NORME INTERNATIONALE

ISO 22388

Première édition
2023-11

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices visant à sécuriser les documents physiques

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for securing physical documents

Numéro de référence
ISO 22388:2023(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'ISO attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de propriété revendiqué à cet égard. À la date de publication du présent document, l'ISO n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié tout ou partie de tels droits de brevet.

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*.

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

Les documents ont un rôle essentiel dans les transactions économiques, légales et sociales, notamment sans toutefois s'y limiter, les transactions financières, les titres de propriété, les transferts de titres, le transport, la vérification d'identité, les opérations douanières, les dossiers scolaires, les licences professionnelles et les permis de port d'arme. En raison de ces rôles, ils sont la cible de la contrefaçon, de la falsification et d'autres formes de fraude, ce qui réduit potentiellement la fiabilité des dites transactions et crée des dangers sur le plan économique, humain et social.

Le présent document est destiné à faciliter la vérification des documents physiques dans tous les contextes d'utilisation et à permettre d'évaluer la désignation des documents physiques. Cette évaluation implique aussi une appréciation visant à déterminer les niveaux de risque concernant les formes d'attaques les plus courantes, ainsi que le type et le nombre d'éléments de sécurité à incorporer dans les documents aux fins de leur authentification. En fonction de ces vérifications et de ces évaluations, il est prévu que les présentes lignes directrices servent de guide pour la sécurisation de tous les documents de sécurité (DS) désignés.

Il est important de tenir compte de l'utilisation des documents physiques dans l'appréciation des risques et des menaces, ainsi que pour déterminer la classification correspondante. Les documents courants peuvent être associés à un haut niveau de risque lorsqu'ils sont utilisés pour des fonctions critiques. Les présentes lignes directrices facilitent l'appréciation des risques pour diverses catégories de documents, mais elles n'ont pas pour objet d'identifier toutes les utilisations potentielles des documents.

Le présent document a pour objet d'aider les utilisateurs et les producteurs à déterminer les recommandations de sécurité associées aux documents produits ou fournis, à établir une classification relative de leurs documents et à renforcer la fiabilité des transactions justifiées par lesdits documents.

Il convient de reconnaître que les présentes lignes directrices fournissent des recommandations concernant les risques et menaces courants et les mesures de réduction au moment de leur publication. Les risques liés à la sécurité des documents physiques étant en constant changement, les technologies de sécurité visant à les atténuer le sont aussi. Pour cette raison, il est important que les utilisateurs des présentes lignes directrices reconnaissent que les notations de risque et de réduction sont relatives et qu'elles peuvent varier selon les changements concernant les risques et l'évolution des technologies de sécurité visant à atténuer ces risques. Il est recommandé aux utilisateurs des présentes lignes directrices de comprendre les concepts utilisés dans la mise au point d'une appréciation des risques liés à la sécurité et d'évaluer toutes les technologies de sécurité appropriées fraîchement mises au point pour déterminer quelle solution est la plus efficace.

Exemples de risques non couverts dans le présent document:

— risques techniques issus, par exemple, d'une utilisation incorrecte des outils de sécurité applicables;

— risques pour la gestion associés à la vérification des documents sous une surveillance inadaptée ou sans surveillance, ou au manque de formation du personnel assigné à l'examen des documents;

— risques organisationnels, notamment la collecte illégale de données provenant des documents examinés, ou l'acceptation de documents contrefaits par des acteurs internes en échange d'un gain économique ou dans le cadre d'une entreprise criminelle (par exemple, des agents de sécurité qui laissent entrer des clients en dessous de l'âge légal sur présentation d'une fausse carte d'identité, une fraude interne au sein d'un organisme de réglementation professionnelle, où le personnel accepte délibérément de faux papiers d'identité pour produire des papiers d'identité valides);

— risques externes, c'est-à-dire que les impacts sont en dehors du contrôle des organismes touchés (par exemple, coupures d'électricité ou panne des équipements à court terme);

— risques concernant la conformité lorsqu'une entreprise ne respecte pas les lois ou les réglementations prescrites, ce qui peut aboutir à des amendes ou à des actions en justice.

Le présent document a été élaboré sur la base de concepts et de méthodologies adaptées de la Référence [7].

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices visant à sécuriser les documents physiques

1 Domaine d'application

Le présent document fournit des recommandations sur la manière de sécuriser les documents physiques pour les entités de spécification de documents physiques. Il établit une procédure de design de sécurité, qui comprend:

— l'appréciation des risques;

— la détermination des classes de documents;

— l'introduction d'éléments de sécurité;

— l'évaluation de sécurité;

— la réduction des risques liés au document.

