
Analyse et modélisation de contrôles d'accès au système GED

Céline Coma — Nora Cuppens-Bouahia — Frédéric Cuppens

GET/ENST Bretagne
2 rue de la Châtaigneraie, BP 78
35512 Cesson Sévigné Cedex
France

RÉSUMÉ. Le respect de la vie privée et le secret médical sont deux des grands principes fondamentaux du milieu médical. Cependant, de nos jours, les personnes sont de plus en plus mobiles et prennent de plus en plus contact avec divers professionnels de santé, d'où l'existence d'une multiplication des données. Pour éviter les informations redondantes, le milieu médical a recours au format électronique. Afin de garantir le secret médical et le respect de la vie privée du patient, il faut assurer la sécurité de ces données électroniques. D'où la nécessité d'établir une politique de contrôle d'accès aux informations médicales. Dans le cadre de la modélisation de cette politique, nous verrons l'utilité de l'abstraction des règles liées à la politique. Nous traiterons des limites du modèle RBAC pour définir les problèmes contextuels. Enfin, nous étudierons quelques aspects clé d'une modélisation basée sur le modèle de contrôle d'accès OrBAC.

ABSTRACT. The respect of privacy and medical secrecy are some of great fundamental principles of the healthcare domain. However, nowadays, the people are increasingly mobile and contact more and more various healthcare professionals. This leads to a multiplication of data. To avoid redundant information, the medical environment makes use of electronic format. In order to guarantee the medical secrecy and patient privacy, it is necessary to ensure the security of these electronic data. So, we have to specify an access control policy to medical information. Within the framework of the policy modeling, we will see the utility of abstraction of the rules related to the policy. We will treat limits of the model RBAC to define the contextual constraints. Finally, we will study some key aspects of a modelization based on OrBAC.

MOTS-CLÉS : contexte, médical, RBAC, OrBAC, XACML, confidentialité, consentement, contrôle d'accès, GED, législation

KEYWORDS: context, healthcare, RBAC, OrBAC, XACML, confidentiality, consent, access control, GED, legislation

1. Introduction

A l'heure où les échanges d'informations sont de plus en plus nombreux et importants, l'accès aux informations d'ordre médical est de plus en plus complexe. Les gens sont mobiles et certaines opérations médicales se font même à distance [TAD 02], lorsque les dossiers médicaux eux sont plus complexes à faire circuler. En effet, la confidentialité et la disponibilité sont deux notions qui s'opposent dans les échanges d'informations concernant les patients. Afin de résoudre les problèmes de disponibilité, en particulier géographique, les informations du patient sont stockées de façon électronique. Néanmoins, il faut assurer la confidentialité liée à ces informations afin de respecter la vie privée du patient et le secret médical. Nous avons dû prendre en compte tous ces aspects dans le cadre du projet SILLAGE réseau de soins. L'objectif visé est de fournir des moyens permettant aux médecins des structures hospitalières d'une ville telle que Rennes de coopérer et d'améliorer la prise en charge de leurs patients. Il s'agit de spécifier et de concevoir un certain nombre de composants tels que le serveur de rapprochement des identités des patients, le composant de réservation de ressources pour l'organisation de visio conférences à distance, le composant de gestion des traces des différentes opérations effectuées sur les données médicales, le serveur de documents de patients partagés et le mécanisme de gestion des droits d'accès aux différentes informations manipulées dans ces composants. La modélisation de la politique de sécurité présentée dans cet article fait partie des études menées dans le cadre de ce projet pour gérer les droits d'accès des utilisateurs (patients, médecins, administratifs, personnels de soins,...) aux informations stockées dans le serveur de documents partagés.

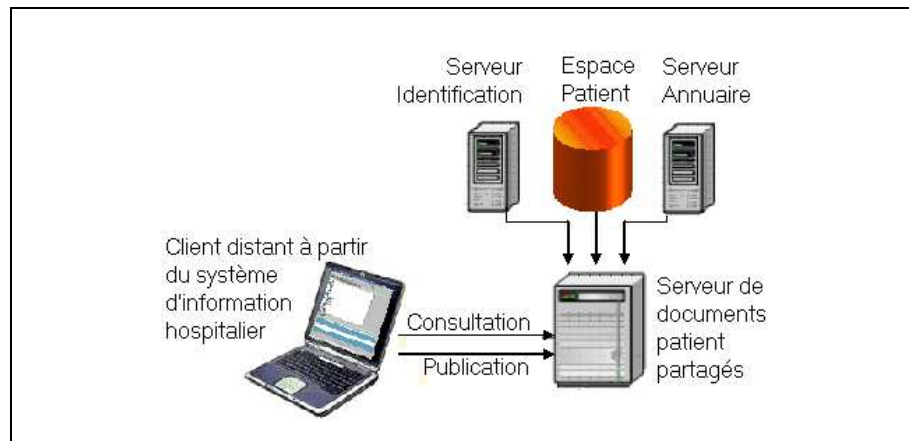


Figure 1. *Serveur de documents patient partagés*

Ce composant de GED (Gestion Electronique de Document) (*cf.* figure 1) doit permettre aux médecins de publier les documents d'un patient suivi pour une pathologie traitée dans les structures hospitalières de ce réseau de soins et de rechercher des documents d'un patient publiés par un confrère en respectant les droits d'accès à l'in-

