NORME INTERNATIONALE

ISO/IEC 19896-2

Première édition
2018-08

Techniques de sécurité IT — Exigences de compétence pour les testeurs et les évaluateurs en matière de sécurité de l'information —

Partie 2: Exigences en matière de connaissances, de compétences et d'efficacité pour les testeurs de l'ISO/IEC 19790

IT security techniques — Competence requirements for information security testers and evaluators —

Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

Numéro de référence
ISO/IEC 19896-2:2018(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/iso/fr/avant-propos.html.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, Technologies de l'information, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

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 à l'adresse www.iso.org/fr/members.html.

Une liste de toutes les parties de la série ISO/IEC 19896 se trouve sur le site Web de l'ISO.

Introduction

Le présent document fournit les exigences spécifiques pour démontrer les exigences en matière de connaissances, de savoir-faire et d'efficacité des personnes lors de la réalisation de projets d'essais de sécurité conformément à l'ISO/IEC 19790 et à l'ISO/IEC 24759. L'ISO/IEC 19790 décrit la spécification des exigences en matière de sécurité pour les modules cryptographiques. Elle a servi de base à l'élaboration de nombreux schémas de certification, de validation et d'accords de reconnaissance. L'ISO/IEC 19790 permet une comparaison entre les résultats des projets indépendants d'essais de sécurité. L'ISO/IEC 24759 soutient cette approche en fournissant un ensemble commun d'exigences d'essai pour soumettre à essai la conformité à l'ISO/IEC 19790 d'un module cryptographique.

La connaissance, le savoir-faire et les exigences d'efficacité des testeurs individuels chargés de la réalisation des projets d'essai sont des facteurs essentiels pour assurer la comparaison des résultats de ces validations ou certifications.

L'ISO/IEC 17025, qui est souvent spécifiée comme une norme à laquelle les installations d'essai doivent se conformer, précise en 5.2.1 que « le personnel effectuant des tâches spécifiques doit être qualifié sur la base d'une instruction, d'une formation, d'une expérience appropriées et/ou d'un savoir-faire démontré ».

Le public visé par le présent document comprend les autorités de validation et de certification, les organismes d'accréditation des essais en laboratoire, les programmes de projets d'essais, les installations d'essais, les testeurs et les organismes proposant des certifications et des reconnaissances professionnelles.

Le présent document établit une base de référence pour les exigences en matière de connaissances, de savoir-faire et d'efficacité des testeurs de l'ISO/IEC 19790 dans le but d'établir la conformité des exigences de formation des professionnels des essais selon l'ISO/IEC 19790 associés aux programmes d'essais de conformité des modules cryptographiques.

L'Annexe D illustre l'utilité du présent document pour les valideurs dans le cadre d'un programme de validation.

Techniques de sécurité IT — Exigences de compétence pour les testeurs et les évaluateurs en matière de sécurité de l'information —

Partie 2:
Exigences en matière de connaissances, de compétences et d'efficacité pour les testeurs de l'ISO/IEC 19790

1 Domaine d'application

Le présent document fournit les exigences minimales en matière de connaissances, de savoir-faire et d'efficacité des personnes chargées de réaliser des activités d'essai dans le cadre d'un schéma de conformité utilisant l'ISO/IEC 19790 et l'ISO/IEC 24759.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 17025, *Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais*

ISO/IEC 17825, *Technologie de l'information — Techniques de sécurité — Méthodes de test pour la protection contre les attaques non intrusives des modules cryptographiques*

ISO/IEC 18367, *Technologie de l'information — Techniques de sécurité — Essais de conformité des algorithmes cryptographiques et des mécanismes de sécurité*

ISO/IEC 19790, *Technologies de l'information — Techniques de sécurité — Exigences de sécurité pour les modules cryptographiques*

ISO/IEC 19896-1, *Techniques de sécurité IT — Exigences de compétence pour les testeurs et les évaluateurs en matière de sécurité de l'information — Partie 1: Introduction, concepts et exigences générales*

