Norme internationale

ISO/IEC 24760-3

Deuxième édition
2025-09

Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre pour la gestion de l'identité —

Partie 3: Mise en œuvre

Information security, cybersecurity and privacy protection — A framework for identity management —

Part 3: Practice

Numéro de référence
ISO/IEC 24760-3:2025(fr)

Document horizontal

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) 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.

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. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'ISO et l'IEC attirent 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 et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient 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 et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

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/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

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

Cette deuxième édition annule et remplace la première édition (ISO/IEC 24760-3:2016), qui a fait l'objet d'une révision technique. Elle incorpore également l'Amendement ISO/IEC 24760-3:2016/Amd 1:2023.

Les principales modifications sont les suivantes:

— mise à jour du titre;

— révision rédactionnelle du document.

Une liste de toutes les parties de la série ISO/IEC 24760 se trouve sur les sites Web de l'ISO et de l'IEC

Le présent document a obtenu le statut de document horizontal conformément aux Directives ISO/IEC, partie 1.

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/members.html et www.iec.ch/national-committees.

Introduction

Les systèmes de traitement des données recueillent généralement une gamme d'informations sur leurs utilisateurs, qu'il s'agisse d'une personne, d'un équipement ou d'un logiciel qui leur est relié, et prennent des décisions sur la base des informations recueillies. Ces décisions fondées sur l'identité peuvent concerner l'accès aux applications ou autres ressources.

Afin de répondre au besoin de mise en œuvre efficace et effective des systèmes qui prennent des décisions basées sur l'identité, la série de normes ISO/IEC 24760 spécifie un cadre pour la délivrance, l'administration et l'utilisation des données qui sert à caractériser les personnes physiques, les organisations ou les composants des technologies de l'information, qui interviennent au nom de personnes physiques ou d'organisations.

Pour de nombreux organismes, la gestion correcte des informations d'identité est essentielle au maintien de la sécurité au sein des processus organisationnels. Pour les individus, une gestion correcte de l'identité est importante pour la protection de la vie privée.

La série ISO/IEC 24760 spécifie les concepts fondamentaux et les structures opérationnelles pour la gestion de l'identité et fournit un cadre sur lequel les systèmes d'information peuvent satisfaire aux obligations métier, contractuelles, réglementaires et légales.

Le présent document spécifie les mises en œuvre de gestion de l'identité. Ces pratiques couvrent l'assurance du contrôle de l'utilisation des informations d'identité, du contrôle de l'accès aux informations d'identité et aux autres ressources basées sur les informations d'identité, et du contrôle des objectifs qu'il convient de mettre en œuvre lors de l'établissement et de la maintenance d'un système de gestion de l'identité.

Le présent document vise à fournir une base pour les mises en œuvre de gestion de l'identité dans d'autres normes internationales relatives au traitement de l'information d'identité, y compris d'autres parties de la série de l'ISO/IEC 24760, de l'ISO/IEC 29100, de l'ISO/IEC 29101, de l'ISO/IEC 29115 et de l'ISO/IEC 29146.

Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre pour la gestion de l'identité —

Partie 3:
Mise en œuvre

1 Domaine d'application

Le présent document:

— fournit des exigences et des recommandations pour la gestion des informations d'identité et pour s'assurer qu'un système de gestion de l'identité est conforme à l'ISO/IEC 24760-1 et à l'ISO/IEC 24760-2;

— est applicable à tout système d'information dans lequel les informations relatives à l'identité sont traitées ou stockées;

— est considéré comme un document horizontal pour les raisons suivantes:

  — il applique des concepts tels que la distinction entre le terme « identité » et le terme « identificateur » concernant la mise en œuvre de systèmes de gestion des informations d'identité et les exigences relatives à la mise en œuvre et au fonctionnement d'un cadre de gestion de l'identité;

  — il apporte une contribution importante à l'évaluation des systèmes de gestion de l'identité en ce qui concerne leur protection de la vie privée et leur capacité à assurer les attributs pertinents d'une identité, et par conséquent il fournit une base et une compréhension commune pour toute autre norme traitant de l'identité, des informations d'identité et de la gestion de l'identité.

