SLOVENSKI STANDARD
SIST EN 18031-1:2024

01-oktober-2024

Splošne varnostne zahteve za radijsko opremo - 1. del: Radijska oprema, povezana z internetom

Common security requirements for radio equipment - Part 1: Internet connected radio equipment

Gemeinsame Sicherheitsanforderungen für mit dem Internet verbundene Funkanlagen

Exigences de sécurité communes applicables aux équipements radioélectriques connectés à linternet

Ta slovenski standard je istoveten z: **EN 18031-1:2024**

ICS:

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

SIST EN 18031-1:2024 **en,fr,de**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 18031-1

August 2024

ICS 35.030

English version

Common security requirements for radio equipment - Part 1: Internet connected radio equipment

Exigences de sécurité communes applicables aux équipements radioélectriques - Partie 1 : Équipements radioélectriques connectés à l'internet

Gemeinsame Sicherheitsanforderungen für Funkanlagen - Teil 1: Funkanlagen mit Internetanschluss

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

European foreword

This document (EN 18031-1:2024) 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 [33] 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 assets and network 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 [34] (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 [27]]

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 network function configuration
network function configuration whose disclosure can harm the network or its functioning or can lead to misuse of network resources

3.11
confidential security parameter
security parameter whose disclosure can harm the network or its functioning or can lead to misuse of network resources

3.12
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 [28]] modified

3.13
device
product external to the equipment

3.14
entity
user, *device*, equipment or service

3.15
entropy

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

3.16
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.

3.17
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.

3.18
hard-coded

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

3.19
initialization

process that configures the network connectivity of the equipment for operation

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

3.20
interface

shared boundary across which *entities* exchange information

3.21
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; or

— a descriptions of equipment's operational environment of use; or

— a description of equipment's technical properties such as security measures; or

— an analysis of relevant risks related to the operation of the equipment within its reasonably foreseeable use and intended equipment functionality.

3.22
machine interface

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

3.23
network asset

sensitive network function configuration or *confidential network function configuration* or *network functions*

3.24
network equipment

equipment that exchanges data between different networks used to permanently connect directly other *devices* to the internet

3.25
network function

equipment's functionality to provide or utilize network resources by itself

3.26
network function configuration

data processed by the equipment that defines the behaviour of the equipment's *network function*

3.27
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.

3.28
operational state

state in which the equipment is functioning normally according to the intended equipment functionality [35] and within its intended operational environment of use

3.29
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 [35] 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.

3.30
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.

3.31
public security parameter

sensitive security parameter that is not confidential

3.32
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 [29]]

3.33
risk

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

[SOURCE: ISO/IEC Guide 51:2014 [30]]

3.34
resource

functional unit or data item needed to perform required operations

[SOURCE: IEC [31]]

3.35
security asset

sensitive security parameter or confidential security parameter or security function

3.36
security function

functionality on the equipment that is relevant to protect it from harming the network or its functioning or misusing network resources

3.37
security parameter

data processed by the equipment that defines the behaviour of the equipment‘s *security function*

3.38
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.

3.39
sensitive network function configuration

network function configuration whose manipulation can harm the network or its functioning or can lead to misuse of network resources

3.40
sensitive security parameter

security parameter whose manipulation can harm the network or its functioning or can lead to misuse of network resources

3.41
security update

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

3.42
software

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

Note 1 to entry: Software also includes firmware.

3.43
storage mechanism

equipment functionality that allows to store information

3.44
update mechanism
equipment functionality that allows to change equipment's *software*

3.45
user interface
external interface between the equipment and a user

3.46
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") [32]]

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

DN decision node

DoS denial of service

DT decision tree

E evidence

E.Info evidence.information

E.Just evidence.justification

GEC general equipment capabilities

IC implementation category

ICMP Internet control message protocol

IP Internet protocol

LAN local area network

OS operating system

MitM Man-in-the-Middle

NNM network monitoring mechanism

OS operating system

PIN personal identification number

PKI public key infrastructure

RLM resilience mechanism

SCM secure communication mechanism

SDO standards developing organization

SQL structured query language

SSM secure storage mechanism

SSP sensitive security parameter

SUM secure update mechanism

TCM traffic control mechanism

USB universal serial bus

WLAN wireless local area network

5 Application of this document

This document uses the concept of mechanisms to instruct the user of this document when to apply certain security measures. Mechanisms address the applicability and appropriateness through a set of requirements including assessment criteria. An applicable/non-applicable decision is taken for each of the items specified. If applicable it is followed by a pass/fail appropriateness decision for each of the items specified. For example, when checking the applicability of a requirement on external interfaces, then the decision whether the requirement needs to be fulfilled is determined for each external interface independently.

The mechanisms and their application are documented using the structure shown in the table below: