
**Informatique de santé — Rôles
fonctionnels et structurels**

Health informatics — Functional and structural roles

Sample Document

get full document from standards.iteh.ai



Numéro de référence
ISO 21298:2017(F)

© ISO 2017

Sample Document

get full document from standards.iteh.ai



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2017, Publié en Suisse

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Sommaire

Page

Avant-propos	iv
Introduction	v
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Abréviations	5
5 Rôles de modélisation dans un contexte architectural	5
5.1 Rôles au sein du modèle de composant générique (GCM)	5
5.2 Rôles et aspects relatifs à la politique	7
5.3 Rôles au sein de la gestion des privilèges	9
5.4 Relations entre la présente norme et les spécifications de gestion des privilèges associées	9
5.5 Rôles structurels	10
5.5.1 Généralités	10
5.5.2 Rôles structurels des professions de santé établis par l'Organisation Internationale du Travail pour la mise en correspondance transjuridictionnelle	10
5.5.3 Spécialités du secteur de la santé	11
5.6 Rôles fonctionnels	12
6 Modélisation formelle des rôles	14
6.1 Rôles au sein du modèle de composant générique (GCM)	14
6.2 Développement du modèle de rôle	14
6.2.1 Relations et transformation	14
6.2.2 Attribution des rôles structurels	15
6.2.3 Spécification de rôle générique	16
6.3 Relations entre rôles structurels et rôles fonctionnels	18
7 Cas d'utilisation des rôles structurels et des rôles fonctionnels dans un contexte interrégional ou international	18
Annexe A (informative) Échantillon de mise en correspondance CITP-08	20
Annexe B (informative) Exemple de profil de certificat pour professionnels de la santé agréés	30
Bibliographie	33

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 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. 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: www.iso.org/iso/fr/avant-propos.html

Cette première édition de l'ISO 21298 annule et remplace l'ISO/TS 21298:2008, qui a fait l'objet d'une révision technique.

Le comité chargé de l'élaboration du présent document est l'ISO/TC 215, *Informatique de santé*.

Introduction

Le présent document contient une spécification de codage des informations liées aux rôles des professionnels et des consommateurs de santé. Cinq domaines au moins ont été identifiés, pour lesquels il est nécessaire de recourir à un modèle de codage des informations relatives aux rôles.

- 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 relatives aux rôles des acteurs de santé.
- b) **Services d'annuaire:** les rôles structurels sont utilement enregistrés au sein d'annuaires de prestataires de santé (voir, par exemple, ISO 21091).
- c) **Traçabilité:** les rôles fonctionnels sont utilement enregistrés au sein de journaux d'audit destinés aux applications de gestion des informations de santé.
- d) **Infrastructure de clé publique (PKI pour Public Key Infrastructure):** la série de normes ISO 17090 permet le codage des rôles de santé dans des extensions de certificat, mais aucun vocabulaire structuré relatif à ces rôles n'est spécifié. Le présent document identifie ce vocabulaire codé.
- e) **But de l'utilisation:** une spécification de rôle détermine dans quel but les informations relatives aux soins de santé peuvent être utilisées. Dans de nombreux cas, le but de l'utilisation est lié à des rôles spécifiques (voir, par exemple, ISO 21091).

Outre ces applications liées à la sécurité, il existe plusieurs autres applications possibles de la présente norme, dont voici quelques exemples ci-après:

- **la prestation de soins cliniques:** trouver et identifier le bon professionnel pour un service de santé donné.
- **la prise en charge des soins:** facturer les services de soins de santé.
- **la gestion de la communication:** router les messages relatifs à la santé au moyen d'un rôle spécifique.
- **la gestion des services de santé et l'assurance qualité:** définir le but de l'utilisation de données spécifiques.

Le présent document sert de complément à d'autres normes applicables qui décrivent et définissent aussi les rôles pour les besoins du contrôle d'accès. Il élargit le modèle en séparant le rôle de la politique. Cette séparation permet d'instancier de manière plus riche et plus souple les règles de gestion dans de multiples domaines et juridictions. La compatibilité ascendante avec l'ANSI INCITS (InterNational Committee for Information Technology Standards) et avec le contrôle d'accès en fonction du rôle (RBAC - Role-Based Access Control) de la HL7 est assurée grâce à une simplification obtenue en combinant la politique et le rôle en un seul et même élément.