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 24760-1:2025, *Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre pour la gestion de l'identité — Partie 1: Concepts fondamentaux et terminologie*

ISO/IEC 24760-2, *Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre pour la gestion de l'identité — Partie 2: Architecture de référence et exigences*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO 24760-1 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
profil d'identité
identité contenant des attributs spécifiés par un modèle d'identité

3.2
modèle d'identité
définition d'un ensemble spécifique d'attributs

Note 1 à l'article: Généralement, les attributs d'un profil sont destinés à soutenir une fin technique ou métier particulière selon les besoins des parties utilisatrices.

3.3
vol d'identité
résultat d'une fausse déclaration d'identité réussie

4 Abréviations

Pour les besoins du présent document, les abréviations suivantes s'appliquent.

TIC Technologies de l'information et de la communication

IIP Fournisseur d'informations d'identité

IIA Autorité gestionnaire des informations d'identité

DCP Données à caractère personnel

RP Partie utilisatrice

5 Atténuation des risques liés à l'identité dans la gestion des informations d'identité

5.1 Vue d'ensemble

Le présent article présente les pratiques destinées à couvrir les risques liés à l'identité lors de l'exploitation d'un système de gestion de l'identité conforme à l'ISO/IEC 24760-1 et à l'ISO/IEC 24760-2.

La Figure 1 montre le champ d'application opérationnel d'un système de gestion de l'identité. Les flèches de la figure identifient les processus qui affectent les informations d'identité enregistrées. Les détails de ces processus sont présentés dans l'ISO/IEC 24760-1:2025, Article 7. Ces processus sont les principaux sujets de préoccupation dans l'évaluation des risques liés à la mise en œuvre d'un système de gestion de l'identité.

NOTE L'ISO/IEC 24760-1:2025, Figure 1 montre que lorsqu'une identité est enregistrée, elle peut se situer à différentes étapes: inconnue, établie, active, suspendue ou archivée. L'authentification d'une entité ne peut généralement réussir que si son identité est active.

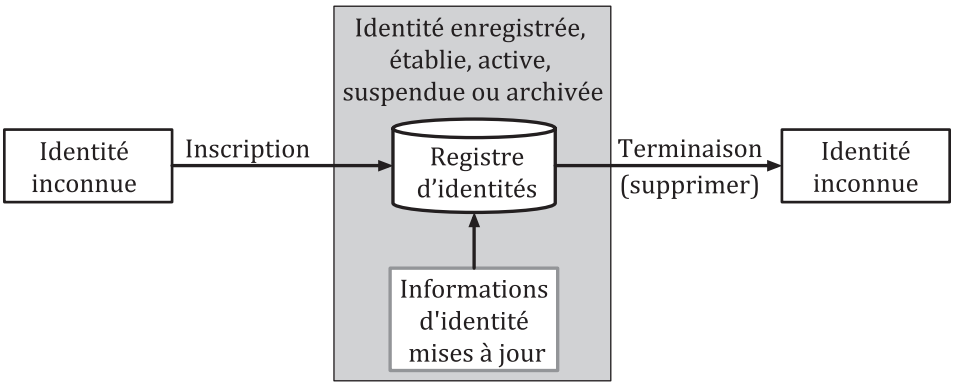

Figure 1 — Champ d'application opérationnel d'un système de gestion de l'identité

5.2 Évaluation des risques

Une fonction d'un système de gestion de l'identité est de gérer l'identité en tant que données; le fonctionnement sécurisé de ce système de gestion des données implique la gestion du risque d'erreurs d'identité, tout en protégeant la confidentialité, l'intégrité et la disponibilité des informations d'identité qui sont stockées, traitées et communiquées. Il convient de réaliser une évaluation des risques afin de déterminer le niveau de risque du système de gestion de l'identité. Il convient que la gestion des risques prenne en compte le cycle de vie de l'identité et des informations d'identité qui évoluent dans le temps et qui peuvent avoir une incidence sur les consommateurs de ces informations. Le résultat fournit des informations, que le système de gestion de l'identité peut utiliser pour déterminer les critères et les processus de gestion du risque nécessaires. Le type d'informations dont un système de gestion de l'identité a besoin comprend le niveau d'assurance de l'identité requis et les exigences en matière de confidentialité, d'intégrité et de disponibilité de ces informations d'identité.