formation déterminés par le consentement du patient (présent au niveau de l'Espace Patient, EsP). Dans cet article nous allons, dans un premier temps, présenter dans la section 2.1 le cadre de la modélisation et les contraintes qu'elle se doit de respecter. Nous verrons ensuite dans la section 2.2 la nécessité d'abstraire les règles de la politique pour une gestion plus aisée des droits d'accès se prêtant moins aux erreurs et aux incohérences. Dans la section 3, nous présenterons brièvement le modèle RBAC ses limites. Nous insisterons particulièrement sur l'absence de prise en compte des aspects contextuels dans la spécification des droits d'accès. Après une introduction dans la section 4 au modèle OrBAC, nous étudierons dans la section 5 comment modéliser la politique de sécurité avec OrBAC. Bien entendu, en raison de la limitation de l'espace qui nous est imparti, nous ne pourrons pas traiter tous les aspects de modélisation liés à la problématique de gestion du dossier médical partagé. Nous porterons donc l'accent sur les éléments qui nous semblent importants et donnerons ainsi l'intuition. La section 6 conclura l'article.

2. Problématique

2.1. *Le respect de la vie privée et le secret médical*

Le milieu hospitalier doit depuis toujours respecter deux grands principes : le respect de la vie privée et le secret médical. Or de nos jours, les personnes intéressées par la collecte, même frauduleuse, de ces informations personnelles sont nombreuses (média, assurance, banque, industrie pharmaceutique, patronat, ...).

Ces deux grands principes sont régis par des lois [JOFb] :

Le respect de la vie privée : un malade hospitalisé peut demander à ce que sa présence ne soit pas diffusée. Cette requête est légitime surtout lorsqu'elle émane d'une population dont la divulgation de l'information peut nuire (on peut citer en particulier les toxicomanes, les politiciens, les jeunes mères,...). Il est alors nécessaire de préserver l'identité et le secret de l'admission du patient dans les divers dossiers le concernant.

Le respect du secret médical, qui protège les données personnelles du patient, ne peut être écarté que dans les cas prévus par la loi. Le secret médical n'est pas opposable au patient (circulaire du 6 mai 1995). Il ne cesse pas à la mort du malade. Les établissements de santé doivent garantir la confidentialité des informations qu'ils détiennent sur leurs patients. L'article L 1110-4 nouveau du Code de la santé publique consacre le droit du malade à décider de l'usage des informations le concernant et n'autorise que de rares cas de partage du secret médical. Le patient peut donc s'opposer à la transmission des informations le concernant. Les conditions dans lesquelles les informations médicales peuvent être transmises à des tiers sont rigoureusement encadrées et des sanctions prévues. La loi prend en compte les problèmes nouveaux posés par le développement des échanges électroniques de données personnelles de santé entre professionnels et soumet ces échanges à de nombreuses règles. Nous avons plus particulièrement étudié l'expression formelle de cet aspect consentement du patient pour les accès à son dossier médical dans un réseau de soin et l'utilisation qui en est faite dans la modélisation de la politique de sécurité.

2.2. *La nécessité d'abstraire*

L'un des grands problèmes liés à la modélisation de la politique de sécurité liée aux données médicales est l'échelle de l'application de cette politique. En effet, ils existent plusieurs milliers de médecins, et plusieurs millions de patients. Il faut cependant définir les droits de chacun afin de préserver la confidentialité des informations liées au patient. Il est facile de s'apercevoir qu'il est nécessaire d'abstraire les règles de la politique de sécurité, afin de ne pas définir la politique pour une entité précise, mais pour un ensemble d'entité. Ainsi, on ne donnera pas explicitement le droit de consulter le dossier médical de Mr. Jacques à Mr. Paul son médecin référent. On donnera implicitement ce droit à Mr. Paul en autorisant tous les médecins référents à consulter le dossier médical de leur patient, sauf opposition expresse de leur part. Ainsi, au lieu de définir à chaque fois une règle pour des millions de patients, on a défini la règle une seule fois pour tous les patients. Donc grâce à l'abstraction des règles de sécurité, on réduit la complexité de la gestion des droits d'accès. L'un des objectifs des modèles de contrôle d'accès basés sur le concept de "rôle" est de permettre une telle abstraction.