Les concepts de rôle définis dans le présent document sont cités en référence et réutilisés dans de nombreuses Normes internationales, par exemple: dans les normes ISO, CEN et HL7 International. En voici quelques exemples: ISO 22600, Référence [7], Référence [8] et Référence [9].

La Commission européenne et le Parlement européen ont émis une Directive relative aux qualifications professionnelles (2005/36/CE), qui définit les spécialités médicales (voir <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:02005L0036-20140117&from=EN>).

L'[Annexe A](#) fournit un échantillon mis en correspondance de la nomenclature CITP-08 alors que l'[Annexe B](#) fournit un échantillon de profil de certificats pour les professionnels de santé agréés.

Sample Document

get full document from standards.iteh.ai

Informatique de santé — Rôles fonctionnels et structurels

1 Domaine d'application

Le présent document définit un modèle qui permet de décrire les rôles fonctionnels et structurels, et l'alimente 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. La présente norme 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 la prestation de soins (par exemple: sujet de soins).

Les rôles peuvent être structurels (par exemple: médecin généraliste agréé, transcripteur médical non agréé, etc.) ou fonctionnels (par exemple: prestataire membre d'une équipe thérapeutique, médecin traitant, prescripteur, 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 objet du présent document ne sont pas traités uniquement sous l'angle de la gestion des privilèges, bien que la gestion des privilèges et le contrôle d'accès soient l'une des applications de ce document. Le présent document ne traite pas des spécifications liées aux permissions. Le présent document considère le rôle et la permission comme des éléments distincts. Des détails supplémentaires concernant les liens avec les permissions, la politique et le contrôle d'accès sont fournis dans l'ISO 22600.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes et définitions

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

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>

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

[SOURCE: ISO/IEC 2382-8:2015, 2126294]

3.2

autorité de certificats d'attribut

AA

autorité qui attribue des privilèges par l'émission de *certificats d'attribut* (3.3)

[SOURCE: ISO/IEC 9594-8:2014, 3.5.2, modifiée]

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* (3.12) concernant son détenteur

[SOURCE: ISO/IEC 9594-8:2014, 3.5.1]

3.4

autorisation

attribution de privilèges comprenant la délivrance de privilèges donnant accès à des données et fonctions

Note 1 à l'article: D'après l'ISO 7498-2: attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

[SOURCE: ISO 22600-1:2014, 3.6]

3.5

autorité de certification

CA

émetteur de certificat; autorité de confiance déclarée compétente par une ou plusieurs parties utilisatrices en matière de création, de délivrance et de gestion de certificats

Note 1 à l'article: L'autorité de certification peut éventuellement créer les clés de parties utilisatrices [ISO 9594-8]. L'autorité de certification émet les certificats en signant les données de certificat à l'aide de sa clé de signature privée.

Note 2 à l'article: La notion d'autorité incluse dans le terme «autorité de certification» n'implique en rien une autorisation gouvernementale, mais véhicule simplement une notion de confiance. Le terme «émetteur de certificat» est peut-être moins ambigu, mais le terme «autorité de certification» est très largement employé.

[SOURCE: ISO 22600-1:2014, 3.8]

3.6

délégation

transmission d'un privilège détenu par une *entité* (3.8) à une autre entité

[SOURCE: ISO 22600-1:2014, 3.10]

3.7

chemin de délégation

séquence ordonnée de certificats qui, lorsqu'ils sont associés à une authentification de l'identité d'un *déclarant de privilège* (3.19), peuvent être traités pour vérifier l'authenticité du privilège que le déclarant revendique

[SOURCE: ISO 22600-2:2014, 3.15]

3.8

entité

tout élément concret ou abstrait, qui présente un intérêt

Note 1 à l'article: 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 de l'univers du discours modélisé.

3.9

rôle fonctionnel

rôle (3.21) lié à un acte

Note 1 à l'article: Les rôles fonctionnels peuvent être attribués en vue d'être remplis pendant cet acte

Note 2 à l'article: Les rôles fonctionnels sont spécifiés dans le présent document.

