NORME INTERNATIONALE

ISO 21091

Première édition
2013-02-15

Informatique de santé — Services d'annuaires pour les fournisseurs de soins de santé, les sujets de soins et autres entités

Health informatics — Directory services for healthcare providers, subjects of care and other entities

Numéro de référence
ISO 21091:2013(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 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 (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée 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.

L'ISO 21091 a été élaborée par le comité technique ISO/TC 215, *Informatique de santé*.

Cette première édition annule et remplace l'ISO/TS 21091:2005, qui a fait l'objet d'une révision technique.

Introduction

Les services d'annuaire en informatique de santé pour les fournisseurs de soins de santé, les sujets de soins et autres entités sont destinés à prendre en charge les exigences relatives à la communication et à la sécurité des professionnels de la santé dans l'exercice de leurs fonctions cliniques et administratives. Les soins de santé requièrent des exigences relatives au chiffrement des données et aux contrôles d'accès pour la divulgation et la transmission de toutes les informations de santé confidentielles. À l'appui de l'infrastructure de clé publique de soins de santé, les soins de santé mettent à disposition un registre de certificats comprenant les informations commerciales et professionnelles nécessaires pour effectuer les transactions de soins de santé. Ces informations doivent comporter l'identification des rôles individuels au sein du système de santé tels qu'ils ne peuvent être identifiés que par les organisations de santé respectives. En tant que tel, les fonctions d'enregistrement et de gestion doivent être extensibles, et éventuellement distribuées à tous les niveaux de la communauté de soins de santé. Le service d'annuaire doit également prendre en charge ces exigences de santé supplémentaires pour la sécurité.

L'annuaire devient une méthode de plus en plus populaire permettant d'assurer les capacités d'ouverture de session unique pour la prise en charge de l'authentification. Cet objectif a conduit à l'inclusion des attributs d'authentification et d'identification en vue d'authentifier l'identité d'une personne de soins de santé ou d'un acteur du domaine de la santé.

L'annuaire prend également en charge la communication d'attributs supplémentaires qui peuvent être utilisés pour appuyer les décisions d'autorisation. Cet objectif a amené les extensions du schéma d'annuaire à inclure les informations de gestion des employés de l'organisation, les informations de contact spécifiques aux soins de santé, et les identifiants de soins de santé. La présente Norme internationale traite des exigences spécifiques des soins de santé de l'annuaire, et définit, au besoin, des spécifications standard relatives à l'inclusion de ces informations dans l'annuaire de soins de santé.

Outre les mesures techniques de sécurité abordées dans d'autres normes ISO, la communication des données de soins de santé requiert une «chaîne de confiance» fiable et contrôlable. Afin de maintenir cette chaîne de confiance au sein de l'infrastructure de clé publique, les utilisateurs (participants faisant confiance) doivent être en mesure d'obtenir des certificats valables corrects et des informations relatives au statut des certificats par la gestion sécurisée de l'annuaire.

L'annuaire de soins de santé prend en charge les recherches standard client (LDAP), les unités d'interface pour la transformation des messages et les mises en œuvre de l'Architecture axée sur le service (SOA) pour faciliter le service dans tout type d'environnement. Les lignes directrices spécifiques de mise en œuvre, les critères de recherche et la prise en charge ne relèvent pas du domaine d'application de la présente Norme internationale.

Bien que les mesures de sécurité et les spécifications de contrôle d'accès spécifiques ne relèvent pas du domaine d'application de la présente Norme internationale, du fait de la nature sensible des informations relatives à la santé et au respect de la vie privée susceptibles d'être prises en charge par les services de l'annuaire, des contrôles importants doivent être activés aux niveaux de la branche, des classes d'objet et des attributs. Il convient que des processus et des procédures soient en place pour assurer l'intégrité des informations représentées dans l'annuaire de santé et la responsabilité vis-à-vis du contenu de l'annuaire doit être clairement attribuée à travers des politiques et processus. Il est à prévoir la conduite de contrôles d'accès appropriés permettant de gérer ceux qui peuvent lire, écrire ou modifier tous les éléments de l'annuaire de soins de santé. Cela peut être réalisé en affectant des individus au sein de l'annuaire au rôle HCOrganizationalRole et en attribuant des privilèges appropriés (par exemple de lecture, modification, suppression) à ce rôle dans la configuration de gestion de l'annuaire.

