SLOVENSKI STANDARD
SIST EN 17640:2023

01-januar-2023

Metodologija ocenjevanja kibernetske varnosti za izdelke IKT za določeno obdobje

Fixed time cybersecurity evaluation methodology for ICT products

Cybersicherheitsevaluationsmethodologie für IKT-Produkte

Méthode d'évaluation de la cybersécurité pour produits TIC

Ta slovenski standard je istoveten z: **EN 17640:2022**

ICS:

35.030	Informacijska varnost	IT Security

SIST EN 17640:2023 **en,fr,de**

EUROPEAN STANDARD **EN 17640**

NORME EUROPÉENNE

EUROPÄISCHE NORM October 2022

ICS 35.030

English version

Fixed-time cybersecurity evaluation methodology for ICT products

Méthode d'évaluation de la cybersécurité pour produits TIC

Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte

This European Standard was approved by CEN on 15 August 2022.

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 17640:2022) has been prepared by Technical Committee CEN/CLC/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of an identical text or by endorsement, at the latest by April 2023, and conflicting national standards shall be withdrawn at the latest by April 2023.

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.

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

The foundation for a sound product certification is a reliable, transparent and repeatable evaluation methodology. Several product or scheme dependent evaluation methodologies exist. The Cybersecurity Act (CSA) [1] will cause new schemes to be created which in turn require (new) methodologies to evaluate the cybersecurity functionalities of products. These new methodologies are required to describe evaluation tasks defined in the CSA. This methodology also adds a concept, independent of the requirements of the CSA, namely the evaluation in a fixed time. Existing cybersecurity evaluation methodologies (e.g. EN ISO/IEC 15408 in combination with EN ISO/IEC 18045) are not explicitly designed to be used in a fixed time.

Scheme developers are encouraged to implement the evaluation methodology in their schemes. This can be done for general purpose schemes or in dedicated (vertical domain) schemes, by selecting aspects for self-assessment at CSA assurance level “basic” or third-party assessments. The self-assessment may be performed at CSA assurance level “basic”, the third-party evaluations at CSA assurance level “basic”, “substantial” or “high”. And the evaluation criteria and methodology might be subject to extra tailoring, depending on the requirements of the individual scheme. This cybersecurity evaluation methodology caters for all of these needs. This methodology has been designed so that it can (and needs to be) adapted to the requirements of each scheme.

Scheme developers are encouraged to implement the evaluation methodology for the intended use of the scheme, applicable for general purpose or in dedicated (vertical) domains, by selecting those aspects needed for self-assessment at CSA assurance level “basic” or third-party evaluation at any CSA assurance level required by the scheme.

This document provides the minimal set of evaluation activities defined in the CSA to achieve the desired CSA assurance level as well as optional tasks, which might be required by the scheme. Selection of the various optional tasks is accompanied by guidelines so scheme developers can estimate the impact of their choices. Further adaption to the risk situation in the scheme can be achieved by choosing the different evaluation tasks defined in the methodology or using the parameters of the evaluation tasks, e.g. the number of days for performing certain tasks.

If scheme developers choose tasks that are not defined in this evaluation methodology, it will be the responsibility of the scheme developer to define a set of companion requirements or re-use another applicable evaluation methodology.

Nonetheless, it is expected that individual schemes will instantiate the general requirements laid out in this evaluation methodology and provide extensive guidance for manufacturers (and all other parties) about the concrete requirements to be fulfilled within the scheme.

Evaluators, testers and certifiers can use this methodology to conduct the assessment, testing or evaluation of the products and to perform the actual evaluation/certification according to the requirements set up by a given scheme. It also contains requirements for the level of skills and knowledge of the evaluators and thus will also be used by **accreditation bodies** or **National Cybersecurity Certification Authorities** during accreditation or authorization, where appropriate, and monitoring of conformity assessment bodies.

Manufacturers and **developers** will find the generic type of evidence required by each evaluation task listed in the evaluation methodology to prepare for the assessment or evaluation. The evidence and evaluation tasks are independent from the fact of whether the evaluation is done by the manufacturer/developer (i.e. 1st party) or by someone else (2nd/3rd party).

