27
operational state

state in which the equipment is functioning normally according to the intended equipment functionality [38] and within its intended operational environment of use

3.28
optional service

service which is not necessary to setup the equipment, and which is not part of the basic functionality but is still relevant for the intended equipment functionality [38] and is 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 can be used to allow a remote access to the equipment.

3.29
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.

3.30
personal information

personal data [40], traffic data [41] or location data [41]

3.31
personal information of special categories

personal information that is genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership

[SOURCE: based on Article 9(1) of Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [31]]

3.32
privacy asset

sensitive personal information or *confidential personal information* or *sensitive privacy function configuration* or *confidential privacy function configuration* or *privacy functions*

3.33
privacy function
equipment's functionality that processes *personal information*

3.34
privacy function configuration
data processed by the equipment that defines the behaviour of the equipment's *privacy functions*

3.35
public security parameter
sensitive security parameter that is not confidential

3.36
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 SP 800-172 [32]]

3.37
resource
functional unit or data item needed to perform required operations

[SOURCE: IEC [33]]

3.38
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:2014 [34]]

3.39
security asset
sensitive security parameter or confidential security parameter or security function

3.40
security function
measure on the equipment that ensures that the personal data and the privacy of the user and of the subscriber are protected

3.41
security parameter
data processed by the equipment that defines the behaviour of the equipment's *security function*

3.42
security strength
number associated with the amount of work that is required to break a cryptographic algorithm or system

Note 1 to entry: The amount of work can for example be the number of operations required to break a cryptographic algorithm or system.

3.43
sensitive personal information
personal information whose manipulation can compromise the user's or subscriber's privacy

3.44
sensitive privacy function configuration
privacy function configuration whose manipulation can compromise the user's or subscriber's privacy

3.45
sensitive security parameter
security parameter whose manipulation can compromise the user's or subscriber's privacy

3.46
security update
software update that addresses security vulnerabilities through *software* patches or other mitigations

3.47
software
assembly of programs, procedures, rules, documentation, and data, pertaining to the operation of an equipment

Note 1 to entry: Software also includes firmware.

3.48
storage mechanism
equipment functionality that allows to store information

3.49
update mechanism
equipment functionality that allows to change equipment's *software*

3.50
user interface
external interface between the equipment and a user

3.51
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") [35]]

4 Abbreviations

ACM access control mechanism
API application programming interface
AU assessment unit
AUM authentication mechanism
CCK confidential cryptographic key(s)
CRY cryptography
CSP confidential security parameter
CWE common weakness enumeration
DHCP dynamic host configuration protocol
DLM deletion mechanism
DN decision node
DoS denial of service
DT decision tree
E evidence