NORME INTERNATIONALE

ISO 22383

Première édition
2020-09

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices pour la sélection et l'évaluation de la performance des solutions d'authentification pour les biens matériels

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for the selection and performance evaluation of authentication solutions for material goods

Numéro de référence
ISO 22383:2020(F)

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

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

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 ne saurait être tenue pour responsable 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/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 292, *Sécurité et résilience.*

Cette deuxième édition annule et remplace la première édition (ISO 12931:2012), qui a fait l'objet d'une révision technique. Les principales modifications par rapport à l'édition précédente sont les suivantes:

— elle porte un nouveau numéro et un nouveau titre ISO et fait désormais partie de la famille de normes ISO 22300;

— la terminologie reflète celle de la norme ISO 22300;

— les normes pertinentes publiées depuis la première édition ont été ajoutées comme références.

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.

Introduction

Depuis la publication de la première édition du présent document en 2012, la contrefaçon et la fraude des biens matériels, tant au niveau quantitatif que qualitatif, ne cessent de se développer, et de nombreux biens de consommation et pièces de rechange sont désormais concernés.

La vente de biens de contrefaçon, ainsi que de produits falsifiés, illégalement copiés ou commercialisés illicitement, est courante dans de nombreux pays en développement et elle se répand dans les économies développées. Certains fabricants et détenteurs de droits sont confrontés à une augmentation du nombre d'attaques de contrefaçon sur leurs biens matériels. L'Internet aggrave le problème. Ces produits de contrefaçon, qui n'offrent pas nécessairement les mêmes garanties en termes de sécurité et de respect de l'environnement et des exigences réglementaires, constituent une source de danger pour les consommateurs, les patients, les utilisateurs et la chaîne de distribution. Ils se traduisent, d'une part, par des pertes de chiffre d'affaires et d'emplois ainsi que par une atteinte à l'image de marque des entreprises et des détenteurs de droits ciblés, et d'autre part, par des pertes de recettes fiscales pour les États. La contrefaçon accroît le potentiel de revendications liées aux biens matériels frauduleux et de litiges pour les entreprises et les chaînes d'approvisionnement et de distribution. Par ailleurs, la contrefaçon des biens matériels est devenue l'une des principales activités du crime organisé, tant sur les marchés intérieurs que dans le domaine du commerce international et dans celui de la contrebande.

Pour lutter contre la contrefaçon et les autres formes de fraude, les titulaires des droits, les institutions et les autorités de régulation exigent et mettent en œuvre de plus en plus fréquemment des solutions d'authentification adaptées à leurs besoins. Il importe de préciser les exigences de performance requises des solutions propres à soutenir la lutte contre la contrefaçon au plan national comme au plan international. Cela favorisera une plus grande confiance parmi les consommateurs, renforcera la sécurité de la chaîne d'approvisionnement et aidera les autorités publiques à concevoir et à mettre en œuvre des politiques préventives, dissuasives et répressives. Par ailleurs, la croissance du commerce mondial et la réduction des contrôles physiques aux frontières ont accentué le risque d'augmentation du nombre de produits de contrefaçon en circulation. Le présent document va contribuer à renforcer ces contrôles en mettant en place des éléments de preuve plus fiables de l'authenticité et de l'intégrité des biens matériels.

La fraude sur les produits inclut, sans toutefois s'y limiter, la contrefaçon, l'adultération, l'effraction, la substitution et la simulation.

L'impact de la fraude sur les produits peut inclure, sans toutefois s'y limiter:

- une tromperie pour le consommateur;
- une tromperie pour l'acheteur de biens matériels neufs ou de pièces de rechange;
- une atteinte aux droits de propriété intellectuelle;
- une violation des lois nationales, régionales ou internationales;
- de fausses déclarations concernant:
    - les droits de propriété intellectuelle;
    - les détails de fabrication;
    - les détails sur la transaction et sur l'origine d'un produit;
    - des codes d'identification et/ou des éléments authentifiants.

Le problème de la fraude sur les produits est aggravé par les facteurs suivants:

- le marché devient de plus en plus mondial;
- les biens matériels et leur chaîne d'approvisionnement deviennent de plus en plus complexes;

— les déplacements de biens matériels à l'échelle mondiale se développent et peuvent emprunter des canaux non traditionnels.

La contrefaçon doit être distinguée du détournement.

Il peut être difficile pour un inspecteur, qu'il s'agisse d'un professionnel, d'un citoyen ou d'un consommateur, de reconnaître les caractéristiques d'un bien matériel authentique donné.

