NORME INTERNATIONALE

ISO 12931

Première édition
2012-06-01

Critères de performance des solutions d'authentification utilisées pour combattre la contrefaçon des biens matériels

Performance criteria for authentication solutions used to combat counterfeiting of material goods

Numéro de référence
ISO 12931:2012(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 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) 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 (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

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. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO 12931 a été élaborée par le comité de projet ISO/PC 246, *Dispositifs techniques anti-contrefaçon*.

Introduction

Depuis plus d'une décennie, la contrefaçon des biens matériels se développe rapidement, tant au niveau quantitatif que qualitatif; elle ne se limite plus aux produits de luxe. La vente de biens de contrefaçon 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 contrefaisantes 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 la chaîne 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 ce fléau, les entreprises utilisent de plus en plus 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 générera une plus grande confiance parmi les consommateurs, renforcera la sécurité de la chaîne de distribution et aidera les autorités publiques à concevoir et mettre en œuvre des politiques préventives, dissuasives et répressives.

La contrefaçon peut comprendre, sans toutefois s'y limiter,

— une escroquerie pour le consommateur,

— une tromperie pour les acheteurs de biens matériels neufs ou de pièces de rechange,

— une atteinte aux droits de propriété intellectuelle, et

— une violation des lois nationales, régionales ou internationales.

La contrefaçon peut englober des revendications frauduleuses portant sur

— des droits de propriété intellectuelle,

— des détails de fabrication, et

— l'ornementation.

La contrefaçon doit être maintenue distincte du détournement.

Le problème de la contrefaçon est aggravé par les facteurs suivants:

— le marché se mondialise de plus en plus et les biens matériels deviennent de plus en plus complexes;

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

Par conséquent, un contrôleur a davantage de difficultés à reconnaître les caractéristiques de n'importe quel 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 d'un bien matériel, autrement dit reconnaître son caractère «vrai» ou «faux» consiste à rechercher si ce bien reproduit les caractéristiques essentielles du bien matériel authentique, qui aident à

établir s'il y a infraction ou non. Il faut donc, pour donner à cette contestation une base solide, commencer par établir en quoi consistent ces caractéristiques essentielles, notamment l'origine du bien matériel, puis vérifier si le bien matériel suspect présente ou non, concrètement et objectivement, ces caractéristiques.

En cas de doute sur l'authenticité d'un bien matériel, le contrôleur devra, après avoir observé les caractéristiques du bien matériel suspect et/ou de l'élément authentifiant, rechercher si celles-ci correspondent aux caractéristiques du bien matériel authentique et/ou de l'élément authentifiant. 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.

La présente Norme internationale a été élaborée pour définir plus précisément les objectifs et les limites requis pour une application dans l'industrie et les services. Elle définit les critères de performance de solutions d'authentification dédiées. Ces solutions d'authentification sont destinées à fournir des éléments de preuve fiables facilitant l'appréciation du caractère authentique ou falsifié de biens matériels.

La présente Norme internationale vise à intégrer les critères de performance des solutions d'authentification dans le cycle de vie du bien matériel dans toutes les situations, lorsque cela est nécessaire. L'authentification occupe ainsi une position au sein même du cycle de vie du bien matériel et des services, pour lutter contre la contrefaçon.

La présente Norme internationale a pour objet de s'intégrer dans un vaste cadre de normes connexes afférentes au domaine de la lutte contre la contrefaçon, où la preuve du caractère authentique ou falsifié d'un bien matériel peut être obtenue par tout moyen; elle n'a ni pour objectif, ni pour effet, de définir un moyen exclusif d'authentification.

Critères de performance des solutions d'authentification utilisées pour combattre la contrefaçon des biens matériels

1 Domaine d'application

La présente Norme internationale spécifie des critères et une méthodologie d'évaluation de la performance des solutions d'authentification utilisées pour établir l'authenticité d'un bien matériel durant l'ensemble de son cycle de vie. Elle ne précise pas comment les solutions techniques remplissent ces critères de performance.

