NORME INTERNATIONALE

ISO/IEC 24760-1

Deuxième édition
2019-05

Sécurité IT et confidentialité — Cadre pour la gestion de l'identité —

Partie 1: Terminologie et concepts

IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts

Numéro de référence
ISO/IEC 24760-1:2019(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) 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 document. 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 et l'IEC ne sauraient être tenues pour responsables 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) ou dans la liste des déclarations de brevets reçues par l'IEC (voir https://patents.iec.c).

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 le lien suivant: www.iso.org/iso/fr/avant-propos.html.

Le présent document a été élaboré par le comité technique 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 24760-1:2011), qui a fait l'objet d'une révision technique. Les principales modifications par rapport à l'édition précédente sont les suivantes:

— de nouveaux termes ont été ajoutés à l'Article 3;

— certaines définitions ont été simplifiées et corrigées;

— certains termes ont été supprimés tandis que d'autres ont été remplacés;

— les textes d'introduction du paragraphe 5.1 ont été reformulés;

— de nouveaux paragraphes 5.4 et 8.5 ont été créés.

Une liste de toutes les parties de la série de normes ISO/IEC 24760 peut être consultée sur le site web de l'ISO.

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 systèmes de traitement des données collectent généralement un éventail d'informations relatives à leurs utilisateurs, qu'il s'agisse d'une personne, d'un matériel ou d'un logiciel qui se sont connectés à ces systèmes, et prennent des décisions sur la base des informations recueillies. Ces décisions basées sur l'identité peuvent concerner l'accès aux applications ou à d'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 nombreuses organisations, la gestion adéquate des informations d'identité est essentielle au maintien de la sécurité des processus organisationnels. Pour les personnes physiques, une gestion adéquate de l'identité est importante pour la protection de la vie privée.

La série de normes ISO/IEC 24760 spécifie les concepts fondamentaux et les structures opérationnelles de la gestion de l'identité dans le but de mettre en œuvre la gestion du système d'information de sorte que les systèmes d'information puissent satisfaire aux obligations contractuelles, règlementaires, légales et métier.

L'objectif du présent document est de spécifier la terminologie et les concepts relatifs à la gestion de l'identité, afin de promouvoir une compréhension commune dans le domaine de la gestion de l'identité.

Sécurité IT et confidentialité — Cadre pour la gestion de l'identité —

Partie 1: Terminologie et concepts

1 Domaine d'application

Le présent document définit les termes relatifs à la gestion de l'identité, et spécifie les concepts fondamentaux de l'identité et de la gestion de l'identité ainsi que leurs relations.

Il s'applique à tout système d'information qui traite des informations d'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 24760-2:2015, *Technologies de l'information — Techniques de sécurité — 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 définitions 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 Termes généraux

3.1.1
entité
élément pertinent aux fins de fonctionnement d'un *domaine* (3.2.3) et qui possède une existence manifestement distincte

Note 1 à l'article: Une entité peut avoir une matérialisation physique ou logique.

EXEMPLE Une personne, une organisation, un dispositif, un groupe d'éléments de cette nature, un abonné humain à un service de télécommunications, une carte SIM, un passeport, une carte d'interface réseau, une application logicielle, un service ou un site Web.

3.1.2
identité
identité partielle
ensemble d'*attributs* (3.1.3) associés à une *entité* (3.1.1)

Note 1 à l'article: Une entité peut avoir plusieurs identités.

Note 2 à l'article: Plusieurs entités peuvent avoir la même identité.

Note 3 à l'article: La Recommandation UIT-T X1252[13] spécifie l'utilisation distinctive d'une *identité*. Dans le présent document, le terme *identificateur* sous-entend cet aspect.

3.1.3
attribut
caractéristique ou propriété d'une *entité* (3.1.1)

EXEMPLE Un type d'entité, une adresse, un numéro de téléphone, un privilège, une adresse MAC, un nom de domaine sont des attributs possibles.

3.1.4
identificateur
attribut ou ensemble d'*attributs* (3.1.3) qui caractérisent de façon unique une *identité* (3.1.2) dans un *domaine* (3.2.3)

Note 1 à l'article: Un identificateur peut être un attribut spécialement créé avec une valeur attribuée de façon à être unique à l'intérieur du domaine.

EXEMPLE Un nom de club avec un numéro d'adhésion au club, un numéro de carte d'assurance santé associé au nom de la compagnie d'assurance, une adresse de messagerie électronique ou un identificateur unique universel (UUID) peuvent tous être utilisés comme identificateurs. Sur des listes électorales, l'association des attributs *nom*, *adresse* et *date de naissance* est suffisante pour identifier de façon sûre un électeur.

3.1.5
domaine d'origine
domaine (3.2.3) où une valeur d'*attribut* (3.1.3) a été créée ou a été (ré)affectée

Note 1 à l'article: Le domaine d'origine peut être fourni en tant que métadonnée pour un attribut.

Note 2 à l'article: Le domaine d'origine spécifie généralement la signification et le format de la valeur d'attribut. Cette spécification peut être basée sur des normes internationales.