Note 3 à l'article: Les rôles fonctionnels correspondent à la contribution du modèle d'informations de référence (ou modèle RIM, pour Reference Information Model) de l'ISO/HL7 21731.

Note 4 à l'article: Voir aussi *rôle structurel* (3.26).

3.10

organisation de soins de santé

organisme officiellement enregistré dont l'activité principale est liée à la prestation de services de soins de santé ou à la promotion de la santé

EXEMPLE Hôpitaux, fournisseurs de sites Internet sur la santé et instituts de recherche sur la santé.

Note 1 à l'article: L'organisme est reconnu légalement responsable de ses activités, mais ne doit pas nécessairement être enregistré pour le *rôle* (3.21) spécifique qu'il remplit en matière de santé.

[SOURCE: ISO 17090-1:2013, 3.1.4]

3.11

professionnel de santé

personnel de santé possédant une habilitation de professionnel de santé reconnue dans une juridiction donnée

Note 1 à l'article: L'habilitation de professionnel de santé autorise un professionnel de santé à dispenser des soins de santé, indépendamment d'un *rôle* (3.21) au sein d'une *organisation de soins de santé* (3.10).

EXEMPLE Médecin généraliste, médecin consultant, thérapeute, dentiste, etc.

3.12

identification

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

3.13

personnel de santé non agréé

personne qui est employée par une *organisation de soins de santé* (3.10), mais qui n'est pas un professionnel de santé agréé

EXEMPLE Massothérapeute, musicothérapeute, etc.

[SOURCE: ISO 17090-1:2013, 3.1.5, modifiée]

3.14

employé d'une organisation

personne employée par une *organisation de soins de santé* (3.10) ou un *organisme de soutien* (3.27)

EXEMPLE Transcriptionneurs médicaux, agents liquidateurs de l'assurance maladie et opérateurs de saisie du secteur pharmaceutique.

3.15

politique

ensemble d'obligations légales, politiques, organisationnelles, fonctionnelles et techniques applicable à une communication et à une coopération

[SOURCE: ISO 22600-1:2014, 3.13]

3.16

accord de politique

accord écrit par le biais duquel toutes les parties impliquées s'engagent à respecter un ensemble de politiques préalablement spécifié

[SOURCE: ISO 22600-1:2014, 3.14]

3.17

acteur principal

utilisateurs humains et objets qui doivent fonctionner avec leurs propres droits

[SOURCE: Spécification de l'OMG relative aux services de sécurité (OMG Security Services Specification): 2001]

3.18

privilège

capacité assignée par une autorité à une *entité* (3.8) selon son attribut

Note 1 à l'article: OASIS XACML (Extensible Access Control Markup Language) V2.0 remplace les notions de privilège, permissions, autorisation, avantage et droits par le terme «règle».

[SOURCE: ISO 22600-1:2014, 3.17]

3.19

déclarant de privilège

détenteur de privilège utilisant son *certificat d'attribut* (3.3) ou son certificat de clé publique pour déclarer un *privilège* (3.18)

[SOURCE: ISO 22600-1:2014, 3.27]

3.20

vérificateur de privilège

entité (3.8) vérifiant des certificats par rapport à une politique de privilège

[SOURCE: ISO 22600-2:2014, 3.30]

3.21

rôle

ensemble de compétences et/ou de comportements associés à une tâche

[SOURCE: ISO 22600-2:2014, 3.33]

3.22

certificat d'attribution de rôle

certificat qui contient l'attribut de rôle, assignant un ou plusieurs *rôles* (3.21) au détenteur du certificat

[SOURCE: ISO 22600-2:2014, 3.34]

3.23

certificat de rôle

certificat qui, au lieu d'attribuer des *privilèges* (3.18) directement à des individus, les attribue à un *rôle* (3.21)

Note 1 à l'article: Les individus affectés à un rôle, grâce à un *certificat d'attribut* (3.3) ou à un certificat de clé publique avec une extension d'attributs d'annuaire de sujet contenant cette affectation, reçoivent indirectement les privilèges contenus dans le certificat de rôle.

