ILNAS

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

ILNAS-EN 17640:2022

Méthode d'évaluation de la cybersécurité pour produits TIC

Fixed-time cybersecurity evaluation methodology for ICT products

Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte

10/2022

Avant-propos national

Cette Norme Européenne EN 17640:2022 a été adoptée comme Norme Luxembourgeoise ILNAS-EN 17640:2022.

Toute personne intéressée, membre d'une organisation basée au Luxembourg, peut participer gratuitement à l'élaboration de normes luxembourgeoises (ILNAS), européennes (CEN, CENELEC) et internationales (ISO, IEC) :

- Influencer et participer à la conception de normes
- Anticiper les développements futurs
- Participer aux réunions des comités techniques

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

NORME EUROPÉENNE
EUROPÄISCHE NORM
EUROPEAN STANDARD

EN 17640

Octobre 2022

ICS 35.030

Version Française

Méthode d'évaluation de la cybersécurité pour produits TIC

Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte

Fixed-time cybersecurity evaluation methodology for ICT products

La présente Norme européenne a été adoptée par le CEN le 15 août 2022.

Les membres du CEN et CENELEC sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à la Norme européenne. Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du Centre de Gestion du CEN-CENELEC ou auprès des membres du CEN et CENELEC.

La présente Norme européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CEN et CENELEC dans sa langue nationale et notifiée au Centre de Gestion du CEN-CENELEC, a le même statut que les versions officielles.

Les membres du CEN et du CENELEC sont les organismes nationaux de normalisation et les comités électrotechniques nationaux des pays suivants: Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République de Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Sommaire

Page

Avant-propos européen

Le présent document (EN 17640:2022) a été élaboré par le Comité Technique CEN-CENELEC/JTC 13 « Cybersécurité et protection des données », dont le secrétariat est tenu par DIN.

Cette Norme européenne devra recevoir le statut de norme nationale, soit par publication d'un texte identique, soit par entérinement, au plus tard en avril 2023, et toutes les normes nationales en contradiction devront être retirées au plus tard en avril 2023.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. Le CEN ne saurait être tenu pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve sur le site web du CEN.

Selon le Règlement intérieur du CEN/CENELEC, les organismes de normalisation nationaux des pays suivants sont tenus de mettre cette Norme européenne en application : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République tchèque, Roumanie, Royaume-Uni, Serbie, Slovaquie, Slovénie, Suède, Suisse et Turquie.

Introduction

Une certification produit solide repose sur une méthodologie d'évaluation fiable, transparente et reproductible. Il existe plusieurs méthodologies d'évaluation dépendant de produits ou de schémas. Le Règlement sur la cybersécurité (Cybersecurity Act, CSA) [1] entraînera la création de nouveaux schémas qui nécessiteront à leur tour de (nouvelles) méthodologies pour évaluer les fonctionnalités de cybersécurité des produits. Ces nouvelles méthodologies sont nécessaires pour décrire les tâches d'évaluation définies dans le CSA. Cette méthodologie ajoute également un concept, indépendant des exigences du CSA, à savoir l'évaluation dans une durée fixe. Les méthodologies d'évaluation de cybersécurité existantes (par exemple, l'EN ISO/IEC 15408 en combinaison avec l'EN ISO/IEC 18045) ne sont pas explicitement destinées à être utilisées dans une durée fixe.

Les développeurs de schémas sont encouragés à implémenter la méthodologie d'évaluation dans leurs schémas. Cela peut se faire pour les schémas à usage général ou pour les schémas dédiés (domaine vertical), en choisissant les aspects nécessaires pour l'auto-évaluation pour le niveau d'assurance CSA « élémentaire » ou pour l'évaluation par un tiers. L'auto-évaluation peut être effectuée pour un niveau d'assurance CSA « élémentaire » et les évaluations par des tiers peuvent être effectuées pour des niveaux d'assurance CSA « élémentaire », « substantiel » ou « élevé ». De plus, en fonction des exigences du schéma spécifique, les critères et la méthodologie d'évaluation peuvent faire l'objet d'une adaptation supplémentaire. Cette méthodologie d'évaluation de la cybersécurité répond à tous ces besoins. Cette méthodologie a été conçue de telle manière à pouvoir (et devoir) être adaptée aux exigences de chaque schéma.

Les **développeurs de schémas** sont encouragés à implémenter la méthodologie d'évaluation compte tenu de l'utilisation prévue du schéma, applicable soit d'une façon générale soit dans des domaines dédiés (verticaux), en choisissant les aspects nécessaires pour l'autoévaluation pour le niveau d'assurance CSA « élémentaire » ou pour l'évaluation par un tiers pour tous les niveaux d'assurance CSA exigés par le schéma.