Informatique de santé — Services d'annuaires pour les fournisseurs de soins de santé, les sujets de soins et autres entités

1 Domaine d'application

La présente Norme internationale définit les spécifications minimales relatives aux services d'annuaire pour les soins de santé. Elle peut être utilisée pour permettre les communications entre organisations, appareils, serveurs, composants d'applications, systèmes, acteurs techniques et dispositifs.

La présente Norme internationale fournit les informations et services d'annuaire communs nécessaires pour prendre en charge l'échange en toute sécurité des informations de soins de santé sur les réseaux publics lorsque les informations et services d'annuaire sont utilisés à cette fin. Elle traite de l'annuaire de santé d'un point de vue communautaire préalablement aux communications interentreprises, inter-juridiction et internationales en matière de soins de santé. Bien que plusieurs options soient prises en charge par la présente Norme internationale, il ne sera pas nécessaire pour un service donné d'inclure toutes les options.

Outre le support des services de sécurité tels que le contrôle et la confidentialité d'accès, la présente Norme internationale doit spécifier d'autres aspects de la communication, tels que les adresses et les protocoles des entités de communication.

La présente Norme internationale concerne également les services d'annuaires qui ont pour objet de prendre en charge l'identification des professionnels et des organisations de santé ainsi que celle des patients.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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/HL7 27931:2009, *Normes d'échange de données — Version 2.5 normalisée de messagerie HL7 — Un protocole d'application pour l'échange de données électroniques dans les environnements de soins*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1
contrôle d'accès
ensemble des moyens garantissant que seules les entités autorisées peuvent accéder aux ressources d'un système informatique, et seulement d'une manière autorisée

[ISO/CEI 2382-8]

3.2
autorité d'attribut
AA
autorité qui attribue des privilèges par l'émission de certificats d'attribut

[X.509]

3.3
certificat d'attribut
structure de données, portant la signature numérique d'une autorité d'attribut qui lie certaines valeurs d'attribut à des informations d'identification concernant son détenteur

[X.509]

3.4
authentification
processus consistant à identifier de manière fiable les sujets de sécurité en associant en toute sécurité un identifiant et son authentificateur

[ISO 7498-2]

3.5
autorisation
attribution de droits, comprenant la permission d'accès sur la base de droits d'accès

[ISO 7498-2]

3.6
disponibilité
propriété d'être accessible et utilisable sur demande par une entité autorisée

[ISO 7498-2]

3.7
certificat
certificat de clé publique

3.8
distribution de certificat
action consistant à publier les certificats et à les transférer aux sujets de sécurité

3.9
émetteur de certificat
autorité jouissant de la confiance d'un ou de plusieurs participants faisant confiance pour la création et l'attribution de certificats

Note 1 à l'article: L'autorité de certification peut, de manière optionnelle, créer les clés des parties faisant confiance.

[ISO/CEI 9594-8]

3.10
gestion de certificat
procédures relatives aux certificats telles que génération, distribution, archivage et révocation de certificat

3.11
révocation de certificat
action qui consiste à retirer tout lien fiable entre un certificat et son propriétaire (ou propriétaire du sujet de sécurité) parce que le certificat n'est plus fiable, même s'il est en cours de validité

3.12
liste de révocation de certificat
CRL
liste publiée des certificats suspendus et révoqués (portant la signature numérique de la CA)

3.13
vérification de certificat
vérification de l'authenticité d'un *certificat* (3.7)

3.14
autorité de certification
CA
autorité jouissant de la confiance d'un ou de plusieurs participants faisant confiance pour la création et l'attribution de certificats et qui peut, de manière optionnelle, créer les clés des parties faisant confiance

Note 1 à l'article: Adapté de l'ISO/CEI 9594-8.

Note 2 à l'article: Autorité dans l'expression CA n'implique aucune autorisation gouvernementale, mais uniquement une notion de confiance.

Note 3 à l'article: Émetteur de certificat peut être un meilleur terme mais CA est plus largement utilisé.

