NORME INTERNATIONALE

ISO/IEC 24760-3

Première édition
2016-08-01

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

Partie 3: Mise en oeuvre

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

Part 3: Practice

Numéro de référence
ISO/IEC 24760-3:2016(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) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/avant-propos.

Le comité chargé de l'élaboration du présent document est l'ISO/IEC JTC 1, *Technologies de l'information*, 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 ;*

— *Partie 3: Mise en œuvre.*

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, 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.

La présente partie de 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 présente les pratiques en matière 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.

La présente partie de l'ISO/IEC 24760 se compose des parties suivantes:

— ISO/IEC 24760-1: Terminologie et concepts ;

— ISO/IEC 24760-2: Architecture de référence et exigences ;

— ISO/IEC 24760-3: Mise en œuvre.

L'ISO/IEC 24760 est destinée à fournir une base pour d'autres Normes internationales liées à la gestion de l'identité, y compris les suivantes:

— ISO/IEC 29100, Cadre privé ;

— ISO/IEC 29101, Architecture de référence pour la protection de la vie privée ;

— ISO/IEC 29115, Cadre d'assurance de l'authentification d'entité ;

— ISO/IEC 29146, Cadre pour gestion d'accès.

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

Partie 3:
Mise en oeuvre

1 Domaine d'application

La présente partie de l'ISO/IEC 24760 fournit 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.

La présente partie de l'ISO/IEC 24760 est applicable à un système de gestion de l'identité dans lequel des identificateurs ou des DCP relatifs à des entités sont acquis, traités, stockés, transférés ou utilisés à des fins d'identification ou d'authentification d'entités et/ou à des fins de prise de décision à l'aide d'attributs d'entités. Les pratiques relatives à la gestion de l'identité peuvent également être traitées dans d'autres normes.

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*

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

[SOURCE: ISO/IEC 24760-2:2015, 3.3, modifié, « système » utilisé à la place de « mécanisme »]

3.2
profil d'identité
identité contenant des attributs spécifiés par un modèle d'identité

3.3
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.

3.4
vol d'identité
résultat d'une fausse déclaration d'identité réussie

3.5
responsable de fédération
acteur d'une fédération responsable de la gestion des problèmes découlant du fonctionnement de la fédération

Note 1 à l'article: Un membre existant de la fédération ou un tiers indépendant peut assumer le rôle de responsable de fédération.

3.6
mandant
entité à laquelle se rapportent les informations d'identité d'un système de gestion de l'identité

[SOURCE: ISO/IEC 24760-2:2015, 3.4]

4 Symboles et abréviations

Pour les besoins du présent document, les symboles et abréviations suivants s'appliquent.

DCP Données à caractère personnel

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

IIA Autorité gestionnaire des informations d'identité (Identity Information Authority)

IIP Fournisseur d'informations d'identité (Identity Information Provider)

RP Partie utilisatrice (Relying Party)

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

5.1 Vue d'ensemble

L'Article 5 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, à l'ISO/IEC 24760-2 et à l'ISO/IEC 29115.

5.2 Appréciation du risque

L'une des fonctions d'un système de gestion de l'identité est de gérer le risque d'erreurs d'identité, ainsi que la confidentialité, l'intégrité et la disponibilité des informations d'identité qu'il stocke, traite et communique. Il est nécessaire de comprendre le niveau de risque, qui dépendra de l'application. Il convient que le propriétaire de l'application réalise une appréciation du risque afin de déterminer le niveau de risque. Le résultat fournira des informations, qui peuvent être utilisées pour déterminer les critères et les processus de gestion du risque nécessaires pour le système de gestion de l'identité. Les informations dont un système de gestion de l'identité a besoin comprennent le niveau d'assurance des informations d'identité requis et les exigences en matière de confidentialité, d'intégrité et de disponibilité de ces informations.

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 (à publier) 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, des mesures de gestion du risque doivent être mises en œuvre par le service de gestion de l'identité afin d'atténuer les risques identifiés par une appréciation du risque effectuée dans le domaine d'application par la partie utilisatrice. Les niveaux d'assurance en ce qui concerne 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 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.