3. Le modèle RBAC

3.1. *Présentation du modèle RBAC*

Le modèle RBAC (Role-based Access Control) [SAN 96] est à l'origine du concept de rôle. Le rôle est une notion permettant de décrire facilement les fonctionnalités des organisations. Un rôle désigne une entité intermédiaire entre utilisateurs et privilèges. On associe à chaque rôle un ensemble de permissions. Tous les sujets ayant reçu l'autorisation de jouer un rôle hérite alors des permissions associées à ce rôle. L'utilisation de la notion de rôle apporte un certain nombre d'avantages. La compréhension de la structure de l'organisation est facilitée. La complexité de gestion des droits d'accès est réduite. Les rôles peuvent être organisés de manière à former une hiérarchie [FER 01, SAN 02] permettant ainsi de raffiner les différentes permissions attribuées à chaque rôle. Ainsi, on définira un ensemble de règles pour tous les médecins. Puis si le rôle "chirurgien" est un sous-rôle du rôle "médecin" alors les chirurgiens posséderont les droits conférés aux chirurgiens spécifiquement ainsi que les droits hérités des médecins. Ainsi les politiques à base de rôles sont plus faciles à administrer. En effet, l'intégration de nouveaux utilisateurs, la gestion des permissions ou même la définition de nouveaux objectifs dans la politique de sécurité ne nécessitent que des modifications ponctuelles.

3.2. *Les limites du modèle RBAC*

Cependant, le contrôle d'accès basé sur les rôles est insuffisant pour satisfaire tous nos besoins en terme de protection. L'un des problèmes majeurs de ce modèle est le fait que tous les utilisateurs associés au même rôle possèdent forcément les mêmes pri-

vilèges. Ceci réduit la flexibilité des politiques de sécurité ainsi modélisées. En effet, dans une organisation tel qu'un hôpital, on peut souhaiter qu'un médecin n'ait accès qu'aux dossiers des patients dont il a le consentement. L'expression de ces aspects contextuels liés aux autorisations d'accès n'est pas inhérent au modèle RBAC et se fonde dans la notion de rôle, ce qui résulte dans une multiplicité des rôles non justifiés voire sémantiquement incorrects.

3.3. Les droits Contextuels

Il est facile d'imaginer que dans un contexte d'urgence, on désirera qu'un infirmier puisse accéder au dossier d'un patient lambda avec son consentement, sans avoir besoin d'appeler l'administrateur afin que celui-ci lui donne les droits (peut-être trop tard). Cette possibilité de nuancer les autorisations n'est pas offerte par DAC, MAC [FAY 01], RBAC, alors qu'il existe un réel besoin de ne donner des droits que dans des circonstances précises [BEZ 98].

Les textes de loi réglementent les accès aux informations liées aux patients. Les règles liées à la politique de sécurité doivent donc en tenir compte. Voici un extrait des textes de loi permettant de s'apercevoir que les règles d'accès sont modifiées selon le contexte :

Article L1111-7 [JOF02] : *"Toute personne a accès à l'ensemble des informations concernant sa santé ,[...], dans des conditions définies par voie réglementaire au plus tard dans le huitième jour suivant sa demande et au plus tôt après qu'un délai de réflexion de quarante-huit heures aura été observé. Ce délai est porté à deux mois lorsque les informations médicales datent de plus de cinq ans [...]."*

On voit clairement dans ce texte que l'accès pour un patient aux informations liées à sa santé ne se fait que dans un laps de temps précis et ce laps de temps varie sous certaines conditions. Il nous faut donc un modèle de contrôle d'accès permettant l'expression de ces autorisations dépendant du contexte.

4. Le modèle OrBAC

4.1. Présentation du modèle OrBAC

L'une des solutions pour répondre à ce problème de droits d'accès contextuels est le modèle de contrôle d'accès OrBAC [Abo 03, CUP 04b] (Organization Based Access Control).

Comme dans RBAC, un sujet est associé à un rôle en fonction du rôle qu'il joue dans une certaine organisation et obtient les permissions associées à ce rôle. Mais dans OrBAC, la structuration va au delà des sujets et touche également les actions et les objets. Ainsi, l'entité activité est une abstraction d'un ensemble d'actions l'implémentant et l'entité vue est une abstraction des objets ayant des propriétés de sécurité communes (proche du concept de vue dans les bases de donnée). Ainsi, contrairement