L'ISO/IEC 24760-2 spécifie les outils de gestion des risques sous la forme de politiques, de réglementations, de conception et d'architecture. Dans certains contextes impliquant des consommateurs, il est essentiel de protéger les données à caractère personnel et de donner aux mandants le contrôle de l'utilisation de leurs données à caractère personnel. L'ISO/IEC 29100, l'ISO/IEC 29101, l'ISO/IEC 29134 et l'ISO/IEC 29151 spécifient des exigences et fournissent des recommandations pour la protection de la vie privée.

Les informations d'identité gérées par un système de gestion de l'identité peuvent également être gérées par référence à des fournisseurs d'informations d'identité d'un autre domaine. Par exemple, la vérification de l'identité peut être effectuée par un fournisseur de services, qui opère dans un domaine différent de celui du système de gestion de l'identité.

Lorsque des informations d'identité sont collectées et stockées, les mesures de gestion des risques doivent être mises en œuvre par le service de gestion de l'identité. Ces mesures atténuent les risques identifiés par une appréciation du risque effectuée dans le domaine d'application par la partie utilisatrice. Les niveaux d'assurance concernant les informations d'identité et les services d'accès doivent être déterminés et spécifiés par la partie utilisatrice en fonction des niveaux de risque évalués.

5.3 Assurance en matière d'informations d'identité

5.3.1 Généralités

La confiance dans les informations d'identité fournies par un système de gestion de l'identité découle de processus qui garantissent la validité des informations depuis leur collecte jusqu'à leur stockage ultérieur et leur maintenance par le système. L'assurance est généralement quantifiée en termes de niveaux d'assurance, les niveaux les plus élevés correspondant à une plus grande assurance. Le niveau d'assurance atteint dépend de la qualité des informations d'identité et de la rigueur des processus de validation de l'identité. Les niveaux d'assurance sont décrits dans l'ISO/IEC 29115.

5.3.2 Vérification de l'identité

La vérification de l'identité, c'est-à-dire la validation des informations d'identité pour l'inscription d'une entité dans un domaine, doit satisfaire à un niveau d'assurance défini. Le niveau d'assurance de la vérification d'identité atteignable dépend du type et des caractéristiques des informations et, dans certains cas, de la portée de ces informations, par exemple le nombre de fournisseurs indépendants d'informations d'identité utilisés comme sources des informations.

Un niveau accru d'assurance dans la vérification de l'identité peut être obtenu:

— par la vérification de justificatifs d'identité supplémentaires émanant de multiples sources; et

— par le recours à une partie externe de confiance qui connaît l'entité pour valider les informations d'identité déclarées.

NOTE 1 L'ISO/IEC TS 29003 fournit les exigences applicables à la vérification de l'identité.

NOTE 2 L'ISO/IEC 29115 spécifie comment atteindre différents niveaux d'assurance.

5.3.3 Justificatifs d'identité

Un système de gestion de l'identité peut émettre plusieurs types de justificatifs d'identité qui diffèrent en termes de niveau d'assurance des informations d'identité représentées par le justificatif d'identité.

Il convient qu'un système de gestion de l'identité qui émet des justificatifs d'identité avec un haut niveau d'assurance soutenu par un mécanisme cryptographique fournisse un service permettant aux parties utilisatrices de soutenir activement le processus de validation cryptographique.

Un émetteur de justificatif d'identité sous forme physique doit mettre en œuvre un système de gestion de l'identité pour traiter l'identité du justificatif d'identité conformément à l'ISO/IEC 24760-1 et l'ISO/IEC 24760-2.

5.3.4 Profil d'identité

Un système de gestion de l'identité peut utiliser un ou plusieurs profils d'identité pour recueillir, structurer ou présenter les informations d'identité.

NOTE Bien qu'un profil puisse contenir des informations d'identité, il n'est pas destiné à l'identification. Sa finalité est de fournir des informations d'identité sur une entité aux processus du système qui ont besoin de ces informations pour leurs processus.

Une entité peut avoir plusieurs profils d'identité, chacun contenant un ensemble différent d'attributs pour l'entité. Par exemple, une préférence linguistique peut être présente dans un profil destiné à une interface d'accès et ne pas l'être dans un profil destiné à des intérêts en matière de lecture.