Le présent document fournit l'ensemble minimal d'activités d'évaluation définies dans le CSA afin d'obtenir le niveau d'assurance CSA souhaité, ainsi que les tâches facultatives qui peuvent être exigées par le schéma. Le choix des diverses tâches facultatives est guidé par des lignes directrices afin que les développeurs de schémas puissent estimer l'impact de leurs choix. Dans un schéma, une adaptation peut encore être faite en fonction de la situation de risque en choisissant les différentes tâches d'évaluation définies dans la méthodologie ou en utilisant les paramètres des tâches d'évaluation, par exemple le nombre de jours pour exécuter certaines tâches.

Si les développeurs de schémas choisissent des tâches qui ne sont pas définies dans la présente méthodologie d'évaluation, il incombe au développeur du schéma de définir un ensemble d'exigences d'accompagnement ou de réutiliser une autre méthodologie d'évaluation applicable.

Néanmoins, il est prévu que les schémas individuels instancient les exigences générales présentées dans cette méthodologie d'évaluation et qu'ils fournissent des recommandations complètes à l'attention des fabricants (et de toutes les autres parties) concernant les exigences concrètes qui doivent être satisfaites dans le cadre du schéma.

Les **évaluateurs, testeurs et certificateurs** peuvent utiliser cette méthodologie pour réaliser une appréciation, des tests ou une évaluation des produits, ainsi que pour réaliser l'évaluation/la certification réelle conformément aux exigences établies par un schéma donné. Elle contient également des exigences concernant le niveau de compétences et de connaissances des évaluateurs et est donc aussi appelée à être utilisée par des **organismes d'accréditation** ou par des **autorités de certification nationales en matière de cybersécurité** pendant la phase d'accréditation ou d'autorisation, selon le cas, et pendant la phase de surveillance des organismes d'évaluation de la conformité.

Pour les **fabricants** et les **développeurs**, la méthodologie d'évaluation répertorie le type générique de preuve exigé par chaque tâche d'évaluation afin de se préparer à l'appréciation ou à l'évaluation. Les preuves et les tâches d'évaluation sont indépendantes du fait que l'évaluation est réalisée par le fabricant/développeur (première partie) ou par une tierce partie (seconde ou tierce partie).

Les **utilisateurs de produits certifiés (organismes de réglementation, associations d'utilisateurs, autorités gouvernementales, entreprises, consommateurs, etc.)** peuvent également utiliser le présent document pour s'informer sur le niveau d'assurance apporté par certains certificats à l'aide de la présente méthodologie d'évaluation. Là encore, il est attendu que les développeurs de schémas fournissent des informations supplémentaires, adaptées au domaine du schéma, concernant l'assurance obtenue par les évaluations/appréciations conduites à l'aide de la présente méthodologie.

De plus, cette méthodologie est destinée à permettre aux développeurs de schémas de créer des schémas qui tentent de réduire autant que possible la charge qui pèse sur le fabricant (ce qui implique une charge supplémentaire pesant sur le laboratoire d'évaluation et sur l'organisme de certification).

NOTE Dans le présent document, le terme « organisme d'évaluation de la conformité » est utilisé pour désigner les organismes d'évaluation de la conformité qui réalisent l'évaluation. Les autres rôles possibles des organismes d'évaluation de la conformité ne sont pas pris en compte dans le présent document.

Il convient de préciser que le présent document ne peut pas être utilisé seul. Il est nécessaire que chaque domaine (schéma) établisse les exigences de cybersécurité propres au domaine concerné (« spécifications techniques ») pour les objets à évaluer/certifier. Cette méthodologie est destinée à être utilisée conjointement avec ces spécifications techniques contenant de telles exigences de cybersécurité. La relation entre la méthodologie indiquée dans le présent document et les activités d'évaluation de la conformité du produit est illustrée à la Figure 1.

