

STN	Metodika hodnotenia kybernetickej bezpečnosti s fixným časom pre produkty IKT	STN EN 17640 36 9801
------------	--	--

Fixed-time cybersecurity evaluation methodology for ICT products

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 01/23

Obsahuje: EN 17640:2022

136241

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 TICZeitlich 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**

EN 17640:2022 (E)

Contents		Page
European foreword		4
Introduction		5
1	Scope	7
2	Normative references	7
3	Terms and definitions	7
4	Conformance	9
5	General concepts	11
5.1	Usage of this methodology	11
5.2	Knowledge of the TOE	12
5.3	Development process evaluation	12
5.4	Attack Potential	12
5.5	Knowledge building	13
6	Evaluation tasks	13
6.1	Completeness check	13
6.1.1	Aim	13
6.1.2	Evaluation method	13
6.1.3	Evaluator competence	13
6.1.4	Evaluator work units	13
6.2	FIT Protection Profile Evaluation	14
6.2.1	Aim	14
6.2.2	Evaluation method	14
6.2.3	Evaluator competence	14
6.2.4	Evaluator work units	14
6.3	Review of security functionalities	15
6.3.1	Aim	15
6.3.2	Evaluation method	15
6.3.3	Evaluator competence	15
6.3.4	Evaluator work units	15
6.4	FIT Security Target Evaluation	16
6.4.1	Aim	16
6.4.2	Evaluation method	16
6.4.3	Evaluator competence	16
6.4.4	Evaluator work units	16
6.5	Development documentation	17
6.5.1	Aim	17
6.5.2	Evaluation method	17
6.5.3	Evaluator competence	17
6.5.4	Work units	17
6.6	Evaluation of TOE Installation	17
6.6.1	Aim	17
6.6.2	Evaluation method	18
6.6.3	Evaluator competence	18
6.6.4	Evaluator work units	18
6.7	Conformance testing	18

6.7.1	Aim	18
6.7.2	Evaluation method	18
6.7.3	Evaluator competence	19
6.7.4	Evaluator work units	19
6.8	Vulnerability review	20
6.8.1	Aim	20
6.8.2	Evaluation method	20
6.8.3	Evaluator competence	21
6.8.4	Evaluator work units	21
6.9	Vulnerability testing	21
6.9.1	Aim	21
6.9.2	Evaluation method	22
6.9.3	Evaluator competence	22
6.9.4	Evaluator work units	22
6.10	Penetration testing	24
6.10.1	Aim	24
6.10.2	Evaluation method	24
6.10.3	Evaluator competence	25
6.10.4	Evaluator work units	25
6.11	Basic crypto analysis	26
6.11.1	Aim	26
6.11.2	Evaluation method	26
6.11.3	Evaluator competence	26
6.11.4	Evaluator work units	26
6.12	Extended crypto analysis	27
6.12.1	Aim	27
6.12.2	Evaluation method	27
6.12.3	Evaluator competence	28
6.12.4	Evaluator work units	28
Annex A (informative)	Example for a structure of a FIT Security Target (FIT ST)	30
Annex B (normative)	The concept of a FIT Protection Profile (FIT PP)	32
Annex C (informative)	Acceptance Criteria	33
Annex D (informative)	Guidance for integrating the methodology into a scheme	40
Annex E (informative)	Parameters of the methodology and the evaluation tasks	45
Annex F (normative)	Calculating the Attack Potential	47
Annex G (normative)	Reporting the results of an evaluation	52
Bibliography	54

EN 17640:2022 (E)**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.

EN 17640:2022 (E)

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.

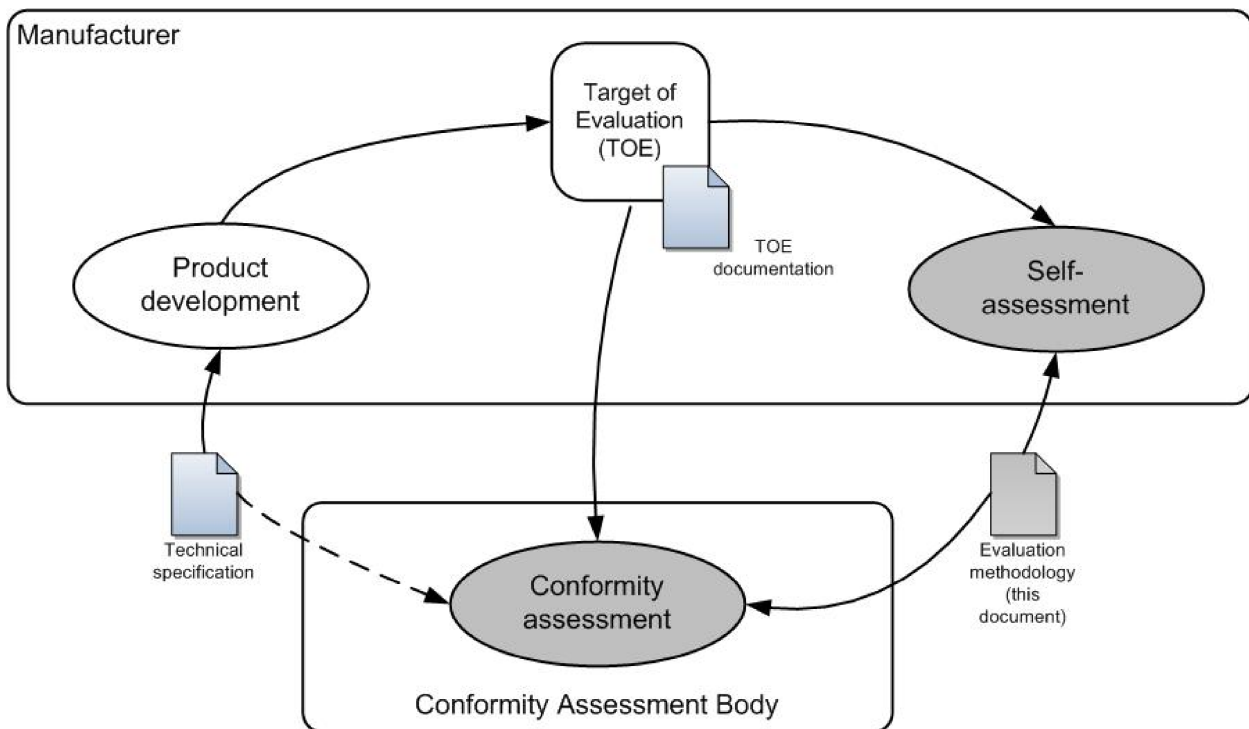


Figure 1 — Relationship of this document to the activities in product conformity assessment

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.

koniec náhľadu – text ďalej pokračuje v platenej verzii STN