SPÉCIFICATION TECHNIQUE

ISO/TS 21298

Première édition
2008-12-01

Informatique de santé — Rôles fonctionnels et structurels

Health informatics — Functional and structural roles

Numéro de référence
ISO/TS 21298:2008(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

Version française parue en 2009

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.

Dans d'autres circonstances, en particulier lorsqu'il existe une demande urgente du marché, un comité technique peut décider de publier d'autres types de documents:

— une Spécification publiquement disponible ISO (ISO/PAS) représente un accord entre les experts dans un groupe de travail ISO et est acceptée pour publication si elle est approuvée par plus de 50 % des membres votants du comité dont relève le groupe de travail;

— une Spécification technique ISO (ISO/TS) représente un accord entre les membres d'un comité technique et est acceptée pour publication si elle est approuvée par 2/3 des membres votants du comité.

Une ISO/PAS ou ISO/TS fait l'objet d'un examen après trois ans afin de décider si elle est confirmée pour trois nouvelles années, révisée pour devenir une Norme internationale, ou annulée. Lorsqu'une ISO/PAS ou ISO/TS a été confirmée, elle fait l'objet d'un nouvel examen après trois ans qui décidera soit de sa transformation en Norme internationale soit de son annulation.

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/TS 21298 a été élaborée par le comité technique ISO/TC 215, *Informatique de santé*.

Introduction

La présente Spécification technique contient une spécification de codage des informations liées aux rôles des professionnels et des consommateurs de santé. Quatre domaines au moins ont été identifiés pour lesquels un modèle de codage des informations relatives aux rôles est nécessaire.

a) **Gestion des privilèges et contrôle d'accès**: le contrôle d'accès en fonction du rôle n'est pas possible sans la mise en place d'un moyen efficace destiné à enregistrer les informations de rôle des acteurs de santé.

b) **Services d'annuaire**: les rôles structurels sont utilement enregistrés au sein d'annuaires des prestataires de santé (voir, par exemple, l'ISO/TS 21091).

c) **Traçabilité**: les rôles fonctionnels sont utilement enregistrés dans une démarche de traçabilité pour des applications de gestion des informations de santé.

d) **Infrastructure de gestion de clés (IGC)**: L'ISO 17090[9][10] (en trois parties) permet le codage des rôles de santé dans des extensions de certificat, mais aucun vocabulaire structuré relatif à ces rôles n'est spécifié. La présente Spécification technique identifie ce vocabulaire codé.

Outre ces applications liées à la sécurité, il existe plusieurs autres applications possibles de la présente Spécification technique, telles que:

e) **Fonction de recherche**: trouver et identifier le bon professionnel pour un service de santé donné.

f) **Administration**: facturer les services de santé.

g) **Messagerie**: router les messages relatifs à la santé au moyen d'un rôle spécifique.

La présente Spécification technique sert de complément à d'autres normes applicables qui décrivent et définissent aussi les rôles pour les besoins du contrôle d'accès. La compatibilité ascendante avec l'ANSI INCITS et l'HL7 RBAC est assurée grâce à une simplification obtenue en combinant la politique et le rôle dans un seul et même élément La présente Spécification technique élargit le modèle en distinguant le rôle et la politique. Cette distinction permet d'instancier de manière plus riche et plus souple les règles de gestion dans de multiples domaines et juridictions.

Informatique de santé — Rôles fonctionnels et structurels

1 Domaine d'application

La présente Spécification technique définit un modèle permettant de décrire les rôles fonctionnels et structurels et le peuple avec une base de rôles pour une utilisation internationale dans les applications de santé. Les rôles sont en général attribués à des entités qui sont des acteurs. Cette spécification mettra l'accent sur le rôle des personnes (par exemple le rôle des professionnels de la santé) ainsi que sur leurs rôles dans le contexte de l'administration de soins (par exemple sujet de soins).

