Norme internationale

ISO/IEC 24760-2

Deuxième édition
2025-09

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

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

Part 2: Reference architecture and requirements

Numéro de référence
ISO/IEC 24760-2:2025(fr)

Document horizontal

DOCUMENT PROTÉGÉ PAR COPYRIGHT

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 24760-2:2015), qui fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— à l'Article 3, les définitions des termes de l'ISO/IEC 24760-1 ont été supprimées;

— pour traiter le concept émergent de l'identité mobile, le terme "IMS privé du mandant" (PPI) a été ajouté aux Articles 3, 4 et décrit en 5.4.2, 5.4.3 et 5.4.6;

— une partie du contenu de l'Article 5 a été déplacée vers les Articles 6 et 7;

— l'ancienne Annexe A a été supprimée et les annexes existantes ont été réétiquetées.

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 aux adresses www.iso.org/fr/members.html et www.iec.ch/national-committees.

Introduction

Les systèmes de traitement des données collectent généralement un éventail d'informations relatives à leurs utilisateurs, ce qui peut inclure des personnes physiques, des matériels ou des logiciels qui sont connectés à l'équipement. Sur la base des informations recueillies sur l'identité de l'utilisateur, ces systèmes de traitement des données prennent des décisions qui peuvent influer sur la manière dont les utilisateurs accèdent aux ressources informatiques.

Pour répondre à la nécessité de mettre en œuvre de manière efficace et efficiente des systèmes qui prennent des décisions basées sur l'identité, le présent document spécifie un cadre pour l'émission, l'administration et l'utilisation des données. Ce cadre sert à caractériser les individus, les organismes ou les composants de technologie de l'information qui agissent pour le compte d'individus ou d'organismes.

Pour de nombreuses organisations, la gestion adéquate des informations d'identité est essentielle pour le maintien de la sécurité 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 définit une architecture de référence pour la gestion de l'identité, y compris les relations. Ces éléments architecturaux sont décrits par rapport aux scénarios de déploiement de la gestion de l'identité ou leurs modèles. Le présent document spécifie les exigences relatives à la conception et à la mise en œuvre d'un système de gestion de l'identité afin qu'il puisse répondre aux objectifs des parties prenantes impliquées dans le déploiement et l'exploitation de la gestion de l'identité.

Le présent document vise à fournir une base pour la mise en œuvre d'autres normes internationales relatives au traitement de l'information d'identité, telles que l'ISO/IEC 29100, l'ISO/IEC 29101, l'ISO/IEC 29115 et l'ISO/IEC 29146.

Le présent document n'est pas une norme de système de management (MSS).

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

1 Domaine d'application

Le présent document:

— fournit des lignes directrices pour la mise en œuvre de systèmes pour la gestion des informations d'identité;

— spécifie les exigences relatives à la mise en œuvre et à l'exploitation d'un cadre pour la gestion de l'identité;

— 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, *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 29115, *Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO IEC 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
conception documentée
description faisant autorité des aspects structurels, fonctionnels et opérationnels du système

Note 1 à l'article: Une conception documentée est la documentation créée afin de servir de document d'orientation pour la mise en œuvre d'un système de technologies de l'information et de la communication (ICT).

Note 2 à l'article: Une conception documentée inclut généralement la description d'une architecture concrète du système ICT.

3.2
autorité gestionnaire d'identité
entité responsable de la définition et de l'application des politiques opérationnelles pour un système de gestion de l'identité

Note 1 à l'article: Une autorité gestionnaire d'identité commande généralement la conception, la mise en œuvre et le déploiement d'un système de gestion de l'identité.

EXEMPLE La direction générale d'une entreprise qui déploie un système de gestion de l'identité afin de soutenir ses services.

3.3
invalidation
processus exécuté dans un système de gestion de l'identité lorsqu'un attribut donné n'est plus valide pour une entité donnée afin de marquer l'attribut comme étant invalide pour une utilisation future

Note 1 à l'article: L'invalidation des attributs peut faire partie de la mise à jour de la valeur de l'attribut, par exemple, avec un changement d'adresse.

Note 2 à l'article: L'invalidation se produit généralement pour un attribut qui est identifié comme n'étant plus valide avant la fin de la période de validité qui lui avait été précédemment associée.