La présente Norme internationale est destinée à tous les types et tailles d'organisations qui requièrent la capacité de valider l'authenticité de biens matériels. Elle a vocation à guider ces organisations lors de la détermination, d'une part, des catégories d'éléments authentifiants dont elles ont besoin pour s'opposer à ces risques, et d'autre part, des critères de choix desdits éléments, une analyse des risques de contrefaçon ayant été préalablement menée. Ces éléments authentifiants peuvent faire partie intégrante du bien matériel proprement dit et/ou de son emballage. Les critères s'appliquent au bien matériel et/ou à son emballage.

Les critères de performance seront pris en considération par ces organisations en relation avec leur situation spécifique.

La présente Norme internationale se concentre sur l'authentification des biens matériels

— couverts par des droits de propriété intellectuelle,

— couverts par la législation régionale ou nationale applicable,

— avec des implications pour la sécurité et la santé publique,

— avec ou sans une identité caractéristique.

La présente Norme internationale est axée sur les biens matériels. Elle n'est pas destinée à s'appliquer, par exemple, aux biens du domaine financier, aux documents officiels administratifs, aux papiers d'identité ou aux produits numériques téléchargeables.

La présente Norme internationale ne s'applique pas non plus aux technologies ou systèmes de suivi logistique des biens matériels. Le suivi logistique en soi n'étant pas une solution d'authentification, il ne relève pas du domaine d'application de la présente Norme internationale.

La présente Norme internationale ne traite pas de critères économiques ayant pour but de mettre en regard la performance et le coût des solutions d'authentification.

Il se peut que certaines industries et services aient des exigences réglementaires particulières qui nécessiteraient une fonctionnalité supplémentaire afin de remplacer une ou plusieurs parties de la présente Norme internationale.

La présente Norme internationale a pour but d'aider les organisations à appréhender leurs propres besoins en matière d'authentification, les stratégies possibles et les défis à relever. Elle vise à leur fournir un ensemble de critères pour analyser, préciser et mettre en œuvre leurs solutions d'authentification.

L'organisation déterminera le niveau d'assurance sécurité requis pour la solution d'authentification choisie. Le fournisseur de la solution d'authentification est censé se conformer aux exigences de l'organisation en matière de risque et de sécurité.

La présente Norme internationale ne vise pas à contraindre l'organisation dans son choix de technologies d'authentification.

2 Termes et définitions

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

2.1
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

2.1.1
attaque interne
attaque perpétrée par des personnes ou entités ayant un lien direct ou indirect avec le fabricant légitime, le créateur du bien ou le détenteur des droits (personnel du détenteur des droits, sous-traitant, fournisseur, etc.)

2.1.2
attaque externe
attaque perpétrée par des personnes ou entités n'ayant pas de lien direct ou indirect avec le fabricant légitime, le créateur du bien ou le détenteur des droits

2.2
bien matériel authentique
bien matériel produit sous le contrôle du fabricant légitime, du créateur du bien ou du détenteur des droits de propriété intellectuelle

2.3
authentification
acte consistant à établir si un bien matériel est authentique ou non

2.3.1
élément authentifiant
objet tangible, caractéristique visuelle ou information associée au bien matériel ou à son emballage, utilisé en tant que partie intégrante d'une solution d'authentification

2.3.1.1
élément authentifiant contrôlable sans outil
élément authentifiant pouvant être détecté et vérifié à l'aide d'un ou de plusieurs sens de l'être humain sans recourir à un outil (autre que les outils courants qui corrigent des sens déficients tels que lunettes ou prothèses auditives)

2.3.1.2
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

2.3.2
outil d'authentification
ensemble de logiciels et/ou matériels faisant partie d'une solution anti-contrefaçon et utilisé pour contrôler l'élément authentifiant