Les rôles peuvent être structurels (par exemple médecin généraliste agréé, transcripteur médical non agréé) ou fonctionnels (par exemple prestataire membre d'une équipe thérapeutique, médecin traitant, etc.). Les rôles structurels sont relativement statiques, souvent valables pendant de nombreuses années. Ils traitent des relations entre les entités exprimées à un niveau de concepts complexes. Les rôles fonctionnels sont liés à la réalisation d'actions et sont très dynamiques. Ils sont généralement exprimés à un niveau détaillé de concepts élémentaires.

Les rôles abordés dans la présente Spécification technique ne se limitent pas à la gestion des privilèges, même si la gestion des privilèges et le contrôle d'accès constituent l'une des applications de la présente Spécification technique. Celle-ci ne traite pas des spécifications liées aux permissions. La présente Spécification technique considère le rôle et la permission comme des éléments distincts. Des détails supplémentaires concernant la relation avec les permissions, la politique et le contrôle d'accès sont fournis dans l'ISO/TS 22600-1.

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 17090-2, *Informatique de santé — Infrastructure de clé publique — Partie 2: Profil de certificat*

ISO/HL7 21731, *Informatique de santé — HL7 version 3 — Modèle d'information de référence — Version 1*

ISO 22600-1, *Informatique de santé — Gestion de privilèges et contrôle d'accès — Partie 1: Vue d'ensemble et gestion des politiques*

Organisation internationale du travail: *Classification internationale type des professions 2008* (CITP-08)

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, définition 08.04.01]

3.2
autorité d'attribut
AA
autorité qui attribue les privilèges en délivrant des certificats d'attribut

NOTE Adapté du document X.509.

3.3
certificat d'attribut
structure de données, signée numériquement par une autorité d'attribut, qui combine les valeurs d'attribut à l'identification de son détenteur

NOTE Adapté du document X.509.

3.4
autorité
entité qui est responsable de l'émission de certificats

NOTE Elles sont classées en deux catégories dans la présente Spécification technique: l'autorité de certification qui émet des certificats de clés publiques et l'autorité d'attribut qui émet des certificats d'attribut.

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

[ISO 7498-2, définition 3.3.10]

3.6
délégation
transfert de privilège d'une entité détenant ce privilège à une autre entité

3.7
chemin de délégation
séquence ordonnée de certificats qui peuvent, conjointement à l'authentification de l'identité d'un déclarant de privilège, être traités pour vérifier l'authenticité d'un privilège de ce déclarant

3.8
entité
tout élément concret ou abstrait, qui présente un intérêt

[ISO/CEI 10746-2, définition 6.1]

NOTE Alors que d'une manière générale le terme entité peut être utilisé pour faire référence à toute chose, son utilisation dans le contexte de la modélisation est réservée aux éléments modélisant l'univers du discours.

3.9
identification
exécution de tests permettant à un système informatique de reconnaître des entités

[ISO/CEI 2382-8, définition 08.04.12 (comme **validation d'identité**)]

3.10
professionnel de santé non agréé
personne employée par un organisme de santé, mais qui n'est pas un professionnel de la santé

[ISO/CEI 17090-1, définition 3.1.5]

EXEMPLES Assistante médicale ou secrétaire qui gère les rendez-vous, ou directeur responsable de la validation de l'assurance maladie des patients.

NOTE Le fait que l'employé ne soit pas agréé par un organisme indépendant de l'employeur dans sa capacité professionnelle ne signifie évidemment pas que l'employé manque de professionnalisme dans sa démarche de prestation de services.

3.11
politique
ensemble d'obligations légales, politiques, organisationnelles, fonctionnelles et techniques pour la communication et la coopération

3.12
accord de politique
accord écrit dans lequel toutes les parties concernées s'engagent à respecter un ensemble spécifié de politiques

3.13
principal
acteur capable d'effectuer des scénarios spécifiques (utilisateur, organisation, système, dispositif, application, composant, objet)

3.14
privilège
capacité attribuée par une autorité à une entité en rapport avec l'attribut de cette entité

NOTE OASIS XACML (Extensible Access Control Markup Language) V2.0 remplace les notions de privilège, permissions, autorisation, avantage et droits par le terme «règle».