Note 3 à l'article: Le terme de "révocation" est couramment utilisé pour l'invalidation d'attributs qui sont des justificatifs d'identité.

Note 4 à l'article: L'invalidation se produit généralement immédiatement après avoir déterminé qu'un attribut n'est plus valable pour une entité donnée.

3.4
organisme réglementaire
organisme reconnu formellement, chargé et habilité par la loi, la réglementation ou un accord à superviser l'exploitation de systèmes de gestion de l'identité

3.5
partie prenante
rôle, position, personne, organisme ou catégories de rôle, de position, de personne ou d'organisme, ayant un intérêt, un droit, une part ou une revendication dans une entité d'intérêt

[SOURCE: ISO/IEC IEEE 42010:2022, 3.17, modifié – l'exemple a été supprimé.]

3.6
système de gestion de l'identité privée du mandant
PPI
système de gestion de l'identité contenant des informations d'identité pour un seul mandant, exploité par ce mandant ou sous son contrôle exclusif

Note 1 à l'article: La formulation "identité mobile" a été utilisée pour, entre autres concepts, faire référence à un système de gestion de l'identité privée du mandant, par exemple tel qu'il est mis en œuvre sur un téléphone mobile ou sous la forme d'un jeton de traitement dédié.

4 Symboles et abréviations

TIC technologie de l'information et de la communication

IMS système de gestion de l'identité

DCP données à caractère personnel

PPI système de gestion de l'identité privée du mandant

UML unified modeling language (langage de modélisation unifié)

5 Architecture de référence

5.1 Généralités

Le présent article décrit les éléments architecturaux pour la gestion de l'identité et les relations entre ces éléments.

Il convient que la conception documentée de l'architecture de gestion de l'identité soit basée sur l'ISO/IEC/IEEE 42010 et réponde aux principales préoccupations de ce système, qui peut être l'un ou les deux des éléments suivants:

a) la gestion des informations d'identité pour les membres d'un organisme (Article 6);

b) la gestion des informations d'identité pour les entités en dehors d'un organisme (Article 7).

NOTE L'architecture de référence et la description de l'architecture spécifiées dans le présent document sont basées sur l'ISO/IEC/IEEE 42010.

Il convient que la conception documentée pour l'architecture d'un système de gestion de l'identité spécifie le système dans son contexte de déploiement sur la base des parties prenantes et des acteurs définis dans le présent document. Les acteurs issus de l'entreprise sont des parties prenantes. Certaines parties prenantes n'interagissent pas avec le système. La conception documentée doit couvrir les exigences des parties prenantes, qu'elles soient des acteurs ou non. La conception documentée doit décrire les acteurs de façon exhaustive.

Il convient qu'une conception documentée pour la gestion de l'identité utilise un langage applicable pour décrire l'architecture de référence; il convient que les composants et les fonctions de cette architecture soient étiquetés selon les termes définis dans la série de normes ISO/IEC 24760.

Le présent article donne une vue d'ensemble des composants qui peuvent être présents dans une ou plusieurs vues architecturales qui peuvent être spécifiées dans une conception documentée, y compris:

— parties prenantes (5.3),

— acteurs (5.4), et

— processus et services (5.5).

Deux points de vue communs pour la gestion de l'identité sont présentés en 5.6.

5.2 Scénarios de déploiement

Un système de gestion de l'identité peut être déployé selon différents scénarios. Un scénario de déploiement a une incidence sur la gouvernance du système de gestion de l'identité. Le scénario de déploiement détermine les relations de confiance qui existent entre les parties impliquées dans l'exploitation et la gouvernance du système de gestion de l'identité.

Un scénario de déploiement peut être choisi lors de l'extension d'un système de gestion de l'identité existant. Un modèle de déploiement d'extension peut être différent du modèle de déploiement d'origine ou d'entreprise.

Les différents scénarios de déploiement qui peuvent être utilisés pour mettre en œuvre un système de gestion de l'identité sont les suivants:

— le scénario d'entreprise (6.3);

— le scénario fédéré (7.3.1);

— le scénario de service (7.3.2);

— le scénario fédéré tel qu'il est appliqué en tant que service (7.3.3).