Le présent document s'applique aux documents physiques sécurisés, utilisés pour des actions importantes comme la validation de transactions de valeur, l'attribution d'accès, la justification de la conformité et la sécurisation de produits.

Le présent document ne s'applique pas aux billets de banque, aux documents de voyage lisibles par machine, aux permis de conduire, aux timbres postaux, aux timbres fiscaux, aux cartes relatives aux soins de santé et aux cartes nationales d'identité, qui sont couverts par les normes et réglementations existantes.

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 https://www.electropedia.org/

3.1
fraude documentaire
tromperie illicite ou criminelle qui utilise des *documents de sécurité* (3.4) pour un gain financier ou personnel

Note 1 à l'article: La fraude désigne une tromperie illicite ou criminelle destinée à générer un gain financier ou personnel qui crée un préjudice social ou économique.

Note 2 à l'article: La fraude comprend les usages frauduleux qui n'impliquent pas nécessairement la régénération de documents (par exemple, un imposteur qui utilise les papiers d'identité d'une autre personne pour usurper son identité).

Note 3 à l'article: Il convient de considérer séparément la fraude liée aux systèmes électroniques à transmission numérique.

3.2
communication sur le risque
échange ou partage d'informations sur les risques entre un émetteur et d'autres parties intéressées

Note 1 à l'article: Ces informations peuvent concerner l'existence, la nature, la forme, la probabilité, la gravité, l'acceptabilité, le traitement, ou d'autres aspects liés au risque.

[SOURCE: ISO 22300:2021, 3.1.220, modifié — Définition révisée.]

3.3
d'investigation (en anglais: *forensic*)
<document physique> application de méthodes scientifiques permettant d'authentifier des documents en confirmant un *élément de sécurité* (3.6) ou un attribut intrinsèque, via l'emploi d'un appareillage spécialisé par un expert qualifié ayant des connaissances particulières

3.4
document de sécurité
DS
document protégé par une combinaison d'éléments choisis pour réduire le risque de contrefaçon

3.5
entité de spécification
personne ou organisme qui définit les exigences relatives à la solution d'authentification devant être appliquée à un *document de sécurité* (3.4) particulier

3.6
élément de sécurité
élément d'un document qui est associé à une méthode de vérification spécifique et permet ainsi de s'assurer de l'intégrité du document et/ou de son authenticité en tant que document émis en bonne et due forme, notamment le fait qu'il n'ait pas fait l'objet d'une effraction

[SOURCE: ISO/IEC 18013-1:2018, 3.27]

3.7
document vierge
document prêt à être personnalisé après l'impression du fond de protection uniformisé sur le substrat

Note 1 à l'article: Le fond de protection inclut souvent des *éléments de sécurité* (3.6).

4 Principes de sécurité des documents

4.1 Catégories d'utilisateurs

Dans le cadre de l'authentification des documents, les utilisateurs potentiels sont classés comme suit:

— généralités: détenteurs de DS et utilisateurs associés à des tiers qui procèdent au traitement des documents;

— spécifiques: guichetiers, vérificateurs de documents et autres personnes fournissant des services prescrits, avec vérification «vrai-faux», sur la base des fonctions des documents définies par l'émetteur;

— autorités et experts: parties qui déterminent les spécifications des DS, personnel des organismes officiels d'investigation et d'analyse ayant une expertise en matière de vérification, et autres contrôleurs ayant une connaissance approfondie des spécifications de sécurité.

Il convient que l'entité de spécification tienne compte des ressources des utilisateurs présentées dans le Tableau 1 pour spécifier la sécurité des documents. Voir également le Tableau D.1.

Tableau 1 — Utilisateurs et ressources

Utilisateurs	Ressources		
	Temps disponible pour l'inspection[a]	Expertise ou formation	Accès aux outils d'inspection
Généraux	Limité	Limité ou aucun	Limité ou aucun
Spécifiques	Moyen	Moyen	Moyen
Autorités et experts	Étendu	Étendu	Étendu

[a] Pour que l'inspection soit correcte, il convient que le temps d'inspection nécessaire corresponde à la disponibilité de l'utilisateur.