Users of certified products (regulators, user associations, governments, companies, consumers, etc.) may also use this document to inform themselves about the assurance drawn from certain certificates using this evaluation methodology. Again, it is expected that scheme developers provide additional information, tailored to the domain of the scheme, about the assurance obtained by evaluations / assessments under this methodology.

Furthermore, this methodology is intended to enable scheme developers to create schemes which attempt to reduce the burden on the manufacturer as much as possible (implying additional burden on the evaluation lab and the certification body).

NOTE In this document the term "Conformity Assessment body" (CAB) is used for CABs doing the evaluation. Other possible roles for CABs are not considered in this document.

It should be noted that this document cannot be used "stand alone". Each domain (scheme) needs to provide domain specific cybersecurity requirements ("technical specifications") for the objects to be evaluated / certified. This methodology is intended to be used in conjunction with those technical specifications containing such cybersecurity requirements. The relationship of the methodology provided in this document to the activities in product conformity assessment is shown in Figure 1.

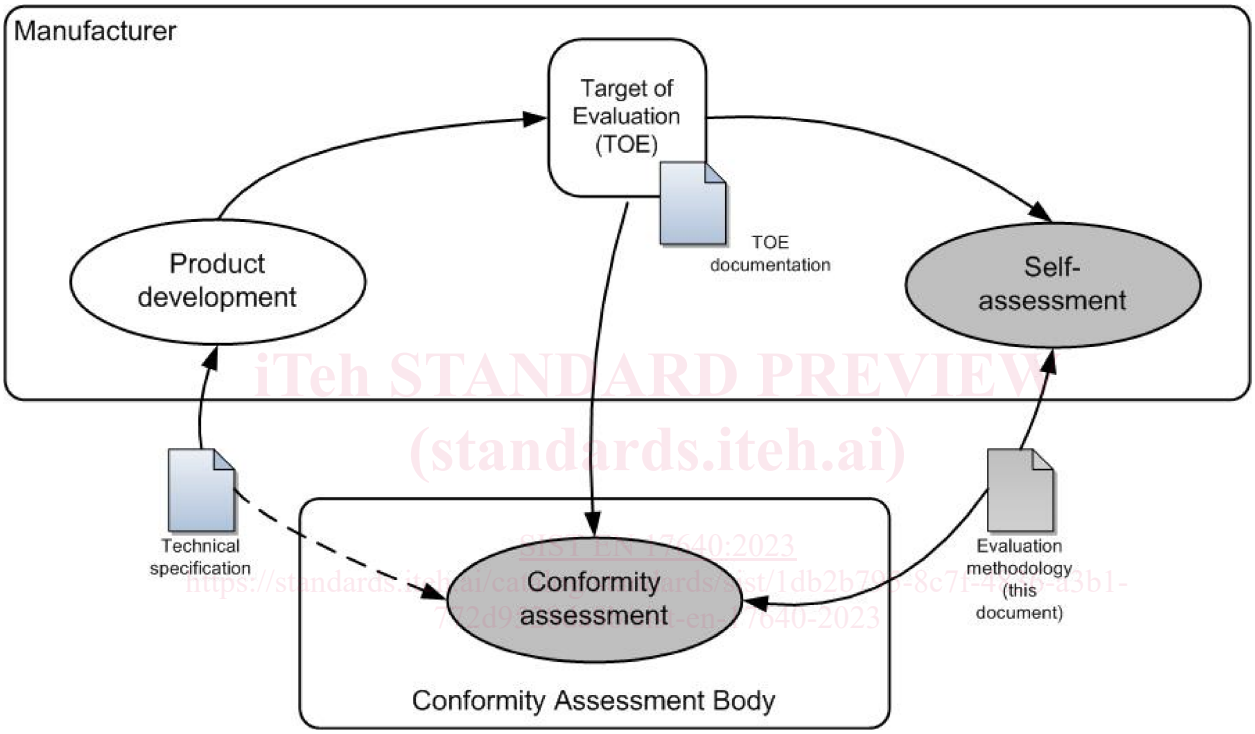

Figure 1 — Relationship of this document to the activities in product conformity assessment

1 Scope

This document describes a cybersecurity evaluation methodology that can be implemented using pre-defined time and workload resources, for ICT products. It is intended to be applicable for all three assurance levels defined in the CSA (i.e. basic, substantial and high).