Les dispositions légales, y compris les garanties de conformité et de qualité, conçues pour permettre aux professionnels de mettre sur le marché des biens matériels sûrs dans des conditions commerciales loyales, ne sont pas respectées en cas de contrefaçon. Les acheteurs n'accordent pas nécessairement toute l'attention requise aux biens matériels qu'ils sont en train d'examiner, en particulier pour des raisons de confiance, par manque de temps, du fait de la tentation imputable à des prix attractifs ou simplement parce que le bien matériel lui-même ne leur est pas familier. L'élément authentifiant fournit une méthode particulière et plus fiable pour déterminer si l'article est authentique ou si c'est un produit de contrefaçon.

Établir l'authenticité et l'intégrité d'un bien matériel, autrement dit identifier s'il s'agit d'un objet «authentique», «faux» ou résultant d'autres activités frauduleuses, consiste à rechercher s'il reproduit les caractéristiques essentielles du bien matériel authentique, afin de définir si l'infraction est avérée.

En cas de doute sur l'authenticité d'un bien matériel, l'inspecteur devra, après avoir observé les caractéristiques du bien matériel et/ou de l'élément authentifiant suspect, rechercher si celles-ci correspondent aux caractéristiques du bien matériel et/ou de l'élément authentifiant authentique. Le processus engagé consiste essentiellement en une analyse technique exploitant l'expérience, des éléments authentifiants, des outils d'authentification ou une combinaison de ces méthodes.

Le présent document a été élaboré pour définir plus précisément les objectifs et les limites nécessaires à une application dans l'industrie et les services. Il définit les critères de performance de solutions d'authentification dédiées.

Ces solutions sont destinées à fournir des éléments de preuve fiables permettant d'apprécier plus facilement si les biens matériels sont authentiques et s'ils n'ont pas été contrefaits, altérés, imités, remplacés, remplis à nouveau, falsifiés ou s'ils n'ont pas fait l'objet d'autres types de fraude.

Le présent document intègre les critères de performance des solutions d'authentification. Le cycle de vie d'un bien matériel doit être pris en compte. Alors que l'authentification des biens de grande consommation est souvent centrée sur l'emballage, les solutions d'authentification des biens matériels à cycles de vie plus longs sont axées sur le bien lui-même, tout au long de son cycle de vie.

Le présent document s'intègre à un cadre plus large de normes connexes. Il n'a ni pour objectif, ni pour effet de définir un moyen exclusif d'authentification.

L'expérience démontre que les progrès technologiques sont utilisés par les contrefacteurs pour rendre les produits contrefaits moins détectables. Parallèlement, de nouvelles technologies d'authentification (par exemple, matérielles, numériques, ou les deux) peuvent donner aux inspecteurs chargés de l'application de la loi, aux opérateurs économiques légitimes et aux consommateurs de meilleurs moyens de détecter les contrefaçons et d'agir en conséquence. Le présent document s'applique indépendamment de la technologie d'authentification utilisée et recommande des moyens d'anticiper les actes frauduleux.

Le présent document comprend donc les parties suivantes:

— une typologie commune des solutions d'authentification;

— une compréhension de la manière dont une solution d'authentification peut constituer une solution plus robuste lorsqu'elle est stratifiée, et de ce fait elle favorise l'utilisation d'éléments authentifiants individuels en combinaison;

— le rôle de la résistance aux effractions et aux preuves d'effraction dans le cadre de la solution d'authentification;

— des critères sur le type de solution pouvant être utilisé pour procéder à des authentifications dans différents scénarios de contrôle;

— les méthodes de vérifications de biens matériels dans tous les lieux, circonstances et conditions d'utilisation prévus;

— les exigences et les critères d'évaluation relatifs à la sécurité pour les solutions d'authentification.

Les thèmes principaux du présent document peuvent être représentés par un cycle PDCA (Plan–Do–Check–Act) (voir Figure 1).