ISO/IEC 20085-1, *Techniques de sécurité IT — Exigences de l'outil de test et méthodes d'étalonnage de l'outil de test utilisées pour tester les techniques d'atténuation des attaques non invasives dans les modules cryptographiques — Partie 1: Outils et techniques de test*

ISO/IEC 20085-2, *Techniques de sécurité IT — Exigences de l'outil de test et méthodes d'étalonnage de l'outil de test utilisées pour tester les techniques d'atténuation des attaques non invasives dans les modules cryptographiques — Partie 2: Méthodes et appareillage d'étalonnage et d'essai*

ISO/IEC 20543, *Technologies de l'information — Techniques de sécurité — Méthodes d'essai et d'analyse des générateurs de bits aléatoires dans l'ISO/IEC 19790 et l'ISO/IEC 15408*

ISO/IEC 24759, *Technologies de l'information — Techniques de sécurité — Exigences d'essai pour modules cryptographiques*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 19896-1 et l'ISO/IEC 19790 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:

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

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

4 Abréviations

AES Norme de chiffrement avancé (Advanced Encryption Standard)

HDD Disque dur (Hard Disk Drive)

RSA Rivest-Shamir-Adleman

SHA Algorithme de hachage sécurisé (Secure Hash Algorithm)

SSD Disque statique à semiconducteurs (Solid State Drive)

5 Structure du présent document

Le présent document est composé des articles suivants: Connaissances (Article 5), Savoir-faire (Article 6), Expérience (Article 7), Instruction (Article 8) et Efficacité (Article 9). Chaque article correspond à un aspect des exigences en matière de connaissances, de savoir-faire, d'expérience, d'instruction et d'efficacité des personnes chargées de réaliser les activités d'essai, telles qu'elles sont introduites dans l'ISO/IEC 19896-1 pour un schéma de conformité utilisant l'ISO/IEC 19790 et l'ISO/IEC 24759.

6 Connaissances

6.1 Généralités

Les connaissances sont ce qu'un testeur connaît et peut décrire. Les Articles 6 à 9 traitent des exigences en matière d'instruction et des domaines de connaissances qui sont spécifiquement nécessaires pour les essais de conformité selon l'ISO/IEC 19790 et l'ISO/IEC 24759.

6.2 Instruction supérieure

6.2.1 Généralités

Les testeurs doivent disposer d'un niveau d'instruction tel qu'un diplôme reconnu, une licence ou un diplôme supérieur en rapport avec les exigences de sécurité traitées dans l'ISO/IEC 19790 et les exigences d'essai de l'ISO/IEC 24759. Les testeurs doivent démontrer qu'ils ont au moins:

a) terminé avec succès un cycle d'instruction supérieure approprié comprenant au moins 3 ans d'études dans des disciplines liées aux IT ou à la sécurité des IT; ou

b) une expérience équivalente à un niveau d'instruction supérieure dans des disciplines liées aux IT, à la sécurité des IT ou à l'administration des systèmes IT.

6.2.2 Spécialités techniques

En plus du niveau d'instruction minimal requis en 6.2.1, les testeurs doivent posséder des qualifications en matière d'instruction telles qu'un diplôme reconnu, une licence ou un diplôme supérieur correspondant aux spécialités techniques spécifiques. Voici quelques exemples de spécialités techniques spécifiques:

— concepts cryptographiques;

— technologie de l'ingénierie;

— ingénierie électrique;

— ingénierie mécanique;

— ingénierie des matériaux;

— ingénierie chimique;

— technologie de l'information informatique;

— ingénierie informatique;

— sciences de l'informatique;

— réseaux informatiques;

— cybersécurité;

— systèmes d'information;

— gestion de laboratoire;

— développement et sécurité des logiciels; ou

— ingénierie des logiciels.