3.15
confidentialité
propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés

[ISO 7498-2]

3.16
intégrité des données
propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée

[ISO 7498-2]

3.17
signature numérique
données ajoutées à une unité de données ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données, et protégeant contre une contrefaçon, par exemple par le destinataire

[ISO 7498-2]

3.18
identification
réalisation d'essais permettant à un système informatique de reconnaître les entités

[ISO/CEI 2382-8]

3.19
identifiant
informations utilisées pour revendiquer une identité, avant une corroboration potentielle par un authentificateur correspondant

[ENV 13608-1]

3.20
intégrité
propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée

[ISO 7498-2]

3.21
clé
série de symboles commandant les opérations de chiffrement et de déchiffrement

[ISO 7498-2]

3.22
gestion de clés
production, stockage, distribution, suppression, archivage et application de clés conformément à la politique de sécurité

[ISO 7498-2]

3.23
protocole LDAP (lightweight directory access protocol)
protocole d'accès standard pour les annuaires permettant l'accès public ou limité aux certificats et autres informations nécessaires dans un PKI

3.24
identifiant d'objet
OID
identifiant alphanumérique/numérique unique enregistré dans le cadre de la norme d'enregistrement ISO pour référencer un objet ou une classe d'objet spécifique

3.25
respect de la vie privée
garantie de l'absence d'intrusion dans la vie privée ou les affaires d'un individu dans la mesure où cette intrusion résulte de la collecte et de l'utilisation illégales et non fondées de données relatives à cet individu

[ISO/CEI 2382-08]

3.26
clé privée
clé qui est utilisée avec un algorithme asymétrique de cryptographie et dont la possession est limitée (habituellement à une seule entité)

[ISO/CEI 10181-1]

3.27
clé publique
clé qui est utilisée avec un algorithme asymétrique de cryptographie et qui peut être rendue publique

[ISO/CEI 10181-1]

3.28
certificat de clé publique
PKC
certificats de clé publique qui lient une identité et une clé publique

[RFC 3280]

3.29
infrastructure de clé publique
PKI
structure de matériel, logiciel, personnes, processus et politiques qui utilise une technologie de signature numérique pour fournir aux participants faisant confiance une association vérifiable entre le composant public d'une paire de clés asymétriques et un sujet spécifique

3.30
participant faisant confiance
destinataire d'un certificat qui fait confiance aux données contenues dans ce certificat et/ou à la signature numérique vérifiée en utilisant ce certificat pour prendre des décisions

[RFC 3647]

3.31
rôle
ensemble de compétences et/ou de performances qui sont associées à une tâche

3.32
sécurité
combinaison de la disponibilité, de la confidentialité, de l'intégrité et de l'imputabilité

[ENV 13608-1]

3.33
politique de sécurité
plan ou programme d'action adopté pour assurer la sécurité informatique

[ISO/CEI 2382-8]

3.34
service de sécurité
service, fourni par une couche de systèmes ouverts, garantissant une sécurité adéquate des systèmes et du transfert de données

[ISO/CEI 7498]

3.35
sujet de sécurité
entité active, désignant généralement une personne, un processus ou un dispositif, qui est à l'origine de la circulation de l'information entre les objets ou qui change l'état du système

Note 1 à l'article: Techniquement, une paire processus/domaine [TCSEC].

3.36
sujet
entité dont la clé publique est certifiée dans le certificat

3.37
patient
personne programmée pour recevoir, recevant ou ayant reçu des soins de santé

3.38
tierce partie
partie autre que l'expéditeur ou le destinataire des données, nécessaire pour réaliser une fonction de sécurité dans le cadre d'un protocole de communication

3.39
tierce partie de confiance
TTP
tierce partie qui est considérée comme de confiance à des fins d'un protocole de sécurité

[ENV 13608-1]

Note 1 à l'article: Ce terme est utilisé dans de nombreuses normes ISO/CEI et autres documents décrivant essentiellement les services d'une CA. Le concept est toutefois plus étendu et comprend des services comme l'horodatage et éventuellement l'entiercement.