4.2 Stades des documents

Il convient que l'entité de spécification utilise les stades suivants pour décrire le cycle de vie d'un DS, voir également la Figure 1:

— le design de sécurité, qui consiste en l'intégration de mesures de sécurité contre diverses fraudes documentaires qui menacent chaque procédure pendant la durée de vie du document. Cette démarche comprend l'examen et l'amélioration de la sécurité du document;

— la production de documents vierges, qui comprend la mise en œuvre des spécifications relatives à la conception et au processus de fabrication global, notamment l'acquisition de matières premières, la production, le contrôle de la qualité, les essais, le stockage et le transport de manière opérationnelle vers l'entité de personnalisation;

— la personnalisation, qui comprend l'intégration de contenus variables comme des valeurs monétaires, des informations sur la qualification personnelle et des références concernant les éléments de certification figurant sur les documents vierges, selon les exigences de l'émetteur;

— l'émission, qui désigne le fait de délivrer un DS à une entité validée;

NOTE La délivrance implique le transport sécurisé du DS jusqu'à l'entité prévue.

— la durée de vie utile, qui correspond à la durée pendant laquelle le document conserve sa fonction documentaire, notamment son efficacité en matière de sécurité;

— la révocation, qui désigne l'abandon et la suspension volontaires des DS par une entité autorisée. Les documents sont soumis à des procédures physiques, comme le strict abandon pour éviter la réutilisation, l'impression, la perforation et d'autres actes, afin d'assurer l'abandon.

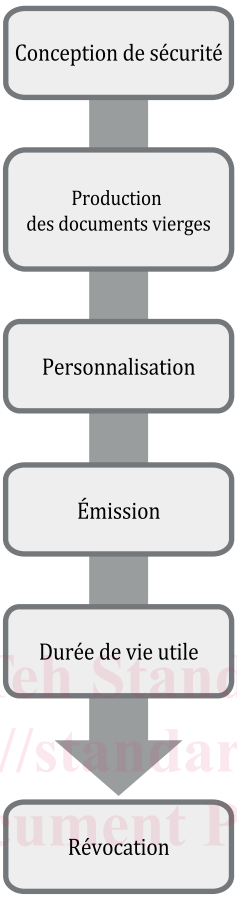

Figure 1 — Progression linéaire des stades d'un document

4.3 Éléments à protéger

Il convient que l'entité de spécification protège les éléments suivants contre diverses menaces:

— DS (pendant tout leur cycle de vie): il convient que les DS soient très résistants vis-à-vis de la contrefaçon et qu'ils soient vérifiables. Il convient de marquer clairement comme telles les copies officielles de DS produites par photocopie ou par d'autres moyens;

— processus de fabrication, notamment la production, la personnalisation et l'émission;

— intégrité des informations enregistrées: il convient que les informations enregistrées sur les DS et les éléments de sécurité associés restent dans leur état d'origine dans lequel ils ont été fournis par l'émetteur et attestés par les éléments de lutte contre la contrefaçon ou l'effraction appropriés, lesquels exigent une résistance physique et chimique. Il convient que les contre-mesures permettent de détecter les falsifications comme la suppression, la modification ou le recouvrement de données.

La personnalisation a une incidence sur la protection de la vie privée; il convient par conséquent que les concepteurs et les développeurs respectent les exigences de l'ISO 31700-1. La protection de la vie privée est réglementée dans de nombreuses juridictions.

4.4 Considérations concernant la fabrication sécurisée

Il convient que l'entité de spécification tienne compte des éléments suivants pour concevoir et fabriquer les DS et pour déterminer les éléments de sécurité:

— matériaux: il convient de contrôler correctement la composition, la formulation et la fabrication des matières premières utilisées pour les éléments de sécurité, et que les matériaux ne soient pas facilement disponibles pour ceux qui tentent de frauder;

— machines de fabrication: il convient de contrôler correctement les dispositifs utilisés pour fournir et pour produire les éléments de sécurité, et qu'ils ne soient pas facilement disponibles;

— méthodes de production: il convient de contrôler correctement les méthodes de production des éléments de sécurité;

NOTE 1 Des recommandations à l'attention de l'entité de spécification, concernant la gestion des processus de sécurité comme la fabrication, le stockage, la distribution et l'obligation de rendre des comptes, sont disponibles dans l'ISO 14298.