3.15
professionnel de santé agréé

personne habilitée par un organisme reconnu au niveau national à effectuer certains services de santé

[ISO/CEI 17090-1, définition 3.1.8]

EXEMPLES Médecins, infirmières diplômées et pharmaciens.

NOTE 1 Les types d'organisme d'enregistrement ou d'accréditation varient selon les pays et selon les professions. Les organismes nationaux reconnus comprennent les agences locales ou régionales, les associations professionnelles indépendantes et d'autres organisations formellement reconnues au niveau national. Ils peuvent être exclusifs ou non dans leur territoire.

NOTE 2 Selon cette définition, un organisme national reconnu n'implique pas un système unique d'enregistrement professionnel piloté au niveau national; toutefois, afin de faciliter les échanges internationaux, il serait préférable qu'il existe à l'échelon national un annuaire d'organismes reconnus d'enregistrement des professionnels de la santé.

3.16
rôle
ensemble de compétences et/ou de performances associées à une tâche

3.17
certificat d'attribution de rôle
certificat contenant l'attribut de rôle, attribuant un ou plusieurs rôles au détenteur du certificat

3.18
certificat de rôle
certificat qui attribue des privilèges à un rôle plutôt que directement à des individus

NOTE Les individus désignés pour ce rôle, grâce à un certificat d'attribut ou à un certificat de clés publiques avec une extension d'attributs d'annuaire contenant cette attribution, se voient indirectement attribuer les privilèges contenus dans le certificat de rôle.

3.19
certificat de spécification de rôle
certificat contenant l'attribution de privilèges à un rôle

4 Abréviations

AA Autorité d'Attribut

XML eXtensible Markup Language (langage de balisage extensible)

OIT Organisation Internationale du Travail

IGC Infrastructure de Gestion de Clés

IGP Infrastructure de Gestion des Privilèges

UML Unified Modelling Language (langage de modélisation unifié)

5 Rôles de modélisation dans un contexte architectural

5.1 Rôles au sein du modèle de composant générique (GCM)

Les composants de système satisfaisant aux exigences fonctionnelles et aux services requis dans un système doivent être gérés dans leur contexte architectural. Par conséquent, l'analyse, la conception et le déploiement des exigences de ces composants doivent être développés et gérés sur la base d'une architecture de référence suivant un processus unifié.

Avec le modèle générique de composant, une telle architecture de référence conforme aux normes essentielles relatives aux systèmes d'information répartis, fondés sur les composants, orientés services et sémantiquement interopérables a été développée au milieu des années 90 (par exemple Références [1], [2], [3]) et utilisée dans le cadre de plusieurs spécifications ISO/TC 215 et CEN/TC 251. Ce modèle spécifie pour tout domaine une architecture fondée sur les composants et orientée services. La présente Spécification technique ne se limite pas aux questions de sécurité et de respect de la vie privée; les rôles fonctionnels et structurels sont également utilisés pour gérer les privilèges et les contrôles d'accès. Dans ce contexte restreint, les rôles fonctionnels et structurels ont été spécifiés et modélisés dans l'ISO/TS 22600-2. La présente Spécification technique étend le domaine d'application, les services et le déploiement des rôles fonctionnels et structurels, mais repose néanmoins sur l'approche architecturale pour les systèmes d'information sémantiquement interopérables eSanté/iSanté (santé individuelle).

Une architecture de système définit les composants systèmes, leurs fonctions et leurs interactions. Une architecture de système est modélisée en trois dimensions:

— les composants permettant de satisfaire aux exigences des domaines spécifiques;

— la décomposition et, après avoir détaillé les concepts sous-jacents, la composition de ces composants d'après les règles/concepts d'agrégation correspondants (par exemple collaboration des composants, workflow, algorithme); les niveaux de granularité sont au moins les concepts métier, les réseaux de relations, les services/fonctions de base et les concepts de base;

— les différentes vues concernant ce composant selon l'ISO 10746-2[8], la vue entreprise (cas métier, cas d'utilisation, exigences), la vue information et la vue traitement qui représentent la logique indépendante de la plate-forme du système/composant, ainsi que la vue ingénierie et la vue technologie qui concernent les aspects de mise en œuvre spécifiques à la plate-forme.