5.3 Parties prenantes

5.3.1 Généralités

La conception documentée peut reconnaître les parties prenantes directes et indirectes suivantes:

— mandant;

— autorité gestionnaire d'identité;

— autorité gestionnaire des informations d'identité;

— partie utilisatrice;

— organisme réglementaire;

— auditeur;

— évaluateur;

— fournisseur de services en nuage; et

— représentant ou défenseur des consommateurs/citoyens.

Chaque partie prenante assume une fonction différente dans le système de gestion de l'identité. Ces fonctions impliquent des responsabilités et obligations spécifiques.

NOTE 1 L'objectif du déploiement d'un système de gestion de l'identité et l'environnement réglementaire de ce déploiement indiquent l'implication des parties prenantes.

Les parties prenantes d'un système particulier de gestion de l'identité peuvent être associées à différents organismes commerciaux ou publics avec leurs intérêts dans le système façonné par cette affiliation. Comme les informations relatives au système disponibles pour différentes parties prenantes peuvent être différentes, il convient que les interactions entre les parties prenantes soient basées sur des relations de confiance explicitement établies.

La conception documentée doit spécifier les représentations concrètes de ses parties prenantes et acteurs, tels que définis en 5.3 et 5.4, respectivement. La conception documentée peut ajouter des parties prenantes ou des acteurs supplémentaires. Elle peut spécifier les parties prenantes et acteurs identifiés en 5.3 et 5.4 avec de multiples représentations distinctes.

Les parties prenantes spécifiées dans le présent document peuvent également être des acteurs. Les parties prenantes autres que les acteurs sont un organisme de réglementation et un représentant ou un défenseur des consommateurs/citoyens.

Les préoccupations des parties prenantes d'un système de gestion de l'identité sont décrites en 5.3.2 et 5.3.7 et il convient qu'elles soient prises en compte dans la conception documentée, la mise en œuvre et l'exploitation du système.

NOTE 2 Les préoccupations exprimées pour chaque type de partie prenante sont prises en compte avec des références lors de l'élaboration des Articles 6 et 7. Les mêmes références peuvent également être utilisées pour documenter une architecture de référence.

5.3.2 Mandant

Les préoccupations d'un mandant d'un système de gestion de l'identité incluent:

— l'exactitude des informations d'identité collectées, traitées et stockées (peut être citée comme “exactitude des données”);

— la minimisation des informations d'identité collectées, traitées et stockées par le système de gestion de l'identité (peut être citée comme “minimisation des données”);

— la minimisation de l'utilisation des informations d'identité par le système de gestion de l'identité dans son domaine d'applicabilité (peut être citée comme “minimisation du partage d'information”);

— la capacité des différentes parties utilisatrices à corréler les informations d'identité pour un seul mandant (peut être citée comme “corrélation du mandant”);

— la capacité d'une partie utilisatrice à établir un lien positif entre le mandant et les informations d'identité enregistrées reçues et les informations d'identité qu'elle a déjà stockées, par exemple un compte utilisateur (peut être citée comme “authentification correcte”);

— les erreurs d'identification, y compris l'identification de faux négatifs et de faux positifs, ainsi que la détection et le traitement des erreurs (peut être citée comme “identification correcte”);

— la connaissance et le consentement au partage des informations d'identité avec des tiers (peut être citée “informations et consentement”);

— être correctement représenté par des informations d'identité qui sont capturées, traitées ou stockées (peut être citée comme “informations représentatives”);

— l'exactitude des opérations dans la fourniture des services et l'accès aux ressources mises à disposition sur la base des attributs présentés dans une situation spécifique (peut être citée comme “bon fonctionnement”);

— la collecte, le traitement et le stockage des informations d'identité n'ont lieu qu'avec son consentement éclairé (peut être cité comme “consentement au traitement”);

— le traitement équitable dans ses interactions avec le système (peut être cité comme “équitable”); et

— une interface utilisateur compréhensible, efficace et appropriée (peut être citée comme “compréhensible”).

NOTE Une préoccupation d'un mandant concernant la manière dont un service tiers utilise des informations d'identité obtenues à partir du système de gestion de l'identité n'est pas une préoccupation relative au système de gestion de l'identité lui-même. Par conséquent, une telle préoccupation n'est pas traitée explicitement dans la conception documentée.