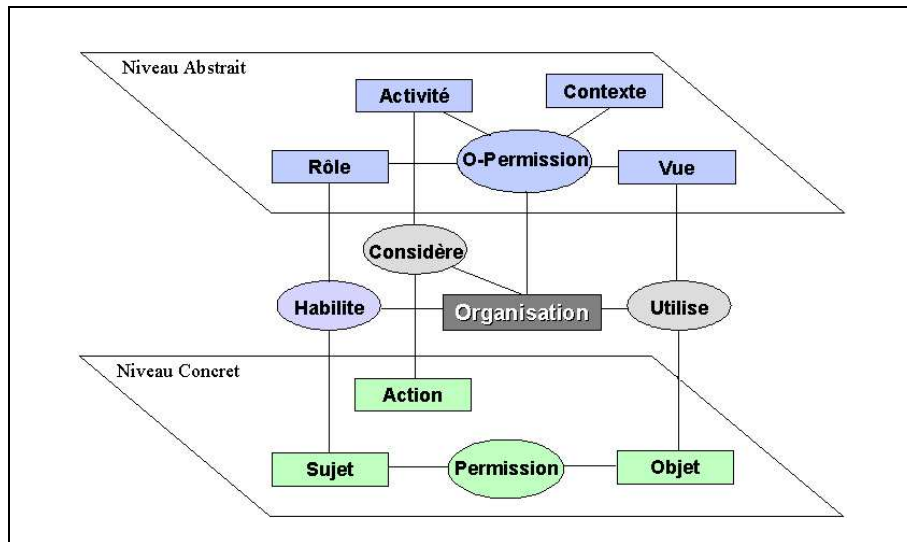


Figure 2. Les différentes entités de OrBAC et leurs relations

à RBAC, avec une seule règle dans OrBAC on peut exprimer que si un patient est opéré par une équipe médicale, tous les membres de cette équipe peut avoir accès au dossier de ce patient en question. L'organisation est au coeur du modèle OrBAC. Ainsi, l'équipe médicale opérant le patient est associée à une entité hospitalière particulière, une organisation donc, à laquelle on aura attribué un ensemble de privilèges qui peut différer de celui qu'aurait eu la même équipe dans un autre centre de soins. Grâce à ce formalisme, on peut ainsi mieux faire coopérer entre elles des organisations et des sous-organisations ayant des politiques de sécurité différentes. On voit apparaître sur la figure 2 le contexte [CUP 03] comme entité. Celui-ci est défini pour une organisation, un sujet, une action et un objet donnés. Les contextes permettent d'exprimer des permissions ou des interdictions dans certaines circonstances (urgence à l'hôpital, ...). Les contextes peuvent être temporels, spatiaux, liés à un historique, liés à l'usage fait par son utilisateur ou liés à l'environnement de l'utilisateur. On peut cumuler les contextes de façon conjonctive ou disjonctive. Ainsi, on peut définir un contexte en cas d'urgence pour une pathologie précise. On verra plus loin comment ils sont utilisés pour exprimer des autorisations dynamiques comme celles qui sont liées au consentement du patient ou aux liens de parenté par exemple.

4.2. Les avantages d'OrBAC

OrBAC permet d'exprimer aussi bien les autorisations, que les interdictions ainsi que les obligations/recommandations. On pourra ainsi, grâce aux obligations, autoriser un infirmier à accéder à un dossier médical en cas d'urgence sous condition qu'il rédige par la suite un rapport. Cette condition est exprimée grâce aux obligations.

OrBAC permet de prendre en compte les contextes. Mais l'abstraction et les contextes ne suffisent pas à définir tous les cas. En effet, il y a toujours des exceptions qui confirment la règle. Il peut arriver que pour des remplacements, lors de restructuration ou de travaux collaboratifs, on ait besoin de déléguer son droit à une personne qui ne le possède pas. OrBAC permet de définir dans quel cadre peut s'effectuer cette délégation (contexte exprimant la personne à qui on peut déléguer,...). Grâce à l'abstraction, au contexte, à l'héritage et à la délégation, OrBAC est un modèle simple à gérer. Les utilisateurs peuvent accéder simplement aux données qui leur sont autorisés.

5. La modélisation OrBAC

5.1. Les organisations

L'entité centrale dans le cas de la modélisation de la politique de sécurité liée au serveur de documents patient partagés est une organisation au sens OrBAC (Org.PS) réunissant un ensemble de professionnels de santé et de patients. Sa structure est donnée par le schéma de hiérarchie d'organisations suivant :

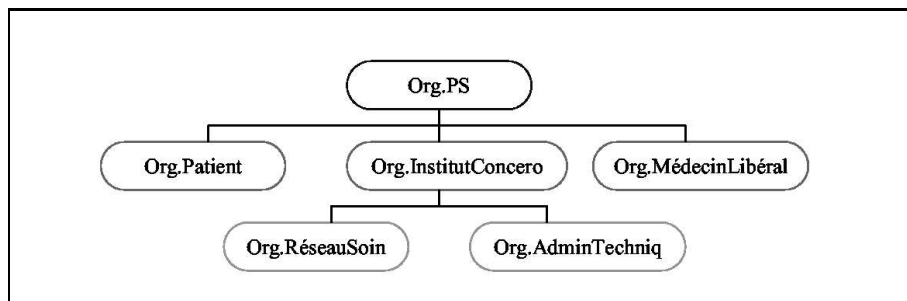


Figure 3. Hiérarchie d'organisation

En particulier, l'organisation *Org.InstitutCancero* représente l'institut de cancérologie et est constituée de l'ensemble du personnel de santé et administratif de trois structures hospitalières souhaitant partager des informations médicales. C'est en fait l'organisation gérant les accès au système GED. L'organisation *Réseau de soins* correspond aux différentes équipes pluridisciplinaires dispersées géographiquement et qui peuvent solliciter des accès au système GED. *Org.AdminTechnique* désigne les équipes techniques chargées du bon fonctionnement et de la maintenance du système GED. Les différentes règles de sécurité vont être identifiées relativement à cette organisation et ses différentes sous-organisations.