2.3.2.1
outil d'authentification autonome
outil d'authentification qui, soit est utilisé pour révéler un élément authentifiant contrôlable avec outil aux sens de l'être humain dans le cas d'une vérification humaine, soit comprend les fonctions requises pour être apte à vérifier l'élément authentifiant de manière indépendante

2.3.2.2
outil d'authentification connecté
outil d'authentification qui nécessite une connexion en temps réel pour pouvoir interpréter localement l'élément authentifiant

2.3.2.3
outil d'authentification en vente libre
outil d'authentification qui peut être acquis dans les réseaux de vente ouverts

2.3.2.4
outil d'authentification dédié
outil d'authentification dédié à une solution d'authentification spécifique

2.3.3
solution d'authentification
ensemble complet de moyens et de procédures qui permet d'effectuer l'authentification d'un bien matériel

2.4
interprétation automatisée
évaluation automatique de l'authenticité par un ou plusieurs composants de la solution d'authentification

2.5
contrefaire
simuler, reproduire à l'identique ou modifier un bien matériel ou son emballage sans autorisation

2.6
produit de contrefaçon
bien matériel imitant ou copiant un bien matériel authentique

2.7
taux de fausses acceptations
proportion d'authentifications déclarées vraies erronément

2.8
taux de faux rejets
proportion d'authentifications déclarées fausses erronément

2.9
analyse scientifique
méthode scientifique permettant d'authentifier des biens matériels en confirmant un élément authentifiant ou un attribut intrinsèque, via l'emploi d'un appareillage spécialisé par un expert qualifié ayant des connaissances particulières

2.10
interprétation humaine
évaluation de l'authenticité par le contrôleur

2.11
contrôleur
quiconque exploite la solution d'authentification dans le but d'authentifier un bien matériel

2.12
élément authentifiant intégré
élément authentifiant ajouté au bien matériel

2.13
intégrité
non-altération de l'élément authentifiant, des données associées, des informations ou des éléments et de leurs moyens de traitement

2.14
interopérabilité
degré de compatibilité d'une solution d'authentification avec des outils différents

2.15
élément authentifiant intrinsèque
élément authentifiant inhérent au bien matériel

2.16
vraisemblance
possibilité que quelque chose se produise

Note 1 à l'article: Dans la terminologie du management du risque, le mot «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

Note 2 à l'article: Le terme anglais «likelihood» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «probability» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «probability» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du management du risque, le terme «vraisemblance» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «probability» (probabilité) dans de nombreuses langues autres que l'anglais.

[SOURCE:ISO Guide 73:2009, définition 3.6.1.1]

2.17
bien matériel
produit manufacturé, cultivé ou fourni par la nature

2.18
cycle de vie d'un bien matériel
les différentes étapes de la vie d'un bien matériel, comprenant la conception, le dessin, la fabrication, le stockage, l'entretien, la revente et la mise au rebut

2.19
détenteur de droits
personne physique ou morale détenant un ou plusieurs droits de propriété intellectuelle ou autorisée à les utiliser

2.20
analyse du risque
processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque

Note 1 à l'article: L'analyse du risque fournit la base de l'évaluation du risque et les décisions relatives au traitement du risque.

Note 2 à l'article: L'analyse du risque inclut l'estimation du risque

[SOURCE: ISO Guide 73:2009, définition 3.6.1]

2.21
robustesse
capacité d'un dispositif à résister à des attaques externes ou internes, de nature physique ou informatique

Note 1 à l'article: Dans le contexte de la présente Norme internationale, il s'agit notamment de la capacité à résister à des tentatives d'imitation, de reproduction, d'intrusion ou de contournement

2.22
sécurité
situation caractérisée par l'absence de dangers ou de menaces, dans laquelle des procédures sont observées ou qui découle de mesures appropriées

2.23
secret
donnée et/ou savoir qui est protégé pour ne pas être révélé à des personnes non-autorisées