5.3.3 Autorité gestionnaire d'identité

Les préoccupations de l'autorité gestionnaire d'identité d'un système de gestion de l'identité incluent:

— définition des objectifs de gestion de l'identité pour le(s) domaine(s) couvert(s) par le système de gestion de l'identité (peuvent être cités comme “objectifs définis”);

— spécification des politiques destinées à maintenir à jour les objectifs de gestion de l'identité pour le(s) domaine(s) couvert(s) par le système de gestion de l'identité (peuvent être citées comme “politiques spécifiées”);

— réalisation des objectifs métier du système de gestion de l'identité en ce qui concerne les mandants et les utilisateurs des informations d'identité (peuvent être cités comme “répondre aux objectifs de l'utilisateur”);

— réalisation des objectifs opérationnels des relations avec d'autres services de gestion de l'identité (peuvent être citées comme “objectifs de rencontre avec des tiers”);

— exactitude des informations d'identité fournies par chaque mandant en ce qui concerne ce mandant et un niveau de garantie spécifique (peuvent être citées comme “informations correctes”);

— conformité à la réglementation (peut être citée comme “conformité”).

5.3.4 Autorité gestionnaire des informations d'identité

Les préoccupations d'une autorité gestionnaire des informations d'identité d'un système de gestion de l'identité incluent:

— l'exhaustivité, l'exactitude et la fraîcheur des informations d'identité (peut être citée comme “qualité des données”);

— la satisfaction des exigences des parties utilisatrices (peut être citée comme “répondre aux besoins des parties utilisatrices”);

— l'efficacité des méthodes cryptographiques pour faire valoir les informations d'identité (peut être citée comme “affirmation appropriée”);

— l'efficacité des méthodes cryptographiques permettant de dé-identifier les informations d'identité (peut être citée comme “dé-identification effective”);

— conformité à la réglementation (peut être citée comme “conformité”) et;

— le respect des obligations métier vis-à-vis des mandants (peut être cités comme “atteindre les objectifs des mandants”).

5.3.5 Partie utilisatrice

Les préoccupations d'une partie utilisatrice d'un système de gestion de l'identité incluent:

— confidentialité, disponibilité et intégrité et applicabilité à un mandant des informations d'identité (peuvent être citées comme “informations d'identité requises”);

— fourniture d'informations d'identité exactes concernant les mandants pertinents au niveau d'assurance requis (peut être citée comme “qualité des informations”);

— interfaces efficaces, documentées et sécurisées (peut être citées comme “interfaces utilisables”);

— conformité à la réglementation applicable à ses opérations (peut être citée comme “conformité”);

— mécanisme et des procédures d'audit efficaces (peut être cité comme “audit”).

5.3.6 Organisme réglementaire

En tant qu'organisation externe indépendante, les préoccupations d'un organisme réglementaire d'un système de gestion de l'identité incluent:

— la documentation adéquate des politiques d'exploitation (peuvent être citées comme “politiques documentées”);

— l'exactitude du fonctionnement, particulièrement dans l'application des politiques opérationnelles (peut être citée comme “bon fonctionnement”);

— la responsabilité et l'audit adéquats des opérations du système (peut être citée “responsabilité”);

— la conformité de la politique et des pratiques opérationnelles aux exigences légales et réglementaires (peut être citée comme “conformité”);

— un rapport efficace sur les opérations du système, y compris l'efficacité des mesures de sécurité, les incidents et les mesures prises pour surmonter les incidents (peut être cité comme “rapport efficace”); et

— une réponse efficace aux incidents qui violent, ou sont susceptibles de violer la protection de la vie privée (peut être citée comme “réactivité aux incidents”).

NOTE En effet, les auditeurs, en tant qu'acteurs d'un système de gestion de l'identité (voir 5.4.9), en inspectant les opérations d'un système de gestion de l'identité (voir 5.5), peuvent représenter les intérêts des organismes réglementaires.

5.3.7 Représentant ou défenseur des consommateurs/citoyens

Les défenseurs des consommateurs/citoyens sont des personnes ou des groupes issus de la société civile qui tentent de protéger les consommateurs et les citoyens contre la surveillance et qui militent pour l'amélioration des réglementations relatives à la vie privée.