5.2. les rôles

Les sujets dans le cadre du système GED correspondent à des professionnels de santé, des personnes administratives ou/et techniques, des patients et des proches des

patients. L'attribution des droits d'accès à ces sujets se fait par le biais de la structuration en rôles. Les sujets se voient attribuer des droits d'accès au système et donc aux documents patient partagés en jouant des rôles. Un rôle correspond à un profil de règles de contrôle d'accès et n'a de sens que dans l'organisation où il été défini. Le tableau suivant (cf. tableau 1) résume l'ensemble des rôles qui ont pu être identifiés, leur affectation aux utilisateurs du système GED et les organisations auxquelles ils se rattachent (voir la notion de pertinence dans [CUP 04a]).

Rôle	Utilisateur	Organisation pertinente			
		Org. Patient	Org.Médecin Libéral	Org.Réseau Soins	Org.Admin Technique
R.Patient	Patients	+			
R.NomPatient	Famille du patient (proche, éloignée) Personne de confiance Connaissance du patient	+			
R.Medecin	Médecins de l'ICancero			+	
R.Med_isole	Médecins libéraux (non attachés à l'IC)		+		
R.Sec_Med	Personnels administratifs et sociaux			+	
R.Paramédiaux	Personnels de soins			+	
R.Admin_Dom	Personnel Informatique Médical				+

Tableau 1. Identification des rôles dans le système GED

Une hiérarchie des rôles a été définie pour permettre l'héritage des différentes permissions et interdictions. Nous ne pouvons pas traiter dans ce papier ces aspects mais nous présentons une hiérarchie de rôles plus finement identifiés dans la figure 4.

5.3. Les Vues

Le dossier médical comporte de nombreux documents. Comme on l'a vu auparavant, la gestion de la politique de sécurité est simplifiée lorsqu'on structure les éléments que l'on manipule en les abstrayant. Dans OrBAC, les documents sont modélisés sous forme d'objets qui sont regroupés dans des vues. Cette abstraction des objets en vues permet de diminuer le nombre de règle à définir dans la politique de sécurité à l'image de l'apport de la structuration des sujets en rôles. En effet, pour chaque document du dossier médical, il existe des contraintes. Pour chaque patient hospitalisé dans un établissement de santé public ou privé, un dossier médical est constitué. D'après la loi [JOFa], ce dossier contient au moins les trois éléments suivants :

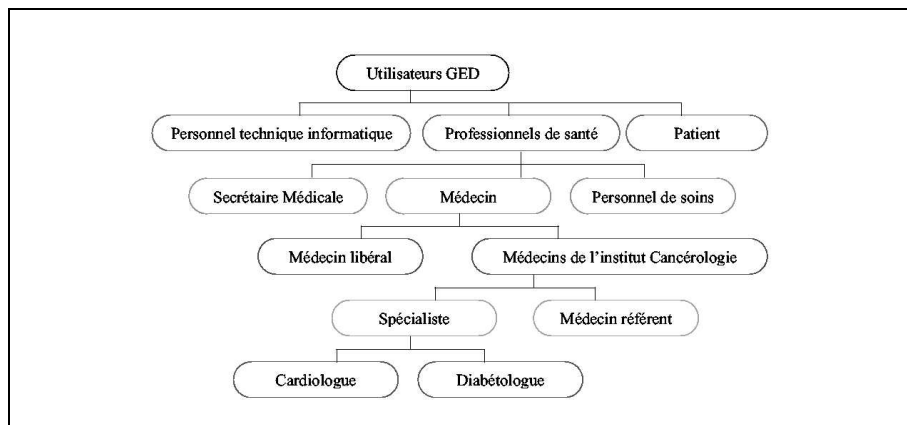


Figure 4. Hiérarchie de rôle

- 1) Les informations formalisées recueillies lors des consultations externes dispensées dans l'établissement, lors de l'accueil au service des urgences ou au moment de l'admission et au cours du séjour hospitalier,
- 2) Les informations formalisées établies à la fin du séjour,
- 3) Les informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant de tels tiers.

Seules les informations contenues dans 1^o et 2^o sont communicables. Pour chaque document, conformément au point 3^o, il faut donc créer une règle qui empêchera toute personne n'ayant pas fourni, ni recueilli ces informations d'y accéder. Or, les informations venant d'une personne n'intervenant pas dans la prise en charge du patient, peuvent être de diverses natures, de divers formats. Il est difficile de vérifier lors de la création d'un document, s'il est créé par une personne n'appartenant pas au personnel de prise en charge, où une personne ayant reçu un droit d'une personne prenant en charge le patient. En effet, on peut envisager qu'un médecin délègue à sa secrétaire le soin de dactylographier le compte rendu post opératoire qu'il aura laissé sur dictaphone. Or dans ce cas, la secrétaire ne fait pas parti du personnel de prise en charge, mais le document qu'elle a créé et vu comme provenant de l'équipe de prise en charge. Cette même secrétaire peut avoir son mari opéré par le médecin pour qui elle travaille. Dans ce cas, toutes les informations recueillies auprès d'elle sur les choix faits lors de l'hospitalisation de son mari sont confidentielles. La solution proposée par le modèle OrBAC et d'abstraire tous les documents de la troisième partie du dossier médical dans une vue (*V.InfoTiers*). Il est alors possible de formuler une règle globale d'interdiction de consulter tous les objets dans cette vue. Cette règle peut ensuite être modulée selon le contexte, le besoin et les priorités d'accès (urgences, absence,...) pour gérer les exceptions. Le dossier médical est régi par des règles législatives strictes. Afin de respecter ces règles, lors de l'accès au serveur de documents de patients partagés qui

