ILNAS

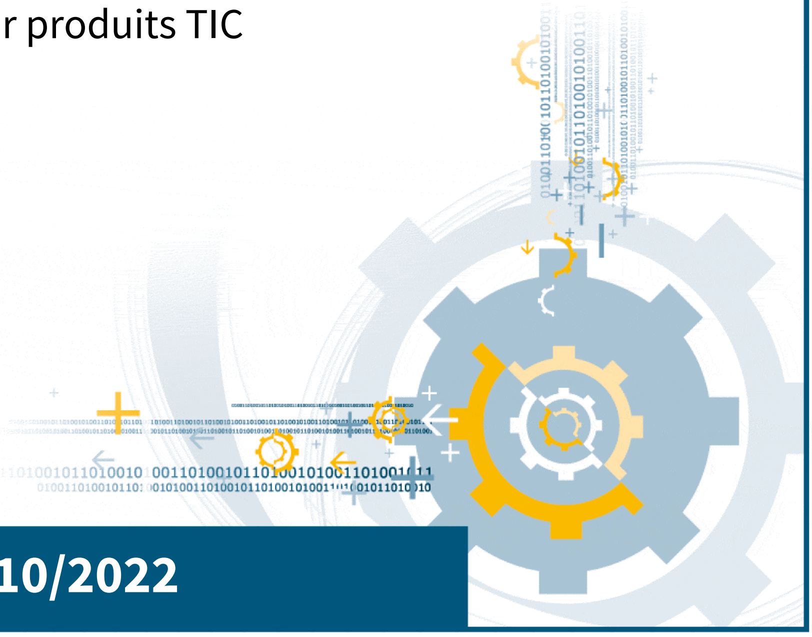
Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 17640:2022

Fixed-time cybersecurity evaluation methodology for ICT products

Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte

Méthode d'évaluation de la cybersécurité pour produits TIC



10/2022

National Foreword

This European Standard EN 17640:2022 was adopted as Luxembourgish Standard ILNAS-EN 17640:2022.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html

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.

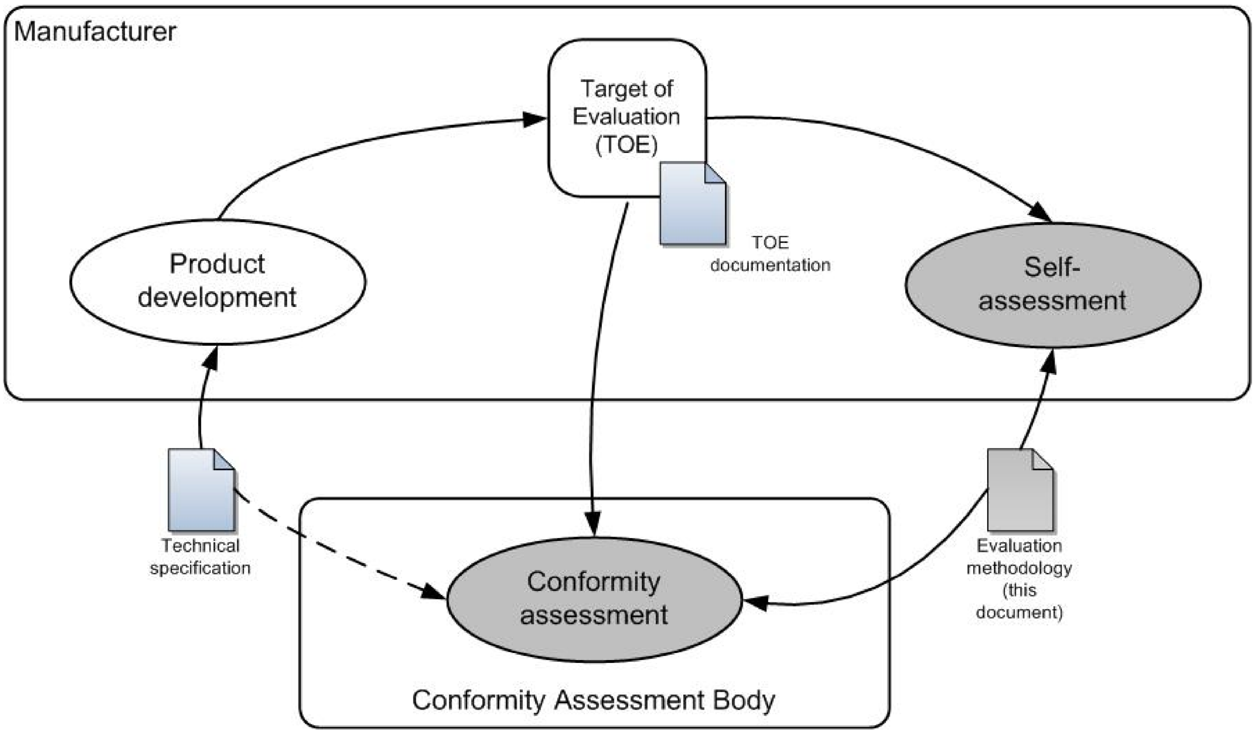


Figure 1 — Relationship of this document to the activities in product conformity assessment

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]