NORME INTERNATIONALE

ISO/IEC 24760-2

Première édition
2015-06-01

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité —

Partie 2: Architecture de référence et exigences

Information technology — Security techniques — A framework for identity management —

Part 2: Reference architecture and requirements

Numéro de référence
ISO/IEC 24760-2:2015(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
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. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

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 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).

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 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: Avant-propos — Informations supplémentaires.

Le comité chargé de l'élaboration du présent document est l'ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

L'ISO/IEC 24760 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité*:

— *Partie 1: Terminologie et concepts;*

— *Partie 2: Architecture de référence et exigences.*

La partie suivante est en cours d'élaboration:

— *Partie 3: Mise en œuvre.*

D'autres parties pourraient être publiées par la suite.

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 y sont connectés, 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 présente partie de l'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.

L'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, réglementaires, légales et métier.

La présente partie de l'ISO/IEC 24760 définit une architecture de référence pour un système de gestion de l'identité qui inclut les éléments architecturaux clés et leurs relations. Ces éléments architecturaux sont décrits par rapport aux modèles de déploiement de la gestion de l'identité. La présente partie de l'ISO/IEC 24760 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 ce système.

La présente partie de l'ISO/IEC 24760 est destinée à fournir une base pour la mise en œuvre d'autres Normes internationales relatives au traitement des informations d'identité telles que:

— ISO/IEC 29100, *Technologies de l'information — Techniques de sécurité — Cadre privé*;

— ISO/IEC 29101, *Technologies de l'information — Techniques de sécurité — Architecture de référence pour la protection de la vie privée*;

— ISO/IEC 29115, *Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité;* et

— ISO/IEC 29146, *Technologies de l'information — Techniques de sécurité — Cadre pour gestion d'accès*.

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité —

Partie 2: Architecture de référence et exigences

1 Domaine d'application

La présente partie de l'ISO/IEC 24760:

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

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

La présente partie de l'ISO/IEC 24760 s'applique à tout système d'information dans lequel sont traitées ou stockées des informations relatives à 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 IT et confidentialité — Cadre pour la gestion de l'identité — Partie 1: Terminologie et concepts*

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 définitions de l'ISO/IEC 24760-1 ainsi que les suivants, s'appliquent.

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 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* (3.3)

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
système de gestion de l'identité
mécanisme composé de politiques, procédures, technologies et autres ressources destinées au maintien à jour d'informations d'identité, y compris les métadonnées

Note 1 à l'article: Un système de gestion de l'identité est généralement utilisé pour l'identification ou l'authentification des entités. Il peut être déployé pour soutenir d'autres décisions automatisées basées sur les informations d'identité pour une entité reconnue dans le domaine d'application pour le système de gestion de l'identité.

3.4
mandant
sujet
entité à laquelle se rapportent les informations d'identité d'un *système de gestion de l'identité* (3.3)

Note 1 à l'article: Dans le contexte d'exigences de protection de la vie privée, le terme mandant se rapporte à une personne.

3.5
invalidation
processus exécuté dans un *système de gestion de l'identité* (3.3) 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.

3.6
organisme réglementaire
organisme chargé et habilité par la loi, la réglementation ou un accord à superviser l'exploitation de *systèmes de gestion de l'identité* (3.3)

3.7
partie prenante
personne, équipe, organisme ou catégories de personnes, d'équipes ou d'organismes ayant un intérêt dans un système

[SOURCE: ISO/IEC 42010]

4 Symboles et abréviations

DCP Données à caractère personnel

ICT Technologies de l'information et de la communication (Information and Communication Technology)

IMS Système de gestion de l'identité (Identity management system)

5 Architecture de référence

5.1 Généralités

Le présent article décrit les éléments architecturaux d'un système de gestion de l'identité et leurs relations.

Il convient que la conception documentée pour l'architecture d'un système de gestion de l'identité soit basée sur l'ISO/IEC 42010.

NOTE L'architecture de référence et la description de l'architecture définies dans la présente norme sont basées sur l'ISO/IEC 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 la présente partie de l'ISO/IEC 24760. 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 d'un système de gestion de l'identité conforme à la présente partie de l'ISO/IEC 24760 utilise un langage de description d'architecture approprié et référence les fonctions et les composants de l'architecture conformément aux termes définis dans la présente Norme internationale.

5.2 Éléments architecturaux

5.2.1 Vue d'ensemble

Les éléments de la présente architecture de référence sont:

— parties prenantes (5.3.1);

— acteurs (5.3.2);

— vues (5.3, 5.4);

— modèles (5.3.3, 5.3.4, 5.3.5, 5.4.1, 5.4.3);

— composants (5.4.1);

— processus (5.4.2); et

— flux d'informations et actions (5.4.2).