The methodology comprises different evaluation blocks including assessment activities that comply with the evaluation requirements of the CSA for the mentioned three assurance levels. Where appropriate, it can be applied both to third-party evaluation and self-assessment.

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 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
evaluator
individual that performs an evaluation

Note 1 to entry: Under accreditation the term “tester” is used for this individual.

3.2
auditor
individual that performs an audit

3.3
certifying function
people or group of people responsible for deciding upon certification

Note 1 to entry: Depending on the scheme the certifying function may use evidence beyond the *ETR (3.13)* as a basis for the certification decision.

3.4
scheme developer
person or organization responsible for a conformity assessment scheme

Note 1 to entry: For schemes developed under the umbrella of the CSA the so-called “ad hoc group” helps the scheme developer.

Note 2 to entry: This definition is based on and aligned with the definition of “scheme owner” in EN ISO/IEC 17000.

3.5
confirm
<evaluation verb> declare that something has been reviewed in detail with an independent determination of sufficiency

[SOURCE: ISO/IEC 18045:2022, definition 3.2 with NOTE removed]

3.6
verify
<evaluation verb> rigorously review in detail with an independent determination of sufficiency

Note 1 to entry: Also see "confirm". This term has more rigorous connotations. The term "verify" is used in the context of evaluator actions where an independent effort is required of the evaluator.

[SOURCE: ISO/IEC 18045:2022, definition 3.22]

3.7
determine
<evaluation verb> affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion

Note 1 to entry: The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms "confirm" or "verify" which imply that an analysis has already been performed which needs to be reviewed.

[SOURCE: ISO/IEC 18045:2022, definition 3.5]

3.8
ICT product
product with information and/or communication technology

Note 1 to entry: ICT covers any product that will store, retrieve, handle, transmit, or receive digital information electronically in a digital form (e.g., personal computers, smartphones, digital television, email systems, robots).

3.9
Target of Evaluation
TOE

product (or parts thereof, if product is not fully evaluated) with a clear boundary, which is subject to the evaluation

3.10
FIT Security Target
FIT ST
documented information describing the security properties and the operational environment of the *TOE (3.9)*

Note 1 to entry: The FIT ST may have different content, structure and size depending on the CSA assurance level.

3.11
FIT Protection Profile
FIT PP
implementation-independent statement of security needs for a *TOE (3.9)* type

[SOURCE: ISO/IEC 15408-1:2022, definition 3.68]

3.12
Secure User Guide
SUG
documented information describing the steps necessary to set up the *TOE (3.9)* into the intended *secure state (3.16)*

3.13
Evaluation Technical Report
ETR
documented information describing the results of the evaluation

3.14
scheme-specific checklist
list of items defining the required level of detail and granularity of the documentation, specified by the scheme

3.15
knowledge
facts, information, truths, principles or understanding acquired through experience or education

Note 1 to entry: An example of knowledge is the ability to describe the various parts of an information assurance standard.

Note 2 to entry: This concept is different from the concept “Knowledge of the TOE”.

[SOURCE: ISO/IEC TS 17027:2014, 2.56, modified — Note 1 to entry has been added from ISO/IEC 19896-1:2018, Note 2 to entry is new]

3.16
secure state
state in which all data related to the *TOE (3.9)* security functionality are correct, and security functionality remains in place

3.17
self-assessment
conformance assessment activity that is performed by the person or organization that provides the *TOE (3.9)* or that is the object of conformity assessment

[SOURCE: EN ISO/IEC 17000:2020, definition 4.3 with Notes and Examples removed]

3.18
evaluation task parameter
parameter required to be set when using this document to define how the evaluation task shall be executed by the *evaluator (3.1)*

4 Conformance

The following Table 1 provides a reference on how the evaluation tasks should be chosen for a certain scheme for the different CSA assurance levels:

Table 1 — Evaluation tasks vs. CSA assurance level conformance claim

		CSA assurance level conformance claim		
Evaluation tasks	**Reference**	**Basic**	**Substantial**	**High**
Completeness check	6.1	Required	Required	Required
Review of security functionalities	6.3	Required		
FIT Security Target Evaluation	6.4		Required	Required
Development documentation[1)]	6.5	Required	Required	Required
Evaluation of TOE Installation	6.6	Recommended	Required	Required
Conformance Testing	6.7	Recommended	Required	Required
Vulnerability review	6.8	Recommended	Required (or done with 6.9)	
Vulnerability testing	6.9		Recommended	
Penetration testing	6.10			Required
Basic crypto analysis	6.11	Recommended	Recommended[2)]	
Extended crypto analysis	6.12			Required
1) The scheme specific checklist may be empty for a particular scheme and then this evaluation tasks would not apply. 2) If crypto functionality is at the core of the product, then it is sensible for scheme developers to include it, e.g. defining appropriate product classes.				