Note 3 à l'article: Un attribut peut contenir une valeur explicite qui fait référence au domaine d'origine, par exemple un code pays ISO pour un numéro de passeport comme référence au pays de délivrance qui est le domaine d'origine des informations d'identité contenues dans le passeport.

Note 4 à l'article: Sur le plan opérationnel, un domaine d'origine peut être disponible en tant que source autorisée pour un attribut (parfois appelée «autorité d'attribut»). Une source autorisée peut être exploitée en dehors du domaine d'origine effectif. Plusieurs sources autorisées peuvent exister pour le même domaine d'origine.

EXEMPLE Le domaine d'origine d'un numéro d'adhésion à un club est le club spécifique qui a attribué le numéro.

3.1.6
identificateur de référence
RI
identificateur (3.1.4) d'un *domaine* (3.2.3) qui est destiné à rester le même pendant la durée au cours de laquelle une *entité* (3.1.1) est connue dans le domaine et qui, une fois que l'entité cesse d'être connue dans ce domaine, n'est pas associé à une autre entité pendant une période spécifiée dans une police

Note 1 à l'article: Un identificateur de référence persiste au moins pendant l'existence de l'entité dans un domaine et peut exister plus longtemps que l'entité, par exemple à des fins d'archivage.

Note 2 à l'article: Un identificateur de référence pour une entité peut changer pendant la durée de vie de l'entité, suite à quoi l'ancien identificateur de référence ne s'applique plus pour cette entité.

EXEMPLE Un numéro de permis de conduire qui reste le même pendant toute la vie d'une personne physique est un identificateur persistant, qui fait référence à des informations d'identité supplémentaires et qui constitue un identificateur de référence. Une adresse IP n'est pas un identificateur de référence car elle peut être attribuée à d'autres entités.

3.1.7
mandant
sujet
entité (3.1.1) dont les informations d'identité sont stockées et gérées par un *système de gestion de l'identité* (3.4.8)

Note 1 à l'article: En général, dans un contexte de protection de la vie privée ou lorsqu'un mandant est perçu comme disposant d'une capacité d'agir, le terme «mandant» fait référence à une personne.

[SOURCE: ISO/IEC 24760-2:2015, 3.4, modifiée — Le terme «se rapporte» a été clarifié et la Note 1 à l'article a été reformulée.]

3.2 Identification

3.2.1
identification
processus de reconnaissance du caractère distinct d'une *entité* (3.1.1) par rapport à d'autres entités dans un *domaine* particulier (3.2.3)

Note 1 à l'article: Le processus d'identification applique une vérification aux attributs déclarés ou observés.

Note 2 à l'article: L'identification fait généralement partie des interactions entre une entité et les services d'un domaine et d'accès aux ressources. L'identification peut se produire plusieurs fois, même si l'entité est connue dans le domaine.

3.2.2
vérification
processus visant à établir que des *informations d'identité* (3.2.4) associées à une *entité* (3.1.1) particulière sont correctes

Note 1 à l'article: La vérification implique généralement de déterminer quels attributs sont nécessaires pour reconnaître une entité dans un domaine, de vérifier que ces attributs requis sont présents, que leur syntaxe est correcte, et qu'ils existent pendant une période de validité définie et se rapportent à l'entité.

3.2.3
domaine
domaine d'applicabilité
contexte
environnement dans lequel une *entité* (3.1.1) peut utiliser un ensemble d'*attributs* (3.1.3) à des fins d'*identification* (3.2.1) et à d'autres fins

Note 1 à l'article: En général, le domaine d'une identité est bien défini par rapport à l'ensemble particulier d'attributs.

Note 2 à l'article: La Recommandation UIT-T X1252[13] utilise le terme «contexte»; le présent document préfère le terme «domaine».

EXEMPLE Un système IT déployé par une organisation et qui permet aux utilisateurs de se connecter constitue le domaine pour le nom de connexion de l'utilisateur.

3.2.4
informations d'identité
ensemble de valeurs d'*attributs* (3.1.3) facultativement accompagné de toute métadonnée associée à l'intérieur d'une *identité* (3.1.2)

Note 1 à l'article: Dans un système de technologies de l'information et de la communication, une identité se présente sous la forme d'informations d'identité.

3.3 Authentification des informations d'identité

3.3.1
authentification
processus formalisé de *vérification* (3.2.2) qui, en cas de succès, se traduit par une *identité authentifiée* (3.3.2) pour une *entité* (3.1.1)

Note 1 à l'article: Le processus d'authentification implique le contrôle, par un vérificateur, d'un ou de plusieurs attributs d'identité fournis par une entité, afin d'en déterminer la validité avec le niveau de garantie requis.

Note 2 à l'article: L'authentification implique généralement l'utilisation d'une politique spécifiant le niveau de garantie requis pour le résultat d'une procédure réussie.

3.3.2
identité authentifiée
informations d'identité (3.2.4) pour une *entité* (3.1.1) créées afin d'enregistrer le résultat de l'*authentification* (3.3.1)

Note 1 à l'article: Une identité authentifiée contient généralement des informations obtenues lors du processus d'authentification, par exemple: le niveau d'assurance atteint.