La Figure 1 présente le modèle de composant générique qui fournit l'architecture de référence mentionnée précédemment.

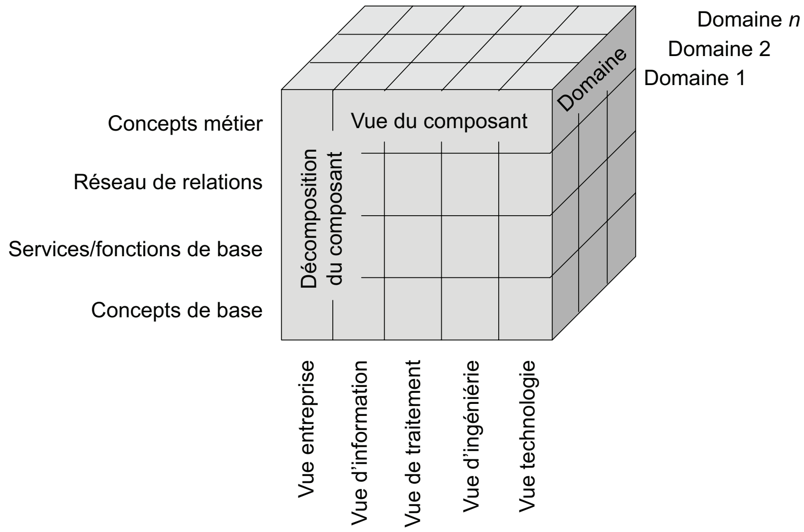

Figure 1 — Modèle de composant générique

Le développement des composants, la représentation de leur concept et leur agrégation sont fondés sur la modélisation des contraintes. Les concepts et les règles peuvent être représentés à l'aide de métalangages tels que UML et ses dérivés ou l'ensemble des langages XML.

5.2 Rôles et aspects relatifs à la politique

Les rôles sont les composants qui reflètent les aspects spécifiques d'un système. Ils doivent être gérés selon toutes les dimensions du GCM. Les politiques sont des propriétés et des fonctions dans une autre dimension du système/composant, et elles doivent être intégrées dans la spécification du composant à travers les contraintes correspondantes. Les classes interdépendantes et les associations peuvent être modélisées de manière simple par les attributs du composant et les contraintes opérationnelles. Cela peut être réalisé par les spécifications d'un simple RBAC qui ignorent la bonne approche par la politique. En associant, par exemple, une classe de rôle fonctionnel à la classe de politique correspondante qui définit le contexte et les autres contraintes d'accès aux objets cibles, le composant résultant peut résumer ces contraintes par une autorisation donnée à ce rôle et exprimée sous la forme d'un attribut d'autorisation.

Pour gérer les relations entre les entités, il est possible de définir les rôles structurels (organisationnels) et fonctionnels. Les rôles peuvent être attribués à toute entité en tant qu'acteur dans une interaction de communication ou de coopération (il s'agit par exemple d'une personne, d'une organisation, d'un système, d'un dispositif, d'une application, d'un composant, etc.). Parce que les entités sont des acteurs engagés dans des «cas d'utilisation», les rôles concernent les acteurs, et par conséquent les actions. Les rôles fonctionnels et structurels sont associés aux politiques et définis par celles-ci.

Une politique peut décrire le cadre juridique, y compris les règles et réglementations, le cadre organisationnel et administratif, les fonctionnalités, les revendications et objectifs, les entités concernées, les accords, les droits, les devoirs et les sanctions définies, ainsi que la solution technologique mise en œuvre pour collecter, enregistrer, traiter et communiquer les données au sein des systèmes d'information.