NOTE 1 FIT Protection Profile Evaluation is a dedicated process and not part of the evaluation of a TOE. While the FIT PP specifies for which CSA assurance level it is applicable, the evaluation of a FIT PP is agnostic to this.

To implement the methodology for a certain scheme, the following steps shall be performed:

1. The scheme developer needs to perform a (domain) risk assessment, reviewing the domain under consideration.

2. The scheme developer shall assign the Attack Potential (cf. Clause 5.4 and Annex F) to each CSA assurance level used in the scheme

3. For each CSA assurance level the scheme developer shall select those evaluation tasks required for this level, these are marked grey in Table 1.

4. For each task chosen, the scheme developers shall review the parameters for this evaluation task and set them suitably based on the risk assessment and the determined attack potential. For the

evaluation task “development documentation” this includes setting up a scheme specific checklist (which maybe empty).

5. For each CSA assurance level the scheme developer shall review those evaluation tasks recommended for this level if inclusion is sensible, these task contain the word “Recommended” in Table 1.

6. For each CSA assurance level the scheme developer shall review if those evaluation tasks are sufficient for the scheme based on the determined Attack Potential. If not, the scheme developer shall select additional evaluation tasks (e.g. from the same CSA assurance level), tasks from a higher CSA assurance level or additional tasks not defined in this methodology. These may replace tasks already chosen.

7. For each new or updated task chosen the scheme developers shall review the parameters for this task and set them suitably based on the risk assessment and the attack potential.

If the scheme developers want to include development process evaluation/assessment, there is an additional task for the scheme: The scheme developer needs to decide about validity of process evaluation/assessment results for future product evaluations. This means that the development related tasks may be performed once, and the output of these tasks is subsequently used in several product evaluations (e.g. as a precondition). Optionally the auditors may define a list of artefacts which are to be provided in each subsequent product evaluation, to show that the audited processes are still operational.

If schemes intend to include this development process evaluation/assessment re-use mechanism, they shall ensure that reuse is limited to cases where the development process is the same in all evaluations or assessments, i.e. the site(s), the knowledge of the people and the actual processes are identical or equivalent. To achieve this, the initial evaluation or assessment may be made more broadly (i.e. cover a larger scope of the development). Additionally, the scheme shall limit the maximum period of time during which the results are to be acceptable.

EXAMPLE A usual maximal age of these results is two years. This means, if the evaluation / assessment occurs more than two years after the results of the development process evaluation have been produced, the development process needs to be re-assessed/re-evaluated. If an existing SDL (Software Development Lifecyle) certificate is used, its validity is another possibility for the validity of this evidence.

For some evaluation tasks the scheme may require additional inputs from the developer, e.g. an architectural overview. This additional input should be limited as much as possible, especially if this documentation is typically only prepared for the assessment or evaluation, i.e. not readily available for the TOE anyhow.

NOTE 2 Requiring design information might preclude some products from assessment or certification, as this information might not be available due to the fact that some third-party components, including hardware, might be proprietary without the possibility to obtain this design information. This is in general not applicable if white box testing is performed (if this is an option in the scheme). Further composition of certified parts is an option to mitigate this problem.

An example of the integration of this methodology in a scheme is given in Annex D.

5 General concepts

5.1 Usage of this methodology

Clause 5 describes elements of an evaluation methodology for fixed-time security certification and self-assessment.

To instantiate a specific evaluation methodology based on this generic methodology, the required evaluation tasks are selected depending on the intended CSA assurance level according to the CSA. Depending on the domain, certain evaluation tasks are required, while others are optional (see Clause 4). For sample-based evaluation tasks, the scheme needs to devise the sample size and sampling strategy as well as the absolute or relative weight, i.e. the number of person days or the percentage of overall evaluation time. Additional constraints on sampling might be provided, e.g. on the limits of sampling depending on the CSA assurance level.