4 Symboles (et abréviations)

CA	Autorité de certification (Certification Authority)
CN	Nom commun (Common Name)
CRL	Liste de révocation de certificat (Certificate Revocation List)
DAP	Protocole d'accès d'annuaire (Directory Access Protocol)
DIT	Arbre des informations de l'annuaire (Directory Information Tree)
DN	Nom distinctif (Distinguished name)
EDI	Échange de données informatisé (Electronic Data Interchange)
LDAP	Protocole LDAP (Lightweight Directory Access Protocol)
MPI	Indice principal de patient (Master Patient Index)
PDA	Assistant numérique personnel (Personal Data Assistant)
PIDS	Service d'identification de personne (Person Identification Service)
PKC	Certificat de clé publique (Public Key Certificate)
PKI	Infrastructure de clé publique (Public Key Infrastructure)
RA	Autorité d'enregistrement (Registration Authority)
RDN	Nom distinctif relatif (Relative distinguished name)
TTP	Tierce partie de confiance (Trusted Third Party)

5 Contexte des soins de santé

5.1 Généralités

Pour tenir compte des questions spécifiques aux soins de santé, les services d'annuaire standards doivent être étendus.

Les attributs définis X.500 ne remplissent pas complètement les exigences pour gérer et distinguer les professionnels de la santé, les patients, les organisations et autres acteurs du domaine de la santé impliqués dans les communications en matière de soins de santé et de décisions de sécurité. L'utilisation accrue des réseaux pour la communication et la gestion des informations de santé rend nécessaire de disposer d'annuaires spécifiques aux soins de santé et du support d'un certain nombre d'informations et de services de sécurité associés. L'utilisation toujours plus croissante des systèmes d'information de santé fondés sur l'internet et l'intranet, nécessite de communiquer les informations de santé par le biais de plusieurs entités et entités non-affiliées, en utilisant des systèmes automatisés et à interface humaine. La gestion et les communications de ce type d'informations de santé distribuées nécessitent une norme pour les communications des données, des annuaires de professionnels de soins de santé, et des informations sur le consommateur.

Les organisations ont de plus en plus confiance dans les infrastructures de technologie de l'information améliorées pour simplifier et améliorer les fonctions de gestion de l'utilisateur grâce à l'utilisation du LDAP et de services similaires pour gérer et avoir accès à un référentiel central de l'utilisateur par le biais de multiples systèmes au sein d'une organisation. Ces activités comprennent les annuaires d'entreprise et institutionnels, la définition des systèmes et services, et la définition des annuaires des partenaires. Indépendamment des modèles d'entreprise, cette application au domaine de santé nécessite un contexte

de schéma amélioré permettant de répondre au besoin de représenter les informations de soins de santé réglementaires, les authentifiants cliniques, les affiliations multiples aux niveaux professionnel et organisationnel des soins de santé, et les membres non affiliés de la communauté des soins de santé, des consommateurs et des partenaires commerciaux de l'organisation.

Il existe également une utilisation accrue d'annuaires pour l'authentification de l'utilisateur. La création d'une source unique pour la gestion de l'utilisateur permet aux organisations de soins de santé d'améliorer l'identification de l'utilisateur, l'authentification, et le retrait de l'identité de l'utilisateur du processus de sortie. La capacité «d'ouverture de session unique» peut favoriser une meilleure sécurité du mot de passe.

Les annuaires peuvent également permettre de communiquer les attributs d'utilisateur pour les décisions d'autorisation au titre de la gestion des infrastructures de sécurité. L'association des attributs de soins de santé, tels que le rôle et les spécialités de soins de santé, permet d'améliorer l'attribution du privilège associé, le retrait du privilège, la gestion du rôle et le contrôle d'accès. Toutefois, bien qu'il s'agisse d'un outil puissant pour améliorer la sécurité, il augmente la complexité des exigences applicables aux annuaires et inter-annuaires.

Un autre service de sécurité de l'annuaire des soins de santé consiste à prendre en charge les efforts de PKI de soins de santé. Les services de cette nature utilisent l'annuaire pour le stockage et l'accès de la clé publique, ainsi que pour le soutien des services PKI tels que le stockage et l'accès à la CRL. La PKI et le soutien du service de sécurité amélioré augmentent la complexité de l'annuaire de soins de santé du fait des exigences applicables aux supports supplémentaires d'objet pour les serveurs, les composants et dispositifs d'application.