Un modèle d'identité peut être établi en tant que Norme internationale ou sectorielle. L'utilisation d'un modèle d'identité normalisé pour enregistrer les attributs d'identité faciliterait l'utilisation des profils d'identité dans différents domaines.

Un profil d'identité peut être utilisé dans la gestion de l'accès afin de déterminer les attributs d'identité requis pour être autorisé à assumer un rôle ou à obtenir un privilège d'accès à des informations. Un profil d'identité peut être utilisé comme un sous-ensemble préconfiguré d'informations d'identité à présenter lors des interactions avec un service.

Un attribut d'un profil d'identité peut être associé à un niveau d'assurance. L'utilisation d'un profil d'identité avec des niveaux d'assurance associés dans le but de présenter des informations d'identité doit impliquer que chaque information a été validée au minimum à son niveau d'assurance associé. Un profil d'identité spécifiant les exigences d'accès aux services ou aux ressources peut être associé à un identificateur d'entité supplémentaire spécifique qui peut indiquer les activités liées aux privilèges spécifiques.

6 Informations d'identité et identificateurs

6.1 Vue d'ensemble

Il convient que les organismes comprennent les problèmes de sécurité de l'information pour leur activité et fournissent un soutien à la gestion pour répondre aux besoins opérationnels, y compris les exigences supplémentaires.

En ce qui concerne la gestion de l'identité, il convient que les organisations comprennent leurs responsabilités et s'assurent que des mesures de sécurité adéquates sont mis en œuvre afin d'atténuer les risques et les conséquences d'une fuite, de la corruption et de la perte de disponibilité des informations d'identité lors de la collecte, du stockage, de l'utilisation, de la transmission et de l'élimination des informations d'identité. Il convient que les organisations spécifient des objectifs de sécurité et des mesures de sécurité pour s'assurer que les exigences en matière de sécurité des informations sont satisfaites.

6.2 Politique d'accès aux informations d'identité

Il convient que les informations d'identité relatives à une entité soient gérées afin de s'assurer que:

— les informations d'identité demeurent exactes et à jour au fil du temps;

— seules les entités autorisées ont accès aux informations d'identité et sont responsables de toutes les utilisations et modifications des informations d'identité, ce qui garantit la traçabilité de tout traitement d'informations d'identité par toute entité, qu'il s'agisse d'une personne, d'un processus ou d'un système;

— l'organisation remplit ses obligations en matière de réglementation et d'accords contractuels;

— les mandants sont protégés contre le risque de vol lié à l'identité et autre crime lié à l'identité.

NOTE En règle générale, une politique de sécurité de l'information souligne la nécessité de gérer les informations d'identité de façon sécurisée. La préservation et la protection des informations d'identité de toute entité sont également requises lors des transactions avec des tiers, tel que généralement documenté dans les procédures opérationnelles.

6.3 Identifiants

6.3.1 Généralités

Un identificateur permet de distinguer sans ambiguïté une entité d'une autre entité dans un domaine d'applicabilité. Une entité peut avoir plusieurs identificateurs différents dans le même domaine. Cela peut faciliter la représentation de l'entité dans certaines situations, par exemple en masquant l'identité de l'entité lors de la fourniture d'informations d'identité de l'entité à utiliser dans certains processus ou dans certains systèmes. Un identificateur créé dans un domaine peut être réutilisé intentionnellement dans un autre domaine, à condition que l'identificateur réutilisé continue à assurer l'unicité de l'identité dans l'autre domaine.

6.3.2 Catégorisation de l'identificateur par le type d'entité auquel l'identificateur est lié

6.3.2.1 Identificateurs de personne

Un identificateur de personne peut comprendre un nom complet, une date de naissance, un lieu de naissance, ou divers pseudonymes, tels qu'un numéro attribué par une autorité comme référence, par exemple un numéro de passeport, un numéro d'identité nationale ou un numéro de carte d'identité.

L'utilisation de pseudonymes en tant qu'identificateurs est fréquente pour les identificateurs de personnes (voir 6.3.3.2).

NOTE Un pseudonyme peut améliorer la protection de la vie privée des personnes dans un échange d'authentification d'identité avec une partie utilisatrice, car un pseudonyme peut révéler moins de données à caractère personnel que si un nom réel était utilisé comme identificateur.