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 organisations comprennent les enjeux en matière de sécurité de l'information pour leur activité et pour la conformité à la législation pertinente et il convient qu'elles fournissent un soutien en matière de gestion pour satisfaire aux besoins métier. 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 Identificateurs

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 type d'entité à laquelle l'identificateur est lié

6.3.2.1 Identificateurs de personnes

Un identificateur de personne peut être, par exemple, 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 non humaine

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.

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

NOTE 2 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'objets d'information dans leurs domaines. L'un de leurs attributs ou une combinaison de leurs attributs est généralement utilisé(e) comme identificateur.

NOTE 3 Exemple: 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.

NOTE 4 Exemple: 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 à partir de la nature du lien

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.

6.3.4 Catégorisation de l'identificateur à partir du regroupement des entités

6.3.4.1 Identificateur individuel

Un identificateur individuel est un identificateur qui est associé à une seule entité dans un domaine d'applicabilité.

6.3.4.2 Identificateurs de groupe

Les entités sont parfois réunies au sein d'une entité de groupe lorsqu'il s'avère nécessaire d'exécuter les activités en groupe. Une identité de groupe distincte représentera l'entité de groupe et les identificateurs de groupe contribueront à identifier sans ambiguïté l'entité de groupe et à enregistrer les activités de l'entité de groupe dans leur domaine. Les identificateurs de groupe répondent au besoin d'une entité humaine d'effectuer des activités en groupe ou au nom d'un groupe ; ils peuvent masquer l'auteur d'une activité au sein d'un groupe. Des techniques supplémentaires peuvent par conséquent être nécessaires pour identifier sans ambiguïté une entité unique comme membre d'une entité de groupe.

6.3.5 Gestion des identificateurs

Lors de la mise à jour d'informations d'identité pour une entité connue, un système de gestion de l'identité peut attribuer un nouvel identificateur à l'identité modifiée ; il peut également supprimer

l'association de l'ancien identificateur avec l'identité. Les informations d'identité modifiées peuvent être communiquées de façon proactive aux sous-systèmes qui s'appuient sur elles.

7 Audit de l'utilisation des informations d'identité

La gestion et le traitement des informations d'identité par des entités autorisées dans un domaine peuvent être soumis à diverses exigences métier légales, réglementaires et sectorielles qui nécessitent un certain niveau de surveillance et de traçabilité.

NOTE Ces exigences peuvent être d'une grande variété, allant des fichiers journaux et autres mesures de protection des données à caractère personnel, au maintien de l'exactitude et de la traçabilité requises des horodatages ; voir l'ISO/IEC 18014.

Il convient qu'une entité qui fournit des services associés à la gestion de l'identité fournisse des mécanismes garantissant l'aptitude à l'audit.

8 Objectifs de sécurité et mesures de sécurité

8.1 Généralités

L'Article 8 résume les objectifs de sécurité et les mesures de sécurité associées à vérifier lors de la mise en place ou de la revue d'un système de gestion de l'identité.

La structure des mesures de sécurité suit la structure présentée dans l'ISO/IEC 27002.

8.2 Composants contextuels pour le contrôle

8.2.1 Établissement d'un système de gestion de l'identité

8.2.1.1 Objectif

Établir un système de gestion afin de lancer et de contrôler la mise en œuvre de la gestion des informations d'identité pour les entités.

8.2.1.2 Définition et documentation du domaine d'applicabilité

Mesure de sécurité

Les parties utilisatrices pour lesquelles une entité, ou un groupe d'entités, est autorisé(e) à appliquer son identité et qui peuvent utiliser l'identité pour l'identification et à d'autres fins doivent être documentées afin d'être clairement comprises, à la fois par les opérateurs et par les entités concernées.

Recommandations de mise en œuvre

Il convient qu'une documentation décrivant les limites du domaine d'un système de gestion de l'identité soit mise à la disposition de toutes les parties intéressées. Il convient que cette documentation spécifie les limites où les informations d'identité peuvent être vérifiées. Il convient que toute extension potentielle à d'autres domaines ou groupes d'entités soit également documentée.

Il convient que la documentation clarifie les contraintes, légales ou autres, ainsi que les responsabilités associées, s'exerçant sur le contrôle des informations d'identité dans un domaine.

Autres informations

Un domaine d'une identité est bien défini par rapport à un ensemble particulier d'attributs définissant des groupes d'entités.