La présente Norme internationale peut prendre en charge plusieurs types de mises en œuvre d'annuaire. Il n'y a aucune exigence qu'un service d'annuaire intègre toutes les options. Les options sont fournies pour permettre à un domaine de communication d'établir l'annuaire qui prendra en charge les organisations, les personnes ou dispositifs de soins de santé appropriés. Les annuaires fournisseurs peuvent être mis en œuvre pour prendre en charge les communications d'ordonnancement, les notifications, les communications de fournisseur à fournisseur et plusieurs autres fonctions. Les annuaires fournisseurs peuvent être améliorés pour les mises en œuvre de la vérification d'authentifiant permettant la communication des sanctions et des informations de statut d'authentifiant. Les services d'annuaire peuvent prendre en charge les demandes du public ou des fournisseurs relatives, par exemple, à l'identification d'un spécialiste dans une zone géographique donnée. Les annuaires assurant les communications avec les patients nécessitent des mesures de protection importantes en matière de contrôle d'accès et il convient qu'ils soient, en tant que tel, gérés séparément des annuaires fournisseurs. De tels annuaires peuvent être améliorés pour venir à l'appui des activités de services sociaux. Il ne s'agit là que de certaines possibilités d'application des annuaires de soins de santé. Des cas d'utilisation supplémentaires figurent dans l'Annexe A.

5.2 Personnes de soins de santé

Bien que les Normes X.500 incluent plusieurs classes d'objet pour représenter les personnes comme des individus et des employés, il n'existe pas d'attribut standard au sein de ces classes d'objet pour représenter les informations clés spécifiques aux soins de santé nécessaires pour prendre en charge les communications et services du secteur. La communauté des soins de santé doit représenter, dans l'annuaire, des informations professionnelles telles que les authentifiants, les identifiants de soins de santé, les informations spécifiques aux rôles et les informations de contact spécifiques aux soins de santé. Les informations de contact en matière de soins de santé sont plus complexes que celles des environnements commerciaux types compte tenu de la nature des affiliations multiples abordées en 5.3. Les personnes de soins de santé comprennent:

— les professionnels de soins de santé réglementés;

— les professionnels de soins de santé non réglementés;

— les employés des organisations de soins de santé et des organisations de soutien;

— les patients.

5.3 Affiliations multiples

Les personnes de soins de santé, dans de nombreux environnements, peuvent être affiliées à plusieurs organisations. Ces personnes peuvent exercer différentes fonctions dans chacune des organisations auxquelles elles sont affiliées. Bon nombre de professionnels de soins de santé agissent de façon autonome, mais sont autorisés à exercer des privilèges au sein d'une ou de plusieurs organisations. Dans le même ordre d'idée, les services de soutien peuvent être fournis à plusieurs organisations de soins de santé. Au sein d'une organisation, un individu peut agir en vertu de différents rôles en fonction de paramètre de soins ou d'autres facteurs. Les consommateurs de soins de santé ont généralement recours à des services de nombreux professionnels et organisations de soins de santé. Afin de réduire au minimum les erreurs de précision associées à la double gestion des informations, le schéma de soins de santé doit assurer des liens avec les sources de gestion primaires venant à l'appui des affiliations multiples.

Un autre facteur important est que les membres du personnel de soins de santé sont également des consommateurs de soins de santé, et il convient que les identités professionnelles soient distinctes de l'identité du consommateur de soins de santé. Du point de vue d'une utilisation appropriée, il est important que les membres du personnel de soins de santé et leurs identités professionnelles associées soient séparés de leurs identités personnelles dans la mesure où les objectifs d'utilisation sont différents dans les différents rôles ou contextes.

5.4 Organisations de soins de santé

Bien que la X.500 fournisse des classes d'objet pour les organisations, les attributs existant au sein de ces constructions sont insuffisants pour représenter les informations spécifiques aux soins de santé nécessaires pour prendre en charge les exigences relatives à l'annuaire de soins de santé. Les informations spécifiques aux soins de santé incluent:

— les identifiants de réglementation;

— la classe de service fournie;

— les emplacements de service;

— les informations de contact pour les fonctions de gestion des informations clé.