5.2.2 Points de vue

5.2.2.1 Généralités

La conception documentée d'un système de gestion de l'identité doit inclure une vue contextuelle et une vue fonctionnelle. Elle peut inclure une vue physique. La conception documentée peut contenir d'autres vues, par exemple une vue information.

NOTE L'ensemble minimal de points de vue requis décrit les interactions du système avec son environnement ainsi que les composants et interactions internes du système.

Il convient que la description d'une vue soit ciblée. Il convient que les diagrammes des descriptions des vues soient accompagnés de texte définissant les éléments représentés.

NOTE La description des points de vue dans le présent paragraphe est basée sur la Référence [2].

5.2.2.2 Point de vue contextuel

Définition — Dans la conception documentée, le point de vue contextuel décrit les relations, les dépendances et les interactions entre le système et son environnement (les personnes, les systèmes et les entités externes avec lesquels il interagit).

Préoccupations — Périmètre et responsabilités du système, identité des entités externes et services et données utilisés, nature et caractéristiques des entités externes, identité et responsabilités des interfaces externes, nature et caractéristiques des interfaces externes, autres interdépendances externes, impact du système sur son environnement, et exhaustivité, cohérence et homogénéité globales.

Modèles — Un point de vue contextuel peut contenir un modèle contextuel, des cas d'utilisation et des scénarios d'interactions. Le modèle contextuel est un diagramme informel constitué de cases et de traits qui représente le système en question comme une boîte noire avec des interfaces, des interactions de haut niveau et des dépendances vis-à-vis d'entités externes. Voir 5.3.3.

Points à surveiller — Entités externes manquantes ou incorrectes, dépendances implicites manquantes, descriptions d'interface vagues ou inexactes, niveau de détail inapproprié, dérive du domaine d'application, contexte ou domaine d'application implicite ou supposé, interactions trop compliquées, utilisation excessive de jargon.

5.2.2.3 Point de vue fonctionnel

Définition — Dans la conception documentée, le point de vue fonctionnel décrit les éléments fonctionnels clés avec les responsabilités opérationnelles, les interfaces et les interactions principales.

Préoccupations — Se rapporte aux capacités fonctionnelles, aux interfaces externes, à la structure interne et à la philosophie de la conception fonctionnelle.

Modèles — Un point de vue fonctionnel peut contenir un modèle de composant, un modèle physique ou un modèle d'infrastructure.

Dans la conception documentée, le point de vue fonctionnel doit identifier les normes et les lignes directrices applicables à chacune des fonctions qu'il décrit.

Voir 5.4 pour des recommandations relatives à la spécification d'un point de vue fonctionnel.

5.3 Vue contextuelle

5.3.1 Parties prenantes

5.3.1.1 Généralités

La présente partie de l'ISO/IEC 24760 reconnaît les parties prenantes directes et indirectes suivantes comme étant de première importance:

— mandant;

— autorité gestionnaire d'identité;

— autorité gestionnaire des informations d'identité;

— partie utilisatrice;

— organisme réglementaire;

— auditeur; 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. À l'exception des organismes réglementaires et des représentants des consommateurs, les parties prenantes interagissent avec un système de gestion de l'identité, et sont donc présentes dans l'architecture de référence en tant qu'acteurs (voir 5.3.2).

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

5.3.1.2 Mandant

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

— exactitude des informations d'identité collectées, traitées et stockées;

— protection de la vie privée;

— minimisation des informations d'identité collectées, traitées et stockées par le système de gestion de l'identité;

— minimisation de l'utilisation des informations d'identité par le système de gestion de l'identité dans son domaine d'applicabilité;

— erreurs d'identification, y compris l'identification de faux négatifs et de faux positifs, ainsi que la détection et le traitement des erreurs;

— connaissance de et consentement au partage des informations d'identité avec des tiers;

— être correctement représenté par les informations d'identité capturées, traitées ou stockées;

— 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;

— la collecte, le traitement et le stockage des informations d'identité n'ont lieu qu'avec son consentement éclairé;

— traitement équitable dans ses interactions avec le système; et

— interface utilisateur facile à comprendre, efficace et appropriée.

NOTE Une préoccupation d'un mandant qui concerne un service tiers qui 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 et ne relève donc pas du domaine d'application de la présente norme.

5.3.1.3 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;

— 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;

— réalisation des objectifs métier du système de gestion de l'identité en ce qui concerne les mandants et les utilisateurs des informations d'identité;

— que les informations d'identité fournies par chaque mandant sont exactes et concernent ce mandant avec un niveau d'assurance spécifique; et

— respect de la réglementation.

5.3.1.4 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:

— exactitude des informations d'identité;

— satisfaction des exigences des parties utilisatrices;

— respect de la réglementation; et

— respect des obligations métier vis-à-vis des mandants.