To use this methodology, it is not necessary to require all evaluation tasks described in Clause 6 for every CSA assurance level. For example, a scheme designed for CSA assurance level "substantial" might require a "Basic crypto analysis" evaluation task or might omit it and possibly integrate the necessary parts into the "Conformance testing" task instead.

NOTE This document and the resulting scheme do not define the exact structure of the documents used or produced by the evaluation, e.g. the FIT ST or the ETR. These are scheme dependent.

5.2 Knowledge of the TOE

The scheme will require different sets of information or information with different levels of detail. This depends on the one hand on the assurance required, on the other hand additional information might speed up certain evaluation tasks.

In general, the developer shall provide a FIT Security Target and a Secure User Guide. The latter may not be needed, if the TOE goes into the secure state as defined in the FIT ST automatically, i.e. no further guidance is necessary.

The scheme may require additional information for certain activities. This is indicated in the respective evaluation tasks where applicable.

The evaluator shall have access to information (like standards, protocol specifications) regarding the technology implemented in the TOE, where this information is publicly available.

NOTE Publicly available does not imply that it is available free of charge.

5.3 Development process evaluation

This methodology is concerned with ICT product evaluation, and a scheme might limit its evaluation tasks to pure ICT product related activities. However, experience in ICT product certification has shown that it is sensible and valuable to evaluate the development process as well. This concerns both the initial development (e.g. regarding security during design and construction of the product, including site security) as well as aspects beyond delivery of the product, e.g. vulnerability and update management processes. To improve usage of audit results in future product evaluations, the auditor may define a set of artefacts (e.g. meeting reports, listing of configuration management systems, filled in checklists) which will then be requested in every subsequent product evaluation to verify that the processes audited have been adhered to in this instance.

Generic standards for development process evaluations should be reused where possible, applicable or available.

5.4 Attack Potential

To determine the necessary evaluation tasks and their parameters it is necessary to define the expected threat agent, characterized with a specific strength, also called Attack Potential. The vulnerability analysis task of the evaluator may include penetration testing assuming the Attack Potential of the threat agent. The following levels of Attack Potential are assumed in this document, the categorization is based on [2] and [5].

— Basic

— Enhanced Basic

— Moderate

— High

NOTE 1 Attack Potential Moderate and High are unlikely to be addressable in a fixed-time evaluation scheme: systematic availability of detailed documentation will probably be necessary to allow evaluators to be on par with high level threat agents.

The CSA [1] defines three assurance levels: basic, substantial and high. Each level has an implicitly defined attack scenario assigned. Scheme developers are advised to review the definitions in the CSA to align the CSA assurance levels (as applicable to their domain) with the attack potential used in this methodology.

NOTE 2 The terms used in the context of attack potential are used as defined in this document and deviate from the meaning of similar terms used in the CSA.

In the end evaluators will assess whether a threat agent possessing a given Attack Potential is able to bypass or break the security functionality of the TOE.

The calculation of the attack potential is given in Annex F.

5.5 Knowledge building

Ensuring that each evaluation task produces the expected results requires certain knowledge and competence by the evaluators. This knowledge is briefly described for each evaluation task and needs to be refined when setting up the scheme.

To ensure that an overall evaluation produces the expected results, the competent evaluators need to work as a good team. In particular the evaluators who work on the document parts of the evaluation need to very closely collaborate with the evaluators performing the actual testing; ideally, they are the same (set of) persons, especially if the total time span of the evaluation is low.

6 Evaluation tasks

6.1 Completeness check

6.1.1 Aim

The aim of this evaluation task is to verify that all evidence required for evaluation is provided.

6.1.2 Evaluation method

This evaluation task is a completeness check of the evidence required by the scheme. No access to internal documents is required. Depending on the TOE, access to publicly available specifications or other documents distributed with or referenced by the TOE might be necessary.

6.1.3 Evaluator competence

The evaluators shall know the scheme requirements regarding evidence.

6.1.4 Evaluator work units

6.1.4.1 Work unit 1

The evaluators shall check that all evidence required for the evaluation is present. This includes a sufficient number of TOEs.