contient les dossiers médicaux, on modélise les vues comme décrites dans le tableau 2.

Vue	Sous vues		Contenu	
V.Dossier Médical Partagé	V.Consentement		droits d'accès autorisés par le patient	
	V.Identification		information d'identification du patient	
	V.Dossier Médical	V.Admission EtSéjour	V.LettreMédecinRef	lettre qui est à l'origine de l'admission
			V.MotifHospitalisation	motif d'hospitalisation
			V.Antécédent	antécédents et facteurs de risques
			V.ConclusionEvaluation	conclusion d'évaluation clinique initiale
			V.PriseEnCharge	prise en charge prévue et prescriptions
			V.SoinConsultExt	soins dus à une consultation externe
			V.InfoHospitalisation	informations prises pour hospitalisation
			V.DémarcheMédicale	informations sur la démarche médicale
			V.Anesthésie	dossier d'anesthésie
			V.CompteRenduOpération	compte rendu opératoire
			V.ConsentementSpecif.	consentement écrit du patient
			V.Transfusion	actes transfusionnels
			V.PrescriptionMédicale	prescription médicale
	V.FinSéjour	V.SoinInfirmier	soins infirmiers	
		V.SoinAutreProSanté	soins dispensés par les autres PS	
		V.CorrespondanceProSanté	correspondances échangées entre PS	
V.CompteRenduSortie		compte rendu et lettre de sortie		
		V.OrdonnanceSortie	prescription de sortie	
		V.ModalitéSortie	modalités de sortie	
		V.FicheLiaison	fiche de liaison infirmière	
		V.InfoTiers	informations recueillies auprès de tiers	

Tableau 2. Vues de la modélisation de la politique de sécurité liée au dossier médical

5.4. les activités

Les activités correspondent aux divers services offerts par le système GED à ses utilisateurs et plus particulièrement le serveur de documents patient partagés. Il doit leur permettre, entre autres, de : publier des documents relatifs à un patient pris en charge pour une pathologie cancéreuse (Act.Publication), rechercher des documents liés à un patient (Act.Recherche), notifier un ou plusieurs tiers de la présence d'un document patient partagé donné (Act.Notification), définir la liste des personnes constituant le consentement d'un patient (Act.GestionConsent). Ces différentes activités sont implantées par des action concrètes. Ainsi, l'activité A.Publication est une abstraction des actions : ajouter, transformer, remplacer, archiver et notifier. La structuration des actions est donnée par le schéma de hiérarchie d'activité dans la figure 5.

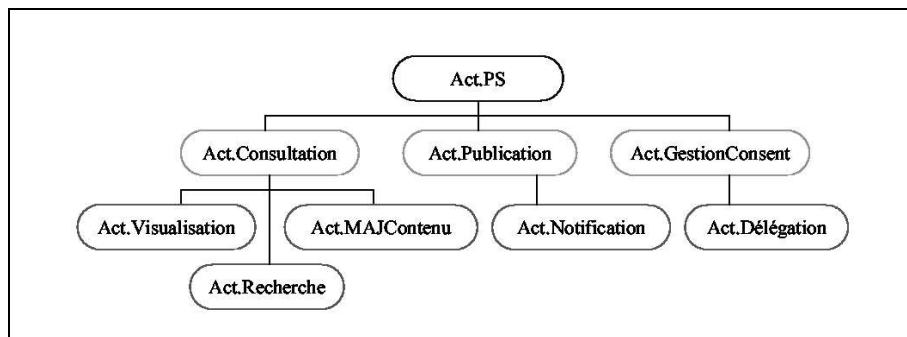


Figure 5. *Hiérarchie d'activité*

5.5. Les contextes

Dans le cadre de la gestion de la confidentialité et de l'intégrité des documents patients partagés, la modélisation OrBAC a permis d'identifier plusieurs contextes d'attribution des droits d'accès à ce type de document qui peuvent être cumulés selon les besoins de sécurité :

- **Contextes de type prérequis** : On peut citer, par exemple, Ctx.DossierDuPatient, Ctx.PersonneConfiancePatient, Ctx.MedTraitant. Leur utilisation permet de contraindre les sujets concernés par les permissions ou les interdictions dépendant de ces contextes et qui vient réduire ou étendre les droits d'accès hérités du rôle associé. Dans une modélisation OrBAC, on définit toujours un contexte par défaut. Celui-ci est traité un peu plus en détail dans la section suivante.