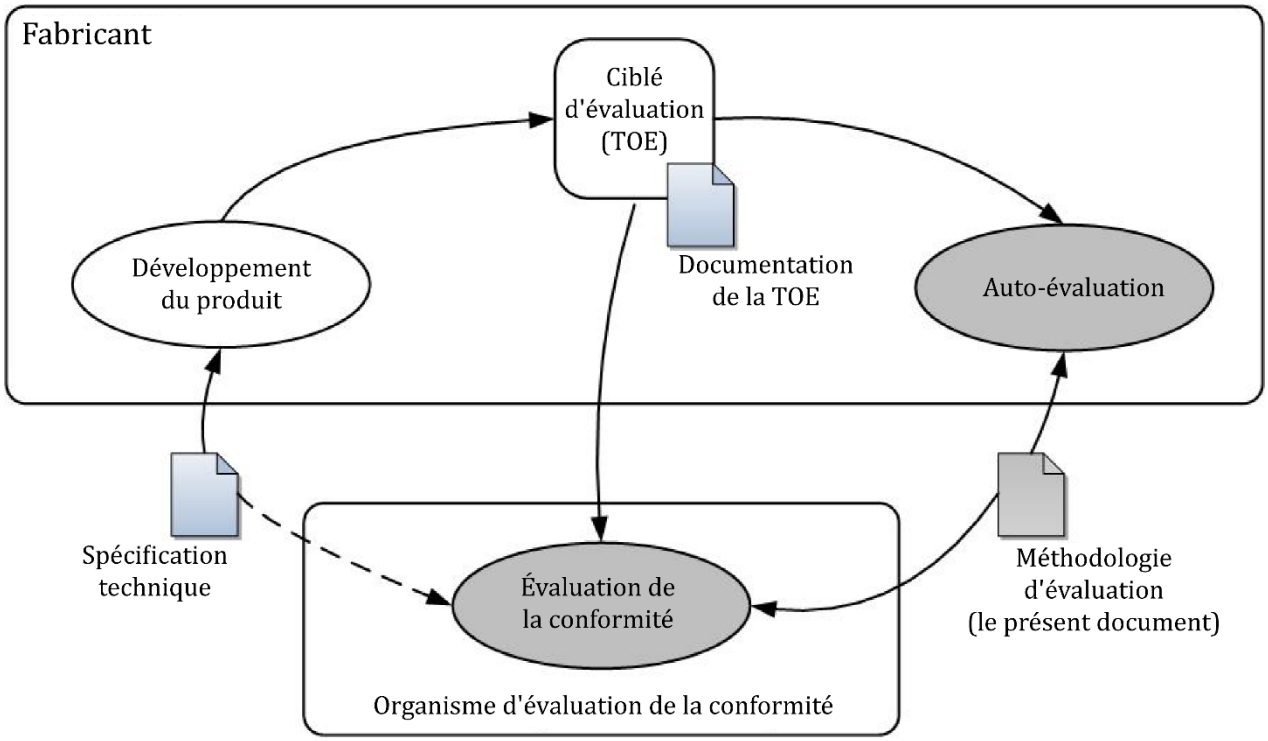

Figure 1 — Relation du présent document avec les activités d'une appréciation de la conformité du produit

1 Domaine d'application

Le présent document décrit une méthodologie d'évaluation de la cybersécurité des produits TIC qui peut être implémentée à l'aide d'une durée et de ressources de charge de travail prédéfinies. Il est destiné à s'appliquer aux trois niveaux d'assurance définis dans le CSA (c'est-à-dire élémentaire, substantiel et élevé).

La méthodologie comprend différents blocs d'évaluation contenant des activités d'évaluation qui sont conformes aux exigences d'évaluation du CSA pour les trois niveaux d'assurance mentionnés. Le cas échéant, elle peut être appliquée à la fois à une évaluation tierce et à une auto-évaluation.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes :

— IEC Electropedia : disponible à l'adresse https://www.electropedia.org/

— ISO Online browsing platform : disponible à l'adresse https://www.iso.org/obp

3.1
évaluateur
personne qui effectue une évaluation

Note 1 à l'article : Dans le cadre de l'accréditation, le terme « testeur » est utilisé pour désigner cette personne.

3.2
auditeur
personne qui effectue un audit

3.3
fonction de certification
personne ou groupe de personnes ayant la responsabilité de décider d'une certification

Note 1 à l'article : En fonction du schéma, la fonction de certification peut utiliser des preuves qui dépassent le cadre du rapport technique d'évaluation (*RTE*) *(3.13)* comme a base de décision pour la certification.

3.4
développeur du schéma
personne ou organisation responsable d'un schéma d'évaluation de la conformité

Note 1 à l'article : Pour les schémas développés sous l'égide du CSA, le « groupe ad hoc » intervient pour aider le développeur du schéma.

Note 2 à l'article : Cette définition est basée et alignée sur la définition du terme « propriétaire » de l'EN ISO/IEC 17000.