6.3.2.2 Identificateur attribué à une entité autre qu'une personne

Les entités non humaines, par exemple les dispositifs ou autres objets d'information, peuvent voir leurs activités identifiées et enregistrées comme pour les personnes.

Les identificateurs de dispositifs permettent de distinguer les dispositifs dans le domaine dans lequel ils opèrent.

EXEMPLE 1 L'IMEI (International Mobile Equipment Identity) est un identificateur du téléphone portable dans le domaine des services de téléphonie mobile.

EXEMPLE 2 Le numéro de carte SIM GSM (ICCID) est un identificateur unique de dispositif dans le domaine d'un service de téléphonie mobile. Une carte SIM contient également d'autres identificateurs, y compris celui de l'utilisateur qui a enregistré la carte SIM.

Il peut également être nécessaire de distinguer les identificateurs d'objet d'information dans leur domaine. L'un de leurs attributs qui compromet une combinaison de leurs attributs est généralement utilisé(e) comme identificateur.

EXEMPLE 3 Le nom de processus, le nom de session, le nom de chemin, les noms de ressource uniforme (URN), l'identificateur de ressource uniforme (URI) sont des exemples d'identificateurs d'objets d'information.

EXEMPLE 4 L'URI est un exemple d'identificateur pour un emplacement, mais l'objet se trouvant à cet emplacement peut changer à tout moment.

6.3.3 Catégorisation de l'identificateur par la nature de la liaison

6.3.3.1 Identificateur vérinyme

Un identificateur vérinyme est un identificateur, persistant dans son domaine d'applicabilité, qui peut être utilisé au sein du domaine et entre domaines, et qui permet à une partie utilisatrice d'obtenir des informations d'identité supplémentaires pour l'entité associée à l'identificateur. Les identificateurs vérinymes couramment rencontrés comprennent l'adresse de messagerie électronique, le numéro de téléphone portable, le numéro de passeport, le numéro de permis de conduire, le numéro de sécurité sociale et la paire nom-date de naissance.

Un identificateur vérinyme peut permettre la corrélation d'informations d'identité pour des entités connues dans différents domaines. Bien qu'il soit tout à fait acceptable de corréler les identités si la personne le souhaite, une corrélation inattendue, par exemple un profilage, a un impact négatif sur la vie privée. De par la nature de l'identificateur vérinyme, si une fuite d'information se produit, cela permet aux adversaires d'effectuer une telle corrélation et de créer des menaces, par exemple de générer toute information liée à la vie privée que le mandant n'avait pas l'intention de divulguer.

6.3.3.2 Identificateur pseudonyme

Un identificateur pseudonyme est un identificateur, persistant dans son domaine, qui ne divulgue pas d'informations d'identité supplémentaires. Tant qu'aucune autre information d'identification n'est pas disponible dans le domaine, il n'est pas possible de corréler les identités d'un domaine différent à partir d'un identificateur pseudonyme. Un identificateur pseudonyme peut être utilisé pour empêcher une corrélation indésirable des informations d'identité des entités entre les domaines.

NOTE La simple utilisation d'identificateurs pseudonymes ne signifie pas que les données d'identité sont pseudonymes. D'autres attributs combinés à un moment donné ou à plusieurs moments peuvent suffire pour déduire des identificateurs vérinymes.

6.3.3.3 Identificateur éphémère

Un identificateur éphémère est un identificateur qui est utilisé uniquement pour une courte durée, et uniquement au sein d'un domaine unique. Il peut changer pour plusieurs utilisations d'un même service ou d'une même ressource.

NOTE 1 S'il est utilisé correctement, un identificateur éphémère rendra très difficile la corrélation de deux visites par une entité.

NOTE 2 Un identificateur éphémère est souvent utilisé dans le contexte du contrôle d'accès basé sur des attributs où l'accès à une ressource est accordé si l'entité dispose d'un attribut particulier. Par exemple, si l'accès aux ressources est accordé pour une personne, car elle est membre d'un groupe donné, l'identité serait composée d'un identificateur éphémère et d'un identificateur de groupe. Ces identificateurs serviraient aux fins du contrôle d'accès tout en minimisant les données divulguées ou la possibilité d'établissement d'un lien entre plusieurs accès, tout en permettant de distinguer chaque entité.