— principes: il convient de conserver les principes, les mécanismes et les spécifications des éléments de sécurité de manière sécurisée et confidentielle;

— stabilité de la qualité: il convient de réduire autant que possible les variations de qualité entre les DS au moment de la mise en œuvre des éléments de sécurité et de la fabrication, afin d'éviter les fausses identifications de contrefaçon;

— durabilité: Il convient que l'authentification des DS soit possible indépendamment des changements d'apparence liés à l'utilisation et au vieillissement (notamment les différences individuelles présentes au moment de la production).

NOTE 2 «Contrôler correctement» signifie que les matériaux et les processus sont contrôlés selon les pratiques de sécurité acceptées, par exemple conformément à l'ISO 14298 et à la Référence [8], ou à des pratiques industrielles de sécurité acceptées équivalentes.

5 Design de sécurité des documents

5.1 Généralités

Il convient que l'entité de spécification suive la procédure de design de sécurité décrite dans la Figure 2, afin de gérer les risques associés aux utilisations abusives ou à la fraude en s'alignant sur l'ISO 31000 lors de la définition de la spécification concernant les DS.

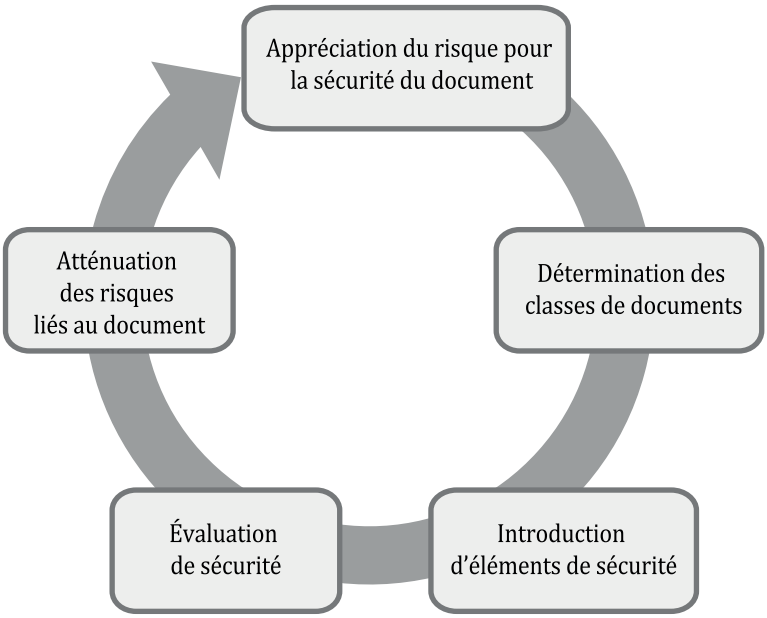

Figure 2 — Procédures de design de sécurité

5.2 Appréciation du risque pour la sécurité des documents

5.2.1 Estimation du risque

L'entité de spécification peut réaliser une appréciation du risque concernant un document lorsqu'un examen initial indique la possibilité d'une fraude ou d'une utilisation abusive et que les impacts possibles, s'ils sont source de risques, ne sont pas atténués. Si possible, il convient de fonder la méthode d'appréciation du risque sur des données quantitatives et, en présence de certains degrés d'incertitude, de reconnaître l'estimation qualitative comme un guide pour l'appréciation. Il convient que la méthode d'appréciation du risque tienne compte:

— des quatre modes de fraude documentaire;

— des intentions et des capacités des auteurs de menace connus ou potentiels;

— des facteurs de risques spécifiques issus de l'objet, de l'utilisation, de la distribution et de la période de validité du document.

NOTE Un exemple d'estimation de la notation de risque pour un DS général est fourni dans l'Annexe A.

5.2.2 Quatre facteurs d'attaque pour la fraude documentaire

La fraude documentaire est généralement divisée entre les quatre modes d'attaque suivants:

— clonage: reproduction d'un original comprenant des éléments de sécurité qui emploient les mêmes composants de base et les mêmes techniques de fabrication que l'original. Dans ce scénario, une partie non autorisée à émettre le document utilise des matériaux équivalents ou semblables aux versions authentiques, imite la structure interne et crée une contrefaçon dont l'apparence et les caractéristiques sont similaires à l'original. Le clonage s'appuie habituellement sur la rétro-ingénierie;

— fac-similé: reproduction non autorisée d'un original avec ses éléments de sécurité, réalisée avec des composants et des techniques de fabrication de base différents de ceux de la version originale, mais dont l'apparence est capable de tromper le contrôleur. La structure interne et les caractéristiques ne sont pas nécessairement similaires à ceux de l'original;