2.24
spécifieur
personne ou entité qui définit les exigences relatives à la solution d'authentification devant être appliquée à un bien matériel particulier

2.25
preuve d'effraction
aptitude de l'élément authentifiant à montrer qu'il a été porté atteinte au bien matériel

2.26
suivi logistique
moyen d'identification de chaque bien matériel ou de chaque lot ou série, permettant de savoir où il était (traçabilité) et où il se trouve (suivi) dans la chaîne de distribution

3 Principes généraux

3.1 Introduction

Les solutions d'authentification revêtent une large palette de formes, allant des solutions simples aux solutions complexes impliquant des architectures TIC (technologies de l'information). Une solution simple ne signifie pas une solution peu performante car, pour un bien matériel, la solution d'authentification la plus appropriée dépendra du contexte de mise en application et de l'usage.

Les critères techniques, logistiques et financiers qui entrent en jeu lors du choix de la solution d'authentification dépendent de nombreux facteurs, à savoir:

— les caractéristiques du ou des éléments authentifiants;

— les niveaux et méthodes de contrôle recherchés;

— tout système d'information requis;

— les exigences en matière de sécurité;

— la résistance à la contrefaçon;

— 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.

Il convient que les solutions d'authentification n'aient aucune incidence sur la fonctionnalité et l'intégrité des biens matériels.

Une application correcte de la présente Norme internationale repose sur le respect des lois et réglementations nationales, régionales et internationales, en particulier en matière de vie privée, de confidentialité et de sécurité.

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.

Ainsi, eu égard à la spécification de la protection du bien matériel, une solution d'authentification découle d'un processus de création qui est suivi d'un processus de contrôle. 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 de contrôle consiste à faire contrôler les 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 des références. Ces deux processus sont reliés en un modèle «Planifier-Déployer-Contrôler-Agir» (PDCA) et les acteurs impliqués font partie intégrante de la solution d'authentification.

Le niveau de performance d'une solution d'authentification doit donc être évalué 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 sont les problèmes de contrefaçon, les conséquences et la vraisemblance d'une menace de contrefaçon?

— Parmi mes biens matériels, 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?

— 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)?

3.2 Processus d'authentification

La solution d'authentification type est représentée sur la Figure 1. Elle révèle les liens existant entre le bien matériel à authentifier et les composantes types de la solution d'authentification. Prises conjointement, celles-ci conduisent à un verdict d'authenticité ou de fausseté, ou fournissent des informations qui permettront de déceler l'authenticité du bien matériel.

3.3 Exigences de performance des solutions d'authentification

la présente Norme internationale a pour objectif:

— d'établir une typologie commune des solutions d'authentification;

— d'établir un consensus sur la manière dont une solution d'authentification peut constituer une solution plus robuste lorsqu'elle est hiérarchisée et, donc, sur le fait qu'il convient d'utiliser des combinaisons des différents éléments authentifiants;

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

Elle vise ainsi à aider les utilisateurs réels et potentiels de solutions d'authentification à comprendre les fonctionnalités de celles-ci et les critères de choix adaptés à leur propre analyse du risque, ce qui facilitera la capacité de l'utilisateur:

— à effectuer des vérifications de biens matériels en tout lieu, dans toutes les circonstances et conditions d'usage prévisibles;

— à définir des exigences spécifiques pour chaque niveau de sécurité souhaité pour ses solutions d'authentification.

3.4 Typologie des solutions d'authentification

Cette typologie a pour but de fournir des indications aux utilisateurs et fournisseurs de solutions d'authentification qui permettent de comparer les solutions ou de les sélectionner en fonction de leurs caractéristiques. Son but n'est pas de classer les solutions selon leurs performances effectives. Le contexte dans lequel se fait l'examen facilite la détermination du choix de la ou des solutions d'authentification.

Les caractéristiques sous-jacentes de cette typologie reposent sur les considérations suivantes.