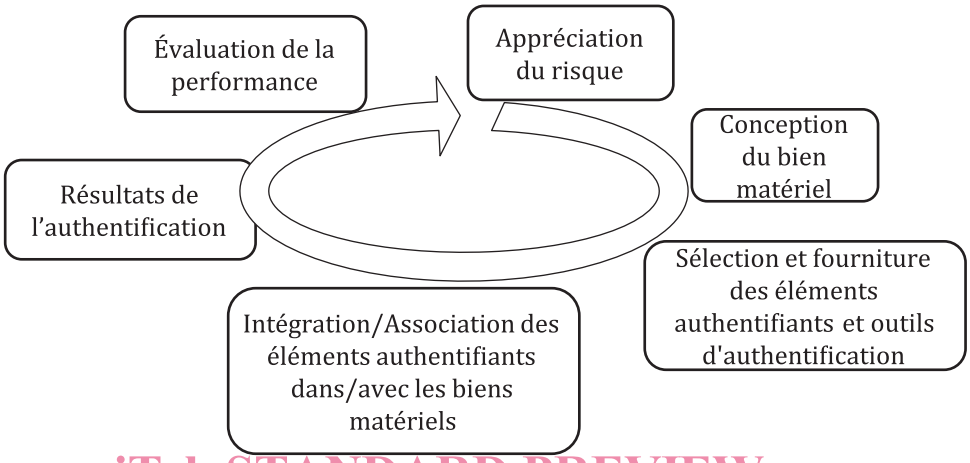

Figure 1 — Séquence des thèmes principaux

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices pour la sélection et l'évaluation de la performance des solutions d'authentification pour les biens matériels

1 Domaine d'application

Le présent document fournit des lignes directrices pour les critères et une méthodologie d'évaluation de la performance des solutions d'authentification qui visent à établir sans ambiguïté l'authenticité et l'intégrité d'un bien matériel durant l'ensemble de son cycle de vie. Il traite essentiellement de l'authentification d'un bien matériel et, le cas échéant, de ses composants, pièces ou des données associées:

— couverts par des droits de propriété intellectuelle;

— couverts par les réglementations internationales, régionales ou nationales;

— pouvant être concernés par la contrefaçon;

— avec ou sans une identité caractéristique.

Le présent document s'applique à tous les types et tailles d'organisations qui requièrent la capacité de valider l'authenticité et l'intégrité de biens matériels. Il aidera les organisations lors de la détermination, d'une part, des catégories d'éléments authentifiants dont elles ont besoin pour s'opposer aux risques liés à la contrefaçon, et, d'autre part, des critères de choix desdits éléments, une appréciation du risque de contrefaçon ayant été préalablement menée.

Les solutions d'authentification peuvent être utilisées dans des domaines tels que la lutte contre la contrefaçon, la prévention des fraudes et la prévention des détournements.

Le présent document ne traite pas des critères économiques ayant pour but d'établir une corrélation entre la performance et le coût des solutions d'authentification.

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 22300, *Sécurité et résilience — Vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO 22300 ainsi que les 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:

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

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

3.1
attaque
tentative(s) réussie(s) ou non de mettre en échec une solution d'authentification, comprenant des tentatives d'imitation, de production ou de reproduction à l'identique des éléments authentifiants

3.2
élément authentifiant contrôlable avec outil
élément authentifiant non perçu par les sens de l'être humain jusqu'à ce qu'une personne expérimentée recoure à un outil pour le leur révéler ou pour en permettre l'interprétation automatisée

[SOURCE: ISO 22300:2018, 3.58, modifiée — La définition a été reformulée.]

3.3
intégrité
propriété de protection de la précision et de l'exhaustivité des actifs

Note 1 à l'article: les actifs désignent les biens matériels et leur emballage primaire.

Note 2 à l'article: l'intégrité concerne également les données associées, les informations ou les éléments, ainsi que les moyens nécessaires à leur traitement.

[SOURCE: ISO 22300:2018, 3.123, modifiée — Les Notes 1 et 2 à l'article ont été ajoutées]

3.4
matière première
tout élément, constituant ou partie d'un bien matériel

3.5
détenteur de droits
personne physique ou morale détenant un ou plusieurs droits de propriété intellectuelle ou autorisée à les utiliser

[SOURCE: ISO 22300:2018, 3.198, modifiée — ajout de «personne physique ou».]

3.6
sécurité
situation caractérisée par l'absence de dangers ou de menaces, dans laquelle des procédures sont observées ou qui découle de mesures appropriées

[SOURCE: ISO 22300:2018, 3.223, modifiée — ajout de «dans laquelle des procédures sont observées ou qui découle de mesures appropriées».]

3.7
simulation
représentation par imitation du fonctionnement d'un système ou d'un processus à l'aide du fonctionnement d'un autre système ou processus

3.8
spécifieur
personne ou entité qui définit les exigences relatives à la solution d'authentification devant être appliquée à un bien matériel particulier

[SOURCE: ISO 22300:2018, 3.246, modifiée — Ajout de «personne ou».]

3.9
preuve d'effraction
aptitude de la solution d'authentification ou de l'élément authentifiant à montrer qu'il a été porté atteinte au bien matériel

[SOURCE: ISO 22300:2018, 3.254, modifiée — Ajout de «de la solution d'authentification ou».]