Les organisations de soins de santé incluent:

— les organisations de soins de santé réglementées (par exemple les hôpitaux, les pharmacies, les cliniques, les unités mobiles, les installations d'infirmerie qualifiées, les unités spécialisées);

— les agents payeurs, les organisations de soutien (par exemple les fournisseurs, les services de transcription, les services de codage, les services de traitement des réclamations);

— les organismes de réglementation/surveillance (c'est-à-dire les associations professionnelles, le contrôle des maladies, la réglementation pharmaceutique, la santé publique).

5.5 Matériel/Logiciel

Bien que la X.500 fournisse des classes d'objet pour les serveurs et les applications, les dispositifs de soins de santé et les logiciels sont soumis à des exigences de réglementation et de validation et, par conséquent, il convient qu'ils comprennent des attributs supplémentaires pour représenter de manière appropriée les exigences relatives à l'annuaire de soins de santé. Les PDA et d'autres dispositifs peuvent également avoir des associations spécifiques avec d'autres entités dans l'annuaire de soins de santé. La représentation du matériel et du logiciel dans l'annuaire est limitée aux paramètres d'identification et de communication de ces derniers, et à leur association avec des individus et des organisations. L'annuaire peut être utilisé pour l'identification des biens, mais il convient de ne pas s'y référer pour la gestion des biens.

5.6 Services de sécurité des soins de santé

Les autorités de certification des soins de santé, les autorités d'attribut et les autorités d'enregistrement doivent être représentées au sein de l'annuaire, et doivent être en mesure de publier des informations pertinentes clé relatives à la gestion. Le soutien à la gestion des rôles de soins de santé dans l'annuaire doit pouvoir représenter les composants spécifiques des soins de santé. Cela inclut la représentation de la fonction d'emploi, des informations de contact spécifiques à l'emploi et des certificats (les certificats professionnels et d'attribut) associés à une personne de soins de santé. Cela n'inclut pas le soutien direct pour la représentation des rôles fonctionnels.

6 Cadre de gestion de la sécurité de l'annuaire

Les soins de santé doivent être pris en charge par un cadre de politiques de gestion de sécurité fortes afin d'assurer l'intégrité des données de communication et de l'infrastructure d'authentification. Les Normes internationales définissent déjà des principes de base pratiques forts de cette nature. Bien que les normes suivantes ne soient pas spécifiques à l'annuaire, il convient de les observer pour la protection des infrastructures de l'annuaire:

— ISO/CEI 27000;

— ISO/CEI 27001;

— ISO/CEI 27005;

— ISO 27799;

— Spécification COBIT (Control Objectives for Information et Related Technologies) produite par le "Information Systems Audit and Control Foundation.

7 Interopérabilité

7.1 Exigences

Les annuaires de soins de santé doivent être en mesure de consulter et/ou d'échanger les informations relatives des annuaires de différents partenaires commerciaux. Les techniques comprennent le chaînage, la réplique, les renvois et la confiance unilatérale ou bilatérale entre les annuaires. Certaines de ces techniques sont sensibles aux manques de cohérence du schéma qui dépendent de l'application ou du service. Les considérations d'ordre hiérarchique suivantes s'appliquent aux modèles d'interopérabilité:

a) doit être en mesure de séparer physiquement la base/communauté des clients de soins de santé en un environnement contrôlé de service élevé;

b) doit être en mesure de fournir une gestion de réplique et d'équilibrage des charges;

c) doit être en mesure de limiter l'arbre de recherche à une zone géographique ou logique spécifique afin de fournir une performance d'accès efficace (c'est-à-dire la règle 80/20);

d) doit être en mesure d'organiser le DIT afin de faciliter la gestion du contrôle d'accès pour protéger les informations sensibles stockées dans l'annuaire (par exemple les certificats des patients ne doivent pas être accessibles au public) par des références de point de branchement;

e) doit être en mesure d'organiser le DIT pour permettre un accès distribué aux juridictions de soins de santé.

7.2 Espace de nom/structure d'arbre (arborescence)

Afin de traiter ces exigences d'une manière cohérente et respecter les juridictions de réglementation de soins de santé existantes, il convient que l'espace de nom et la structure d'arbre de niveau élevé suivants soient disponibles: