NORME INTERNATIONALE

ISO 22385

Première édition
2023-02

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices visant à établir un cadre pour la confiance et l'interopérabilité

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines to establish a framework for trust and interoperability

Numéro de référence
ISO 22385:2023(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'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*.

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

Il est essentiel d'instaurer la confiance, l'interopérabilité et l'interopération dans le monde numérique. Pour limiter les dommages résultant de la contrefaçon de documents physiques et électroniques, de produits, de logiciels et de services, il est nécessaire de prévoir des couches de sécurité physiques et numériques.

Les schémas des ensembles de données encodées signés électroniquement (Electronically signed encoded data set, ESEDS) peuvent être utilisés pour décourager la contrefaçon lorsque quiconque tout au long de la chaîne d'approvisionnement, y compris les distributeurs, les courtiers indépendants, les agents des forces de l'ordre et les clients finaux, peut les utiliser pour accéder à une description locale ou distante sécurisée d'un produit ou d'un document. Un mécanisme commun et unique de contrôle d'intégrité des données appliqué à divers éléments spécifiques et individuels ou à des identifiants de ressource uniforme (URI) peut contribuer à la détection précoce des contrefaçons.

Le présent document, applicable aux schémas ESEDS, est destiné à permettre l'utilisation de processus fiables et sûrs d'authentification et de traçabilité des produits (matériel, logiciel, services, etc.) en décrivant l'environnement de confiance nécessaire. Cela afin de favoriser l'interopération des services de confiance par le biais de mécanismes de marquage et de surveillance tout au long de la chaîne de valeur des produits et des documents.

Le schéma ESEDS proposé est destiné à rester un schéma totalement volontaire, indépendant des autres systèmes d'authentification comme de suivi et traçabilité.

L'utilisation de l'ESEDS pour accéder à des données dignes de confiance provenant d'une source locale ou distante donne aux utilisateurs finaux et aux agents des forces de l'ordre un outil puissant pour détecter les contrefaçons et réduire le risque d'exposition à des produits et documents contrefaits.

L'ESEDS utilise la capacité de signature électronique à vérifier l'intégrité des données et à identifier/authentifier le fabricant/émetteur du produit ou du document sur lequel l'ESEDS est mis en place. La vérification peut être effectuée en ligne ou hors ligne en utilisant les fonctions prises en charge par le fichier descripteur du cas d'usage signé (« manifeste »).

L'ESEDS peut prendre la forme de deux supports différents ou de toute combinaison:

— imprimé sur un produit physique ou tout document physique;

— comme un ensemble de données électroniques et/ou affiché et lu comme un code lisible par machine (machine-readable code, MRC).

La mise en œuvre de ces lignes directrices permet à différents secteurs et acteurs du marché de partager la même architecture et sémantique du schéma ESEDS global, la définition des acteurs et les processus associés. Il est ainsi possible d'obtenir une interopérabilité sectorielle et une interopération croisée globale.

La lutte contre la fraude qui affecte les documents physiques et électroniques, les produits, les logiciels et les services dans la chaîne d'approvisionnement est un défi majeur. Les problèmes de fraude ont un impact considérable sur les sous-traitants, les partenaires et les fournisseurs. Parallèlement, un nombre croissant de réglementations nationales et internationales exigent une responsabilité totale « dos à dos », comme la Directive sur la responsabilité des produits aux États-Unis d'Amérique et en Europe, ainsi que le Règlement général sur la protection des données personnelles (RGPD) dans l'Union européenne (UE).

L'instauration de la confiance et de l'interopération facilitera cette conformité en matière de responsabilité grâce à l'utilisation d'un ESEDS. Celui-ci aidera à comprendre correctement l'UID de tout fabricant/fournisseur particulier pour un produit, un sous-produit, un logiciel et des services donnés dans différents secteurs du marché. Il deviendra alors possible de mettre en place une identification et un contrôle d'authenticité interopérables en ligne et/ou hors ligne du produit, du document, du logiciel ou des services.

Cela implique que tous les acteurs des différents secteurs du marché aient la même compréhension du schéma ESEDS complet, de son modèle de gouvernance et de sa hiérarchie et structure de documentation.

Le schéma global est résumé dans l'organigramme de la Figure 1.