6.2.3 Domaines de spécialité

L'ISO/IEC 19790:2012 et les exigences d'essai de l'ISO/IEC 24759 traitent des domaines de connaissances de spécialité spécifiques suivants. Un testeur doit, au minimum, démontrer ses connaissances dans au moins un domaine de spécialité spécifique.

Un laboratoire d'essai doit disposer de connaissances dans tous les domaines de spécialité, en tant qu'ensemble de son personnel technique.

L'ISO/IEC 19790:2012 et l'ISO/IEC 24759 spécifient des domaines de spécialité:

a) développement de logiciel et micrologiciel:

   1) langages de programmation (par exemple assembleur et langage de haut niveau);

   2) compilateurs;

   3) outils de débogage;

   4) essais de produit réalisés par le fournisseur;

      i) essais unitaires;

      ii) essais d'intégration;

iii) essais de régression;

b) systèmes d'exploitation:

1) installation;

2) configuration;

3) fonctionnement;

4) architecture;

5) durcissement du système;

6) machines virtuelles;

7) environnement d'exécution java;

c) développement de matériel:

1) réalisations matérielles:

i) simple puce;

ii) multipuces embarquées;

iii) multipuces indépendantes;

2) technologie:

i) fabrication à une seule puce;

ii) composants électriques et conception, schémas et concepts, y compris la conception logique et les représentations en langage de description de matériel (Hardware Description Language, HDL);

iii) conception mécanique et conditionnement;

3) fabrication:

i) intégrité de la chaîne d'approvisionnement;

ii) méthodes de fabrication;

iii) initialisation des paramètres;

iv) conditionnement et expédition;

v) essais et caractérisation;

4) fonctions de sécurité du matériel;

d) environnements opérationnels:

1) chargeur de démarrage (boot loader);

2) chargement;

3) création de liens:

4) gestion et protection de la mémoire;

5) communication inter- processus;

6) contrôle d'accès discrétionnaire;

7) contrôle d'accès basé sur les rôles;

8) formes exécutables;

9) mécanismes d'audit;

e) algorithmes, mécanismes et techniques cryptographiques:

1) algorithmes cryptographiques et fonctions de sécurité:

i) clé symétrique;

ii) clé asymétrique;

iii) hachage;

iv) générateurs de bits aléatoires;

v) authentification de messages;

vi) entropie;

vii) modes de fonctionnement;

2) gestion des paramètres sensibles de sécurité (SSP):

i) génération de paramètres sensibles de sécurité;

ii) établissement de paramètres sensibles de sécurité;

I) transport de SSP ou accord de SSP automatisés;

II) entrée ou sortie manuelle de SSP via des méthodes directes ou électroniques;

iii) entrée et sortie de paramètres sensibles de sécurité;

iv) stockage de paramètres sensibles de sécurité;

v) remise à zéro (zeroization) des paramètres sensibles de sécurité;

f) mécanismes d'identification et d'authentification:

1) authentification basée sur l'identité;

2) authentification basée sur les rôles;

3) authentification multifactorielle;

g) bonnes pratiques de conception et de développement:

1) l'assurance de la conception, comme la gestion de la configuration, la livraison, l'exploitation et le développement;

2) conception par contrat;

h) modélisation informelle;

1) modèle à état fini;

i) sécurité non invasive;

1) attaques non invasives:

i) DPA/DEMA;

ii) SPA/SEMA;

iii) attaques de synchronisation;

2) contre-mesures;

i) contre-mesures physiques;

EXEMPLE 1 Logique de précharge, logique à double rail, aplanissement du courant, détection des sondes, ajout de bruit, interruptions aléatoires, gigue de l'horloge.

ii) contre-mesures logiques;

EXEMPLE 2 Masquage, dissimulation, opération factice, synchronisation équilibrée, mélange, modification automatique de clés.

i) mécanismes d'auto-test:

1) essais pré-opérationnels;

2) essais conditionnels;

j) mécanismes de sécurité:

1) remise à zéro;

2) chemin de confiance;

3) dispositifs à indicateur d'effraction;

4) époxydes, matériaux d'enrobage et adhésifs (y compris les propriétés chimiques);

5) boîtiers et matériaux d'encapsulation;

6) mécanismes d'inviolabilité;

7) contre-mesures contre les attaques par déclenchement de fautes;

EXEMPLE 3 Schéma basé sur la redondance, code de détection d'erreur, empreinte.