- **Contextes de type déclaré par l'utilisateur** : Ce type de contexte est activé, par exemple, par le médecin chef du service des urgences dans le cas où un patient dans un état grave y est transféré. En effet, aucun traitement ne peut lui être appliqué sans consultation au préalable du dossier médical. Dans ce cas, le médecin chef de ce service est habilité à activer ce contexte pour récupérer les droits d'accès appropriés. Il est obligé en contrepartie de faire un compte-rendu des opérations effectuées.

- **Contextes de type temporel** : ce sont des contextes régissant la durée de validité des droits d'accès au dossier médical partagé.

5.5.1. Expression du consentement du patient

Une des données d'entrée au serveur de documents patient partagés d'importance est celle provenant du composant EsP qui contient le résultat du consentement du patient. Ce résultat se traduit par des droits d'accès définis par le patient régissant l'accès à son dossier médical. Une API permet de notifier le composant EsP de la plateforme de télé santé du recueil du consentement du patient. Cette information est utilisée par les autres composants lors des demandes d'accès au dossier du patient. En l'absence du consentement du patient, l'accès au dossier médical partagé ou la publi-

cation de documents pour ce patient ne sera pas possible. Le consentement du patient sera recueilli depuis les systèmes d'information hospitalier (SIH). Il correspond à une interrogation adressée au patient : "Autorisez vous l'accès à votre dossier aux professionnels susceptibles de vous prendre en charge au sein des réseaux dans lesquels vous serez traités, ainsi que tous les professionnels de santé expressément nommés par vous". Il est enregistré dans le dossier médical du patient géré au niveau du SIH et est caractérisé par les points suivants :

- Il est enregistré à une date déterminée,
- Il est accordé par le patient pour une durée déterminée,
- Il est accordé par le patient aux professionnels de santé d'un ou plusieurs réseaux de soins et/ou pour une liste nominative de personnes appartenant ou non à un réseau. Ainsi, le médecin généraliste du patient n'appartient pas à un réseau, mais le patient peut donner son accord pour que ce médecin accède à son dossier médical,
- Il est révocable même si la durée de son octroi n'a pas expiré.

On peut distinguer trois types de consentement :

- **Consentement nominatif** : le patient Mr A. Soigner est pris en charge dans le réseau de cancérologie. Lors du recueil de son consentement, il donne son accord aux médecins qui vont le prendre en charge (Dr Médecinun - Dr Médecindeux - Dr Médecintrois) pour l'accès à son dossier. Son médecin généraliste obtient également son aval pour accéder aussi à son dossier.

- **Consentement permissif** : le patient Mr A. Soigner est pris en charge dans le réseau de cancérologie et le réseau de diabétologie. Lors du recueil de son consentement, il donne son accord à son médecin référent pour que l'ensemble des médecins du réseau de cancérologie ainsi que l'ensemble des médecins du réseau de diabétologie accède à son dossier partagé. Mr A. Soigner souhaite également que son médecin généraliste accède aussi à son dossier.

- **Consentement exclusif** : le patient Mr A. Soigner est pris en charge dans le réseau de cancérologie. Lors du recueil de son consentement, il donne son accord à son médecin référent pour que tous les médecins du réseau puissent accéder à son dossier, sauf le Dr Bistouri.

Cet aspect consentement pour l'attribution des droits d'accès au dossier ne peut être formulé en terme de rôle tel que pourrait le suggérer une modélisation RBAC. L'utilisation de ce type de modélisation nécessiterait l'introduction d'une notion "bâtarde" que l'on pourrait appeler *rôle dynamique*, i.e. un ensemble de règles labellisées activables lorsque certaines contraintes sont satisfaites. le modèle RBAC ne donne pas de moyens élégants pour exprimer de telles contraintes. Ces droits liés au consentement sont circonstanciels et dépendent des décisions d'accès prises par le patient concerné par le dossier médical à un moment donné. Ce sont des droits dépendant du contexte, une entité native dans le modèle OrBAC. Ainsi, le consentement nominatif identifié ci-dessus peut être modélisé par $Ctx_Consent$ exprimé de la façon suivante :

$$\forall org \in \mathcal{O}, \forall s \in \mathcal{S}, \forall a \in \mathcal{A}, \forall o \in \mathcal{O}, \forall p,$$

$$\begin{aligned} & Hold(org, s, a, o, Ctx_Consent) \\ & \leftarrow Empower(org, p, R_Patient) \wedge N_consent(p, s, a, o) \end{aligned}$$

Cette règle indique qu'il suffit donc qu'un patient donne un consentement explicite à un sujet s pour effectuer une action a sur un document du dossier médical o , introduit par le prédicat $N_consent(p, s, a, o)$, pour que le contexte de consentement nominatif $Ctx_Consent$ soit valide. Tout sujet ne bénéficiant pas de ce consentement se verra invalidé les permissions liées à ce contexte.