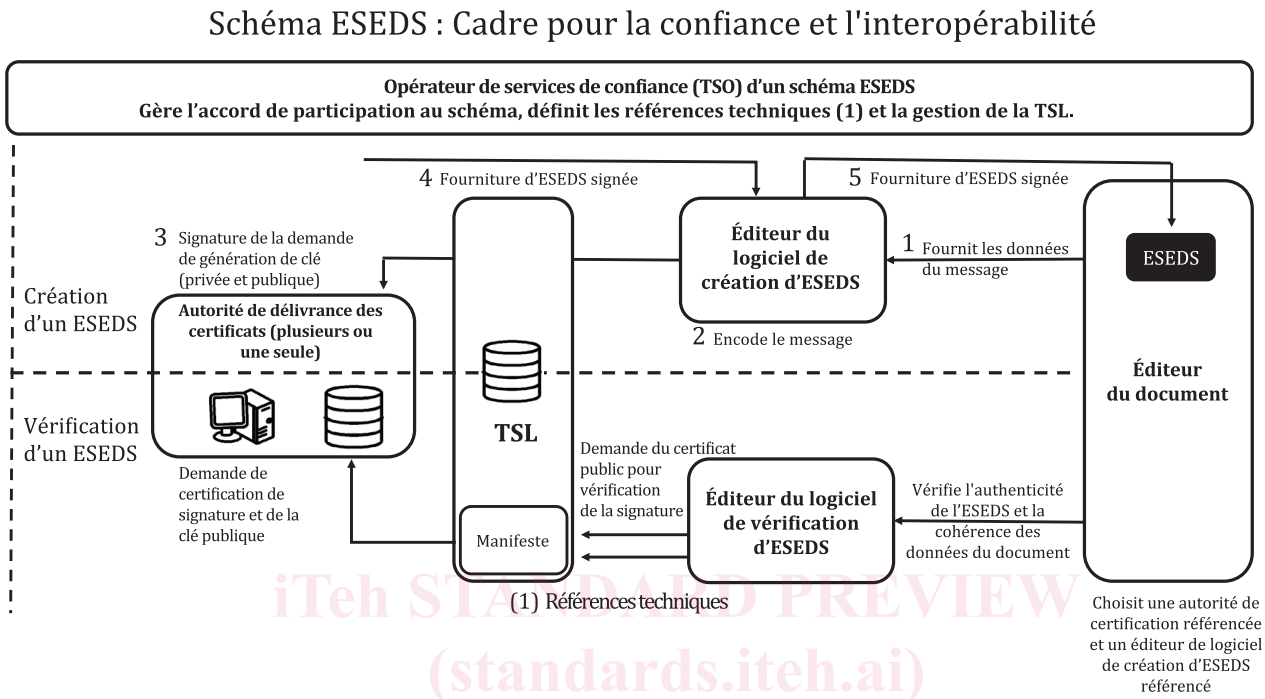

Figure 1 — Schéma ESEDS

Le présent document contient les éléments suivants à prendre en considération pour la conception d'un ESEDS fiable et sûr:

— document fondamental du schéma (voir Article 4);

— recommandations s'appliquant aux acteurs du schéma (voir Article 5);

— mesures organisationnelles (voir Article 6);

— mesures techniques (voir Article 7);

— ressources du schéma interne (voir Article 8);

— annuaires (voir Article 9).

Ces articles sont les éléments essentiels du modèle de gouvernance d'un ESEDS. Chaque article est constitué d'un ou plusieurs documents qui décrivent les éléments obligatoires à produire par les différents acteurs du schéma ESEDS.

Tous les éléments essentiels du schéma ESEDS sont présentés sous forme hiérarchisée dans la Figure 2.

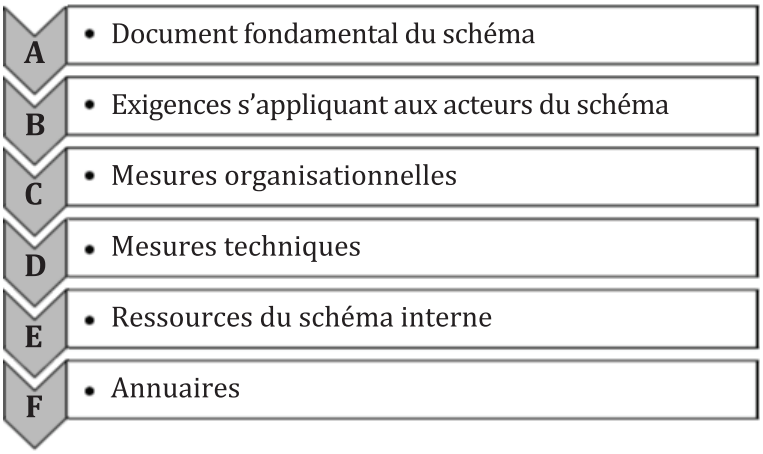

Figure 2 — Éléments essentiels de l'ESEDS

Le modèle ESEDS proposé par le présent document peut être appliqué par de multiples autorités de certification (AC) indépendantes, contrairement au modèle de l'Organisation de l'aviation civile internationale (OACI) qui concerne uniquement les AC hiérarchiques multinationales parent/enfant. L'organisation de l'environnement de confiance proposée par le présent document permet donc à la fois aux modèles d'AC hiérarchiques (comme l'OACI) et aux modèles sectoriels, nationaux ou internationaux basés sur des AC multisectorielles de coopérer. Sur la base de cette approche, il est possible de développer une application de lecture universelle (trusted entry point, TEP, ou « point d'entrée de confiance ») qui est agnostique à tout cas d'usage, à condition que des structures de données communes soient utilisées. Le système ESEDS peut être considéré comme un environnement de confiance mondial potentiel si les règles et principes du présent document sont respectés. En fin de compte, l'interopération entre les réseaux de confiance des opérateurs de services de confiance (TSO) indépendants peut être obtenue en utilisant les mêmes structures de données communes, fondées sur des normes et des spécifications appropriées, et par la reconnaissance mutuelle de leurs schémas ESEDS respectifs.

Le présent document est applicable aux développeurs et aux utilisateurs des systèmes d'identification sécurisés et interopérables. Il est ouvert à tous les secteurs d'activité et est agnostique sur le plan technologique. Il n'interfère pas avec les systèmes d'identification, de suivi et traçabilité et d'authentification existants, mais est capable d'introduire une interaction entre eux.

Le présent document fait partie d'une série de normes qui inclut l'ISO 22380, l'ISO 22381, l'ISO 22382, l'ISO 22383 et l'ISO 22384.

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices visant à établir un cadre pour la confiance et l'interopérabilité

1 Domaine d'application

Le présent document établit un cadre pour un environnement de confiance pour le traitement et la communication de l'information qui protège l'intégrité tout au long de la chaîne d'approvisionnement des documents physiques et électroniques connexes, des produits, des logiciels et du cycle de vie des services pour limiter la fraude sur les produits et les marchandises contrefaites, en utilisant des techniques d'identification des objets.

Le présent document donne des lignes directrices visant à établir un cadre pour garantir la confiance, l'interopérabilité et l'interopération par le biais de schémas d'ensembles de données encodées signés électroniquement (ESEDS) sûrs et fiables pour les applications multi-acteurs et sont même applicables dans un environnement multisectoriel.

Le présent document n'interfère pas avec les systèmes de traçabilité, d'identification et d'authentification existants, mais est capable de soutenir l'interopération entre eux en introduisant un schéma d'ESEDS.

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
ensemble de données encodées signé électroniquement
ESEDS (electronically signed encoded data set)
ensemble de données structuré contenant l'en-tête, les données utiles, la signature et un bloc de données auxiliaires facultatif

Note 1 à l'article: Le type de données utiles et l'identité de l'émetteur sont inclus dans l'en-tête.

Note 2 à l'article: L'ESEDS peut souvent être exprimé sous forme de *code lisible par une machine* (3.3).

3.2
opérateur de service de confiance
TSO (trust service operator)
entité juridique qui est le propriétaire unique du schéma complet d'*ensemble de données encodées signé électroniquement* (*ESEDS*) (3.1) et qui remplit trois rôles:

— gestion de la liste de services de confiance;

— gestion du manifeste;

— établissement des règles de gouvernance opérationnelle du schéma ESEDS

3.3
code lisible par une machine
MRC (machine-readable code)
symbole graphique ou dispositif électronique, ou une combinaison des deux, contenant un ensemble de signes ou de lettres qui peuvent être interprétés par un système d'acquisition

Note 1 à l'article: Les exemples de MRC comprennent, sans s'y limiter, les codes à barres 2D et les étiquettes de radio-identification (RFID).