3.10
suivi logistique
moyen d'identification de chaque bien matériel ou de chaque lot ou série, permettant de savoir où il se trouve (suivi) et où il était (traçabilité) dans la chaîne de distribution

[SOURCE: ISO 22300:2018, 3.264, modifiée — «où il se trouve (suivi) et où il était (traçabilité) dans la chaîne de distribution» remplace «où il était (traçabilité) et où il se trouve (suivi) dans la chaîne d'approvisionnement».]

3.11
vérification
confirmation, par des preuves, que les exigences spécifiées ont été satisfaites

Note 1 à l'article: La vérification peut inclure un contrôle de l'existence d'un identifiant unique et de sa validité au sein d'un système d'identification des objets.

4 Principes

4.1 Généralités

Il convient que l'organisation choisisse les éléments authentifiants les plus appropriés pour constituer une solution d'authentification d'un bien matériel en fonction de l'appréciation du risque et du contexte de la mise en œuvre et de l'usage de ce bien matériel.

Lors du choix d'une solution d'authentification, il convient que l'organisation prenne en compte des critères techniques, logistiques et financiers qui dépendront de nombreux facteurs, par exemple:

— les caractéristiques du ou des éléments authentifiants;

— les méthodes de vérification;

— tout système d'information requis;

— les exigences en matière de sécurité;

— la résistance à la contrefaçon;

— la résilience en cas d'effraction;

— la valeur des biens matériels à protéger;

— les risques associés à la contrefaçon durant tout le cycle de vie du bien matériel;

— les exigences en matière d'intégration et de mise en œuvre;

— le type d'emballage;

— les éléments de preuve de la falsification, contrefaçon ou copie de certaines caractéristiques.

Il convient que l'organisation ne choisisse pas une solution d'authentification qui affecte ou modifie de manière non contrôlée les fonctionnalités et l'intégrité prévues des biens matériels.

NOTE Les éléments authentifiants peuvent faire partie des fonctionnalités d'un produit, par exemple dans l'approche sécurité par conception, selon laquelle la sécurité est intégrée au produit au stade de sa conception.

Il convient que l'organisation connaisse les lois et règlements applicables, notamment en matière de confidentialité et de sécurité.

Pour que la solution d'authentification d'un bien matériel puisse être établie, le processus de création doit être suivi d'un processus d'inspection. Le processus de création consiste à définir, générer et fabriquer les éléments authentifiants, puis à les intégrer dans le bien matériel ou dans son emballage. Le processus d'inspection inclut la vérification des éléments authentifiants tout au long de la chaîne de

distribution par des personnes ayant reçu une formation, utilisant les sens de l'être humain, des outils ou références. Ces deux processus sont reliés en un cycle «Planifier-Déployer-Contrôler-Agir» (PDCA) et les acteurs impliqués font partie intégrante de la solution d'authentification.

Les processus de vérification des éléments authentifiants déployés dans ces solutions requièrent une capacité de lecture, d'observation, d'analyse, de capture, et parfois de prélèvement, en faisant appel aux sens de l'être humain ou à des outils. Ces outils vont soit apporter une réponse locale immédiate, soit faire appel en temps réel à un système d'information sécurisé, soit encore acheminer l'information, le prélèvement ou le bien matériel vers une structure d'expertise qui donnera un diagnostic en temps différé.

Il convient donc que le niveau de performance d'une solution d'authentification soit apprécié dans son ensemble, pour toutes ses composantes et leurs interfaces.

L'analyse de la stratégie impose que les titulaires de droits examinent les questions majeures suivantes.

— Quels problèmes et menaces la contrefaçon présente-t-elle?

— Quelle est la probabilité que mes produits, mon organisation et mon activité soient concernés par des risques de contrefaçon, et quelles en seraient les conséquences?

— Parmi mes biens matériels (ou les matières premières qui les constituent), lesquels sont contrefaits ou pourraient l'être?

— À quels endroits sommes-nous confrontés à la contrefaçon et comment les contrefaçons sont-elles distribuées?

— Quel est le contexte de la fabrication et de la chaîne de distribution des biens matériels et quels sont les risques de contrefaçon?

— Quel est le contexte de la fabrication et de la chaîne de distribution des matières premières et quels sont les risques de contrefaçon?

— Comment et par qui le processus d'authentification sera-t-il réalisé?

— Quel est l'impact de l'erreur humaine sur la solution (processus et authentification)?

4.2 Processus de sécurité par conception pour les solutions d'authentification

Il convient que l'organisation suive le diagramme de processus décrit à la Figure 2 lors de la conception de la solution d'authentification. Ce processus inclut une analyse adéquate des risques associés aux caractéristiques des biens matériels, y compris des matières premières, des options d'authentification, et des conséquences et de l'historique des actes de contrefaçon tels que l'adultération, l'effraction, la substitution/le remplissage, la simulation, le clonage ou le détournement.