8) protocoles de communication sécurisés (par exemple, Secure Sockets Layer, Transport Layer Security, Internet Key Exchange, Secure Socket Shell, Over the Air Rekeying, etc.);

9) attributs de la politique de sécurité;

10) modes opératoires à connaissance répartie;

k) caractéristiques de conception:

1) ports et interfaces;

2) modes de fonctionnement approuvés;

3) spécification des services;

4) spécification des paramètres sensibles de sécurité;

l) outils et méthodes d'essai:

1) construction de gabarits d'essai (logiciels ou matériels);

2) méthodes d'essai environnemental telles que l'utilisation de la température (par exemple, chaleur et froid) et de la tension (par exemple, changements de puissance d'entrée);

i) enceintes thermiques (par exemple, mécanismes de chauffage et de refroidissement);

ii) alimentations électriques variables;

3) utilisation d'outils manuels (par exemple, scies, perceuses, outils de levier, meulage, outils rotatifs à vitesse variable, cure-dents et miroirs, etc.);

4) utilisation de solvants chimiques (par exemple, à base d'acides et d'alcalins);

5) sources lumineuses artificielles;

6) outils de grossissement;

7) utilisation d'oscilloscopes à stockage numérique ou d'analyseurs logiques;

8) utilisation de volt-ohm-mètres ou de multimètres numériques;

9) scanners numériques;

10) caméras numériques (y compris capacités de mise au point rapprochée ou MACRO);

11) outils fournis par le programme de validation.

NOTE L'étalonnage des outils est uniquement requis en fonction de la méthode d'essai.

Des informations supplémentaires concernant l'association de connaissances spécifiques à la sécurité des modules cryptographiques sont spécifiées à l'Annexe C.

6.3 Connaissance des normes

6.3.1 Généralités

Le testeur doit avoir connaissance des références normatives spécifiées à l'Article 2. Le testeur doit être capable de démontrer sa compréhension ou sa familiarité avec un ou plusieurs des sujets suivants.

6.3.2 Concepts de l'ISO/IEC 19790

Le testeur doit avoir une connaissance des concepts décrits dans l'ISO/IEC 19790. L'ISO/IEC 19790 spécifie les exigences de sécurité pour un module cryptographique utilisé dans un système de sécurité qui protège les informations sensibles contenues dans les systèmes informatiques et de télécommunications. L'ISO/IEC 19790 spécifie quatre niveaux de sécurité pour chacun des 11 domaines d'exigences, chaque niveau de sécurité offrant une augmentation de la sécurité par rapport au niveau précédent pour les modules cryptographiques.

6.3.3 ISO/IEC 24759

6.3.3.1 Généralités

L'ISO/IEC 24759 spécifie les exigences d'essai pour les modules cryptographiques à utiliser par les fournisseurs et les laboratoires d'essai. L'ISO/IEC 24759:2017 comprend 11 paragraphes correspondant aux 11 domaines d'exigence de sécurité et six paragraphes correspondant à l'ISO/IEC 19790:2012, Annexes A à F. Ces exigences de sécurité correspondantes sont énumérées dans l'ISO/IEC 19790:2012, 5.2.2.5 et 5.2.2.6, respectivement.

6.3.3.2 Exigences relatives au fournisseur

L'ISO/IEC 24759 spécifie toutes les exigences relatives aux preuves du fournisseur (VE) que ces derniers apportent aux laboratoires d'essai, qui sont applicables au module soumis à essai, en tant que preuve servant à démontrer la conformité de leur module cryptographique aux exigences de sécurité spécifiées dans l'ISO/IEC 19790:2012.