Les représentants des consommateurs/citoyens sont des personnes nommées par un mandant ou sélectionnées par des organisations de consommateurs pour représenter un consommateur ou un citoyen dans ses droits en matière de vie privée.

Les principales préoccupations des représentants et des défenseurs des consommateurs/citoyens sont les suivantes:

— transparence, notification, conformité et protection contre le langage juridique complexe (peut être cité comme “langage clair”);

— disponibilité des procédures permettant d'exercer les droits du consommateur/citoyen (peuvent être citées comme “procédures accessibles”);

— accès des populations défavorisées aux services (peuvent être cités comme “services accessibles”).

NOTE 1 Les représentants des consommateurs et des citoyens participent à des processus sociétaux reconnus impliquant de multiples parties prenantes, tels que la gouvernance, et établissent les bonnes pratiques et les exigences à respecter par ceux qui fournissent des biens et des services aux consommateurs et aux citoyens.

NOTE 2 Les représentants des consommateurs et des citoyens sont sélectionnés, informés et, si nécessaire, formés afin de garantir qu'ils participent à des discussions raisonnables et raisonnées, basées dans la mesure du possible sur des preuves de bonne qualité.

5.4 Acteurs

5.4.1 Généralités

Un acteur interagit avec un système de gestion de l'identité afin de participer à des opérations de gestion de l'identité. Une entité peut interagir avec le même système de gestion de l'identité sous la forme de multiples acteurs différents. La conception documentée doit définir toutes les interactions de tout acteur pris en charge par le système.

NOTE 1 Les acteurs peuvent être directement liés au domaine qui utilise un IMS ou ils peuvent être des tiers, ce qui peut être un autre IMS.

Il convient que la conception documentée décrive les interactions des acteurs en termes de fonctions auxquelles les interactions se rapportent. Lorsque l'authentification préalable d'un acteur qui interagit avec le système de gestion de l'identité est requise pour que les interactions soient autorisées, la conception documentée doit spécifier la base de l'authentification (par exemple: authentification basée sur l'entité,

basée sur le rôle), la méthode d'authentification et le niveau d'assurance requis pour chaque interaction, tel que défini dans l'ISO/IEC 29115.

NOTE 2 L'une des finalités de la spécification des acteurs dans la conception d'un système de gestion de l'identité est d'être en mesure de décrire toutes les interactions prévues avec le système.

Une conception documentée peut reconnaître les acteurs suivants:

— mandant;

— autorité gestionnaire d'identité;

— autorité d'enregistrement de l'identité;

— partie utilisatrice;

— fournisseur d'informations d'identité;

— autorité gestionnaire des informations d'identité;

— vérificateur;

— auditeur.

La conception documentée doit spécifier le niveau d'assurance requise pour l'identification et l'authentification des entités qui demandent l'accès aux informations d'identité contenues dans son système de gestion de l'identité, conformément à l'ISO/IEC 29115. Le niveau d'assurance peut être différent pour différents types d'informations et selon le type d'accès accordé, c'est-à-dire lecture, écriture, etc. L'autorisation peut être mise en œuvre tel que spécifié dans l'ISO/IEC 29146.

5.4.2 Mandant

Un mandant est un acteur qui fournit des informations d'identification pour établir et valider ses informations d'identité au sein des processus de gestion de l'identification. Le mandant a les responsabilités suivantes:

— fournir des informations d'identité exactes pour l'inscription en tant que nouvelle personne, lorsqu'elle présente une demande d'enregistrement en tant qu'entité dans un domaine d'application;

— une fois inscrit comme utilisateur du système, de demander à être reconnu par le système de gestion de l'identité et d'avoir la permission d'accéder aux services ou à utiliser les ressources disponibles dans le domaine d'applicabilité associé au système de gestion de l'identité;

— faciliter l'observation, en tant que sujet d'observation, pour obtenir des informations d'identité.

NOTE 1 En tant que sujet d'observation, les informations d'identité obtenues sont anonymes, jusqu'à ce que leur relation avec le mandant ait été établie.