3.4
point d'entrée de confiance
TEP (trusted entry point)
méthode fournie et/ou certifiée par l'*opérateur de service de confiance* (3.2) prenant en charge la fonction de formatage des réponses (RFF) et ouverte à des systèmes d'identification et d'authentification d'objets (OIAS) supplémentaires capables de résoudre sans ambiguïté tout identifiant unique (UID)

3.5
liste de services de confiance
TSL (trust service list)
liste contenant des informations conformes sur l'*opérateur de service de confiance* (3.2), les prestataires de services de confiance (TSP) et l'autorité de certification (AC) du TSP autorisée à émettre des certificats pour signer les *ensembles de données encodées signés électroniquement* (3.2)

Note 1 à l'article: L'ETSI TS 119 612 définit ce qu'est une TSL conforme.

Note 2 à l'article: Les TSL sont extensibles grâce au langage de balisage extensible (XML) défini par l'*opérateur de service de confiance* (3.2).

3.6
prestataire de services de confiance
TSP (trust service provider)
entités juridiques participant au schéma d'*ensemble de données encodées signé électroniquement (ESEDS)* (3.1) et fournissant plusieurs fonctions ou services de confiance tels que:

— le certificat électronique;

— la signature électronique;

— l'horodatage;

— tout autre service de confiance relatif aux exigences du schéma ESEDS

3.7
responsabilité dos à dos
transfert complet de la responsabilité du prestataire aux sous-traitants

3.8
manifeste
manifeste de cas d'usage
ressource externe contenant des informations au format XML relatives à chaque cas d'utilisation de l'*ensemble de données encodées signé électroniquement* (3.1), son schéma de données, ses politiques de validation et ses extensions facultatives

4 Document de gouvernance du schéma

Le document fondamental de gouvernance du schéma est créé par le TSO.

Il convient qu'il soit accepté par tous les acteurs comme la référence pour le modèle de gouvernance du schéma ESEDS.

Il s'agit d'un schéma dans lequel les acteurs acceptent d'être liés par la gouvernance.

Le document de gouvernance fournit les grands principes qui permettront de décrire les éléments essentiels devant être présents et énumérés dans le contrat d'adhésion pour participer au schéma ESEDS.

L'objectif est de définir les rôles, les responsabilités et les obligations des acteurs du schéma ESEDS.

5 Recommandations s'appliquant aux acteurs du schéma ESEDS

Il convient que le schéma ESEDS, tel que défini par le TSO, comprenne cinq spécifications techniques (TS) qui ont un impact sur les acteurs participants, à savoir:

— TS 1: Mesures techniques spécifiant comment les TSO d'un schéma ESEDS garantissent la confiance dans les TSO du schéma ESEDS;

— TS 2: Mesures techniques spécifiant comment les prestataires de services de confiance (TSP) garantissent la cohérence du niveau de service des TSP du schéma ESEDS;

— TS 3: Mesures techniques spécifiant comment les systèmes de création de l'ESEDS assurent l'interopérabilité;

— TS 4: Mesures techniques spécifiant comment le logiciel de vérification de l'ESEDS garantit l'interopérabilité;

— TS 5: Mesures techniques spécifiant comment l'éditeur du document garantit l'interopérabilité.

6 Mesures organisationnelles

Il convient que le schéma ESEDS, tel que défini par le TSO, comprenne un document dédié qui décrit le processus de gestion du cycle de vie que tous les acteurs et participants suivent.

Le présent document doit être utilisé par tous les acteurs du schéma ESEDS. Il s'agit d'une mesure clé pour garantir l'utilisation harmonieuse du schéma ESEDS.

7 Mesures techniques

Le schéma ESEDS, tel que défini par le TSO, peut suivre d'autres normes ou spécifications qui comprennent des mesures techniques décrivant l'organisation des données pour l'utilisation d'un ESEDS ou de structures de données comparables.

EXEMPLE L'ISO/IEC 20248:2022 ou la norme AFNOR XP Z42-105:2019 pour l'authentification, la vérification et l'acquisition des données véhiculées par un document ou un objet.

L'Annexe A donne un exemple d'ESEDS.