3.24

certificat de spécification de rôle

certificat qui contient l'attribution de *privilèges* (3.18) à un *rôle* (3.21)

[SOURCE: ISO 22600-2:2014, 3.35]

3.25

prestataire de soins de santé parrainé

prestataire de services de santé non agréé dans sa juridiction d'exercice, mais actif au sein de sa communauté professionnelle et parrainé par une *organisation de soins de santé* (3.10) agréée

EXEMPLE Éducateur spécialisé dans les drogues et l'alcool qui œuvre auprès d'un groupe ethnique particulier, ou coopérant humanitaire dans un pays en développement.

[SOURCE: ISO 17090-1:2013, 3.1.10]

3.26

rôle structurel

rôle (3.21) spécifiant les relations entre les entités en termes de compétences, reflétant souvent les relations organisationnelles ou structurelles (hiérarchies)

Note 1 à l'article: Les rôles structurels sont spécifiés dans le présent document.

Note 2 à l'article: Les rôles structurels correspondent au rôle du modèle d'informations de référence (RIM) de l'ISO/HL7 21731.

Note 3 à l'article: Voir aussi *rôle fonctionnel* (3.9).

3.27

organisme de soutien

organisme officiellement enregistré qui fournit des services à une *organisation de soins de santé* (3.10), mais qui ne propose aucun service de soin de santé

EXEMPLE Organismes de financement des soins de santé, tels que les institutions d'assurance, fournisseurs de produits pharmaceutiques et d'autres biens.

[SOURCE: ISO 17090-1:2013, 3.1.11]

3.28

employé d'un organisme de soutien

personne employée par un *organisme de soutien* (3.27)

4 Abréviations

AA	Autorité d'attribut (Attribute Authority)
CA	Autorité de certification (Certification Authority)
GCM	Modèle de composant générique (Generic Component Model)
HL7	Health Level 7
OIT	Organisation Internationale du Travail
NIST	National Institute for Standards
PKI	Infrastructure de clé publique (Public Key Infrastructure)
PMI	Infrastructure de gestion des privilèges (Privilege Management Infrastructure)
RBAC	Contrôle d'accès en fonction du rôle (Role-Based Access Control)
UML	Langage UML (Unified Modeling Language)
XACML	Langage XACML (eXtensible Access Control Markup Language)
XML	Langage XML (eXtensible Markup Language)

5 Rôles de modélisation dans un contexte architectural

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

Les composants de système qui satisfont 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 de composant générique (GCM), 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: ISO/IEC 9594-8, ISO/IEC 10746-2 et ISO/IEC 2382-8) et utilisée dans le cadre de plusieurs spécifications ISO/TC 215, CEN/TC 251 et HL7. Ce modèle spécifie, pour tout domaine, une architecture fondée sur les composants et orientée services. Même si le présent document va au-delà des questions de sécurité et de respect de la vie privée, les rôles fonctionnels et structurels sont également utilisés pour gérer les privilèges et le contrôle d'accès. Dans ce contexte restreint, des rôles fonctionnels et structurels ont été définis et modélisés dans l'ISO 22600. Le présent document élargit le domaine d'application, les services et le déploiement des rôles fonctionnels et structurels, mais reste fondé sur l'approche architecturale des systèmes d'information sémantiquement interopérables eSanté/iSanté (santé individuelle)[Z][8].

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

- Les composants permettant de satisfaire aux exigences de domaines spécifiques;
- La décomposition et, après avoir détaillé les concepts sous-jacents, la composition de ces composants d'après la règle/les concepts d'agrégation correspondants (par exemple: la collaboration entre composants, le workflow, l'algorithme). Les niveaux de granularité sont, au minimum: 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, la vue entreprise (cas métier, cas d'utilisation, exigences), la vue information et la vue traitement qui représentent la logique indépendante de la plateforme du système/composant, ainsi que la vue ingénierie et la vue technologie qui concernent les aspects de mise en œuvre spécifiques à la plateforme.

La [Figure 1](#) illustre le modèle de composant générique qui fournit l'architecture de référence susmentionnée, en ajoutant un point de vue d'entreprise réel aux points de vue de l'ISO 10746.