Pour un PPI, le mandant met à disposition une plate-forme matérielle appropriée pour le registre d'identités et l'environnement d'exécution pour la mise en œuvre des fonctions IMS. Une plate-forme matérielle PPI peut être fournie par un domaine où le mandant est connu, ou par un tiers. Les exigences relatives à cette plate-forme matérielle et à ses opérations, y compris la délivrance et la fourniture de données, ne relèvent pas du domaine d'application du présent document.

NOTE 2 La plate-forme matérielle peut être un téléphone mobile auquel cas l'IMS peut être une implémentation installée sur le téléphone.

Un mandant peut utiliser un système de gestion de l'identité pour:

— demander à être reconnu à partir des informations du système de gestion de l'identité et à être autorisé à accéder aux services ou à utiliser les ressources disponibles dans le domaine d'applicabilité associé au système de gestion de l'identité; et

— être informé, en tant que personne physique, des informations d'identité appartenant au mandant qui sont conservées dans le système de gestion de l'identité et demander la correction de toute erreur dans les informations d'identité.

NOTE 3 Dans des circonstances définies de manière appropriée, un représentant légalement autorisé peut agir au nom d'un mandant.

5.4.3 Autorité gestionnaire d'identité

Une autorité gestionnaire d'identité est associée à un domaine d'applicabilité avec le devoir et les capacités de définir et d'ajuster les objectifs métier de la gestion d'identité dans ce domaine et d'établir des politiques de gestion pour atteindre ces objectifs.

NOTE 1 Un Directeur des Systèmes d'Information (DSI) dans un organisme qui utilise un IMS agit généralement comme autorité d'enregistrement de l'identité. Dans la pratique, cela peut également être réalisé par une équipe de conformité.

Une autorité gestionnaire d'identité utilise des politiques pour réguler l'utilisation des informations d'identité enregistrées. Les politiques peuvent spécifier les niveaux de service fournis, y compris le niveau d'assurance sur les informations d'identité qui peut être fourni par le système de gestion de l'identité. Les politiques peuvent également spécifier comment obtenir l'autorisation d'accès et de modification des informations d'identité dans des circonstances imprévues.

L'autorité gestionnaire d'identité doit définir les objectifs de gestion de l'identité pour un domaine d'applicabilité desservi par le système de gestion de l'identité fonctionnant sous son autorité. L'autorité gestionnaire d'identité doit spécifier les politiques permettant d'atteindre les objectifs de gestion de l'identité pour un domaine associé.

Les responsabilités d'une autorité gestionnaire d'identité comprennent:

— créer, modifier ou révoquer les politiques opérationnelles;

— garantir la conformité légale et réglementaire des politiques et du fonctionnement du système de gestion de l'identité;

— exiger et approuver la modification des mécanismes destinés à établir un niveau d'assurance requis dans l'authentification des entités pour l'accès aux informations d'identité et aux fonctions de contrôle du système;

— répondre aux incidents;

— approuver les modifications apportées au type d'informations enregistrées dans le registre d'identités;

— lancer des audits réguliers;

— évaluer les rapports d'audit, particulièrement en ce qui concerne l'efficacité des politiques.

Pour un PPI, l'autorité gestionnaire d'identité est partagée entre le mandant et une partie externe qui a fourni la mise en œuvre de l'IMS, par exemple en tant qu'application installable. Après le déploiement de l'application IMS, un mandant peut agir dans une configuration opérationnelle activée par l'intermédiaire d'une interface utilisateur fournie par la partie externe. Après l'installation d'une application IMS, la gestion de l'identité peut être impliquée dans le soutien de la sécurité à l'engagement d'un ou plusieurs fournisseurs d'informations d'identité ou autorités gestionnaires des informations d'identité devant être utilisés par l'IMS.

NOTE 2 Le fournisseur de l'application IMS peut prendre en charge la configuration opérationnelle par le mandant avec un certain nombre de menus à choisir parmi les options et les politiques préconfigurées.

Une autorité gestionnaire d'identité peut établir une relation commerciale avec une autre autorité gestionnaire d'identité afin de partager des informations d'identité et des opérations de gestion d'identité, en particulier l'authentification. Une telle relation d'affaires peut être qualifiée de fédération si elle implique plusieurs parties qui partagent un accord commun. Une relation d'affaires qui implique le partage