Note 2 à l'article: L'existence d'une identité authentifiée dans un domaine particulier indique qu'une identité a été reconnue dans ce domaine.

Note 3 à l'article: Une identité authentifiée possède généralement une durée de vie limitée par une politique d'authentification.

3.3.3
autorité gestionnaire des informations d'identité
IIA
entité (3.1.1) associée à un *domaine* (3.2.3) particulier qui peut produire des déclarations démontrables relatives à la validité et/ou à l'exactitude d'une ou plusieurs valeurs d'attribut dans une *identité* (3.1.2)

Note 1 à l'article: Une autorité gestionnaire des informations d'identité est généralement associée au domaine, par exemple le domaine d'origine, dans lequel les attributs, sur lesquels l'IIA peut formuler des affirmations, ont une importance particulière.

Note 2 à l'article: L'activité d'une autorité gestionnaire des informations d'identité peut être soumise à une politique relative à la protection de la vie privée.

Note 3 à l'article: Une entité peut combiner les fonctions de fournisseur d'informations d'identité et d'autorité gestionnaire des informations d'identité.

3.3.4
fournisseur d'informations d'identité
fournisseur d'identités
IIP
entité (3.1.1) qui met à disposition des *informations d'identité* (3.2.4)

Note 1 à l'article: Les opérations types effectuées par un fournisseur d'informations d'identité sont la création et le maintien à jour d'informations d'identité pour les entités connues dans un domaine donné. Un fournisseur d'informations d'identité et une autorité gestionnaire des informations d'identité peuvent être la même entité.

3.3.5
justificatif d'identité
représentation d'une *identité* (3.1.2) destinée à être utilisée dans le cadre d'une *authentification* (3.3.1)

Note 1 à l'article: Tel que décrit au paragraphe 5.4, les matérialisations habituelles d'un justificatif d'identité sont très variées. Afin de tenir compte de ce large éventail, la définition adoptée dans le présent document est très générique.

Note 2 à l'article: Un justificatif d'identité est généralement produit afin de faciliter l'authentification de *données* des informations d'identité se rapportant à l'identité qu'il représente. L'authentification des données est généralement utilisée dans l'autorisation.

Note 3 à l'article: Les informations d'identité représentées par un justificatif d'identité peuvent, par exemple, être imprimées sur un support lisible par l'homme, ou être stockées dans un jeton physique. Généralement, ces informations peuvent être présentées de façon à renforcer leur validité perçue.

Note 4 à l'article: Un justificatif d'identité peut être un nom d'utilisateur, un nom d'utilisateur avec un mot de passe, un numéro d'identification personnel, une carte à puce, un jeton, une empreinte digitale, un passeport, etc.

3.3.6
vérificateur
entité (3.1.1) qui effectue une *vérification* (3.2.2)

Note 1 à l'article: Un vérificateur peut être le même que, ou agir pour le compte de, l'entité qui contrôle l'identification des entités pour un domaine particulier.

3.3.7
partie utilisatrice
RP
entité (3.1.1) qui se fonde sur la *vérification* (3.2.2) des *informations d'identité* (3.2.4) pour une entité particulière

Note 1 à l'article: Une partie utilisatrice est exposée au risque lié à des informations d'identité incorrectes. Généralement, une relation de confiance la lie à une ou plusieurs autorités gestionnaires des informations d'identité.

3.3.8
affirmation d'identité
déclaration d'une *autorité gestionnaire des informations d'identité* (3.3.3) utilisée par une *partie utilisatrice* (3.3.7) à des fins d'*authentification* (3.3.1)

Note 1 à l'article: Une affirmation d'identité peut être la preuve cryptographique d'une authentification réussie, créée avec des algorithmes et des clés convenues entre les parties, par exemple dans une fédération d'identité.

3.4 Gestion de l'identité

3.4.1
gestion de l'identité
IDM
processus et politiques impliqués dans la gestion du cycle de vie et de la valeur, du type et des métadonnées facultatives d'*attributs* (3.1.3) d'*identités* (3.1.2) connues dans un *domaine* particulier (3.2.3)

Note 1 à l'article: En général, la gestion de l'identité est impliquée dans les interactions entre les parties où des *informations d'identité* (3.2.4) sont traitées.

Note 2 à l'article: Les processus et politiques en matière de gestion de l'identité soutiennent les fonctions d'une *autorité gestionnaire des informations d'identité* (3.3.3) le cas échéant, particulièrement pour gérer l'interaction entre une entité pour laquelle une identité est gérée et l'autorité gestionnaire des informations d'identité.

3.4.2
vérification de l'identité
authentification initiale de l'entité
vérification (3.2.2) fondée sur une *preuve d'identité* (3.4.4) destinée à atteindre un niveau d'assurance spécifique

Note 1 à l'article: La vérification de l'identité est généralement réalisée dans le cadre de l'inscription. Une preuve d'identité peut également être nécessaire lors de la maintenance des informations d'identité enregistrées, par exemple la récupération d'un compte utilisateur.

Note 2 à l'article: En général, la vérification de l'identité implique une vérification des informations d'identité fournies et peut inclure des contrôles de l'unicité, éventuellement fondés sur des techniques biométriques.