Les politiques peuvent être spécifiées et mises en oeuvre de différentes manières, notamment

— dans un accord de politique tel que spécifié dans l'ISO/TS 22600-1,

— en tant qu'attribut,

— en tant que politique implicite faisant partie d'un autre composant,

— en tant qu'élément de politique distinct, à combiner avec un autre composant ou à utiliser directement,

— en tant que politique de règles combinée à une autre politique,

— en tant qu'expressions structurées (par exemple en utilisant XACML).

Une politique peut être appliquée comme un ensemble de règles qui décrit la conception et le fonctionnement d'un système. Il convient que les systèmes d'information de santé tels que le Dossier de Santé Informatisé (DSI), par exemple, respectent une politique du patient, une politique d'entreprise, des politiques définies par des lois et réglementations, ainsi qu'une politique par rôle structurel et une politique par rôle fonctionnel. Des détails supplémentaires concernant la spécification de la politique et sa relation avec la gestion des privilèges et le contrôle d'accès sont fournis dans l'ISO/TS 22600-1.

Les rôles peuvent être instanciés grâce à de nombreux mécanismes, notamment les entrées d'annuaire, les variables dans les bases de données et les certificats. Les certificats d'attribution de rôle peuvent être des certificats d'attribut ou des certificats de clés publiques. Les privilèges spécifiques sont attribués à un rôle plutôt qu'à un individu grâce à des certificats de spécification de rôle. L'attribution indirecte permet aux privilèges attribués à un rôle d'être mis à jour, sans affecter les certificats attribuant ces rôles à des individus. Les certificats de spécification de rôle doivent être des certificats d'attribut, et non des certificats de clés publiques. Si les certificats de spécification de rôle ne sont pas utilisés, l'attribution des privilèges à un rôle peut être effectuée grâce à d'autres moyens (elle peut, par exemple, être configurée localement à un vérificateur de privilège).

Toutes les solutions suivantes sont possibles:

a) une autorité d'attribut peut définir un nombre quelconque de rôles;

b) le rôle lui-même et les attributaires d'un rôle peuvent être définis et gérés séparément par différentes autorités d'attribut;

c) un privilège peut être délégué;

d) les rôles peuvent être attribués quelle que soit la durée de validité appropriée.

Des informations supplémentaires concernant l'attribution des différents rôles structurels et fonctionnels sont abordées ci-dessous. Des détails supplémentaires concernant l'expression des rôles grâce à des certificats numériques sont fournis dans l'ISO 17090-2. Des détails supplémentaires concernant la représentation des rôles en tant qu'entrées d'annuaire sont fournis dans l'ISO/TS 21091.

Les rôles fonctionnels et structurels sont associés aux politiques et définis par celles-ci.

Il convient que les systèmes d'information de santé tels que le Dossier de Santé Informatisé (DSI), par exemple, disposent d'une politique du patient, d'une politique d'entreprise, de politiques définies par des lois et réglementations, ainsi que d'une politique par rôle structurel et d'une politique par rôle fonctionnel. Des détails supplémentaires concernant la spécification de la politique et la relation avec la gestion des privilèges et le contrôle d'accès sont fournis dans l'ISO/TS 22600-1.

5.3 Rôles au sein de la gestion des privilèges

Les privilèges peuvent être attribués à un individu grâce à une attribution de rôle ou de manière directe. Un rôle peut être exprimé dans des certificats de clés publiques, des certificats d'attribut ou une entrée d'annuaire, tel que décrit dans l'ISO 17090-2 et l'ISO/TS 21091. Si le certificat d'attribution de rôle est un certificat de clés publiques, l'attribut de rôle est contenu dans l'extension subjectDirectoryAttributes. Dans ce cas, tous les privilèges supplémentaires contenus dans le certificat de clés publiques sont des privilèges qui sont directement attribués à un sujet de certificat, et non des privilèges attribués à un rôle. Si le certificat d'attribution de rôle est un certificat d'attribut, l'attribut de rôle est contenu dans le composant attribut du certificat d'attribut.