5.3.1.5 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;

— fourniture d'informations d'identité exactes concernant les mandants pertinents au niveau d'assurance requis;

— interfaces efficaces, documentées et sécurisées;

— conformité à la réglementation applicable à ses activités; et

— mécanisme et procédures d'audit efficaces.

5.3.1.6 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;

— l'exactitude du fonctionnement, particulièrement dans l'application des politiques opérationnelles;

— une responsabilité et un audit adéquats des opérations du système;

— la conformité de la politique et des pratiques opérationnelles aux exigences légales et réglementaires;

— 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; et

— une réponse efficace aux incidents qui violent, ou sont susceptibles de violer la protection de la vie privée.

NOTE En effet, les auditeurs, en tant qu'acteurs d'un système de gestion de l'identité (voir 5.3.2.9), en inspectant les opérations d'un système de gestion de l'identité (voir 5.4), peuvent représenter les intérêts des organismes réglementaires.

5.3.1.7 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 défenseurs des consommateurs/citoyens sont:

— transparence, notification, conformité et protection contre le langage juridique complexe; et

— accès des populations défavorisées aux services.

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.

5.3.2 Acteurs

5.3.2.1 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.

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

NOTE 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 nécessaire 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, tel qu'indiqué dans 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.

5.3.2.2 Mandant

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

— en tant qu'entité, lorsqu'il demande à être enregistré dans un domaine d'applicabilité, de fournir des informations d'identité exactes pour son inscription en tant que nouveau mandant;

— en tant qu'utilisateur du système, une fois inscrit, de demander à être reconnu par le système de gestion de l'identité et d'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

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

NOTE 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.

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 le concernant qui sont conservées dans le système de gestion de l'identité et demander la correction de toute erreur dans les informations d'identité.

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

5.3.2.3 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.

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 à fournir, 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; et

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

Une autorité gestionnaire d'identité peut s'associer formellement avec une ou plusieurs autres autorités gestionnaires d'identité en vue de former une «fédération».

NOTE L'objectif est d'étendre le domaine d'applicabilité des mandants aux autres domaines d'applicabilité d'une fédération. Cette extension est obtenue avec un partage strictement contrôlé des informations d'identité.

Au sein d'une fédération, les responsabilités de chaque autorité gestionnaire d'identité comprennent:

— fournir un niveau d'assurance des informations d'identité qui satisfait à l'exigence spécifiée de tout autre membre de la fédération;

— maintenir le contrôle de l'accès aux informations d'identité contenues dans son système de gestion de l'identité;

— vérifier que le niveau d'assurance atteint par tout autre membre de la fédération pour autoriser l'accès aux informations d'identité dans les systèmes fédérés de gestion de l'identité satisfait à ses exigences en matière d'accès à ses propres informations d'identité;

— opérer avec des politiques communes en matière de partage d'informations; et

— spécifier des politiques destinées à maintenir sa confiance dans le niveau d'assurance de l'authentification de l'identité.

NOTE 1 Typiquement, au sein d'une fédération, certaines des politiques de gestion de l'identité, en particulier en ce qui concerne l'autorisation d'accès, feront partie d'un accord entre les autorités gestionnaires d'identité impliquées dans les domaines.

NOTE 2 Des politiques de gestion de l'identité à utiliser dans de multiples domaines d'applicabilité peuvent être établies par des Normes internationales.

NOTE 3 Les modifications de la structure, de l'organisation et de l'étendue d'une fédération de données peuvent être soumises à des contraintes externes telles que des exigences légales ou réglementaires ou l'octroi d'une autorisation par des organismes réglementaires.

NOTE 4 Les membres d'une fédération peuvent convenir de déléguer les responsabilités opérationnelles de l'autorité gestionnaire d'identité à un opérateur commun, désigné comme étant «l'autorité de la fédération».

5.3.2.4 Autorité d'enregistrement de l'identité

Une autorité d'enregistrement de l'identité est un acteur d'un système de gestion de l'identité chargé et en mesure de définir et de faire appliquer des politiques opérationnelles pour la collecte, l'enregistrement et la mise à jour des informations d'identité dans le registre d'identités.

Les politiques d'enregistrement de l'identité doivent identifier les différents types de modifications des informations d'identité et les conditions opérationnelles et de sécurité dans lesquelles ces modifications sont autorisées. Ces politiques doivent spécifier les procédures permettant d'atteindre le niveau d'assurance des informations d'identité recueillies.

Les responsabilités d'une autorité d'enregistrement de l'identité comprennent:

— modifier, créer ou révoquer les politiques opérationnelles;

— approuver les modifications apportées au type d'informations enregistrées dans le référentiel; et

— approuver la modification des informations d'identité enregistrées dans le référentiel.