Le consentement permissif lie un sujet s entreprenant une action a sur un document du dossier médical o dans le cas où il est attribué aux sujets jouant certains rôles ou explicitement cités. Ce n'est uniquement que dans le cas de sujets jouant un certain rôle et bénéficiant du consentement du patient que des exceptions peuvent être précisées de façon nominative par le patient. C'est pourquoi le consentement permissif et exclusif ne peuvent être modélisés séparément. Un autre cas de consentement peut être formalisé de la façon suivante :

$$\begin{aligned} & \forall org \in \mathcal{O}, \forall s \in \mathcal{S}, \forall a \in \mathcal{A}, \forall o \in \mathcal{O}, \forall p, \\ & Hold(org, s, a, o, Ctx_Consent) \\ & \leftarrow Empower(org, p, R_Patient) \wedge Empower(org, s, r) \\ & \quad \wedge P_consent(p, r, a, o) \wedge \neg E_consent(p, s, a, o) \end{aligned}$$

Dans cette règle, les prédicats $P_consent$ et $E_consent$ représentent respectivement les consentements permissifs et exclusifs. Le contexte de consentement ainsi défini, on peut exprimer les permissions d'accès des médecins aux dossiers médicaux des patients pris en charge par le réseau de soins et par le système GED.

$$\begin{aligned} & Permission(OrgReseauSoin, R_Medecin, Act_Consultation, \\ & \quad V_Dos_Med_Pat, Ctx_Consent) \\ & Permission(OrgReseauSoin, R_Medecin, A_Recherche, \\ & \quad V_Dos_Med_Pat, Ctx_Consent) \end{aligned}$$

Le modèle OrBAC permet la spécification de règles de sécurité de type interdiction et gère, au niveau abstrait, les conflits qui peuvent en dériver. Un module de gestion de conflit en Swi-Prolog intégré à OToKit (un prototype de spécification et de simulation de politique de sécurité basée sur OrBAC a été développé. Au cours de la modélisation du contrôle d'accès au système GED, on s'est rendu compte que faire le choix de s'orienter vers une politique de sécurité ouverte (tout ce qui n'est pas interdit est permis) ou vers une politique fermée (tout ce qui n'est pas permis est interdit) ne peut pas toujours répondre à toutes les conditions d'accès en particulier pour les exceptions nominatives. Nous avons opté pour une politique mixte. Ainsi, les secrétaires médicales ont l'interdiction de réaliser une activité de type gestion sur la vue consentement du patient :

$$\begin{aligned} & Prohibition(OrgReseauSoin, R_Sec_Med, Act_GestionConsent, \\ & \quad V_ConsentementSpecif, Ctx_Consent) \end{aligned}$$

Dans OrBAC, les permissions et interdictions concrètes sont dérivées de façon automatique conformément à la règle suivante :

$$\begin{aligned}
&\forall Organization \in \mathcal{O}, \forall Role \in \mathcal{R}, \forall Activity \in \mathcal{A}, \forall View \in \mathcal{V}, \forall Context \in \mathcal{C}, \\
&\forall Subject \in \mathcal{S}, \forall Action \in \mathcal{A}, \forall Object \in \mathcal{O}, \\
&\quad Authorisation(Organization, Role, Activity, View, Context) \wedge \\
&\quad Empower(Organization, Subject, Role) \wedge \\
&\quad Consider(Organization, Action, Activity) \wedge \\
&\quad Use(Organization, Object, View) \wedge \\
&\quad Hold(Organization, Subject, Action, Object, Context) \\
&\quad \leftarrow Is_authorised(Subject, Action, Object)
\end{aligned}$$

Où *Authorisation* a été mis pour signifier une *Permission* (resp. une *Prohibition*) et *Is_authorized* pour *Is_permitted* (resp. *Is_prohibited*).

6. Conclusion

Dans cet article, on a pu voir l'importance des lois et des principes qui régissent le milieu médical. Ainsi que les problèmes que ceux-ci posent lors des échanges d'informations. Du fait du grand nombre d'entités concernées par les règles de la politique de sécurité, il est apparu nécessaire d'abstraire les règles. L'abstraction permet de réduire la complexité de la gestion de la politique de sécurité. On a pu constater les limites du modèle RBAC. En effet, les politiques liées au domaine médical reposent sur de nombreux contextes qui ne sont pas pris en compte par les principaux modèles de contrôle d'accès. Afin de pallier ce problème, nous avons étudié un exemple de modélisation grâce à OrBAC. Les avantages d'OrBAC sont l'abstraction des sujets, des actions et des objets, la prise en compte des contextes, la simplification de la gestion de la politique (via l'héritage et la délégation). Nous avons pu voir l'utilité d'avoir des contextes pour le consentement qui est un élément déterminant pour contrôler l'accès à un dossier médical puisqu'il permet de définir les droits donnés par le patient sur son dossier.

Dans le cadre de ce projet, un des axes également exploré est l'étude des modalités de mise en œuvre ou de transposition XACML [ARM 03] de la modélisation OrBAC. Le terme approprié pour le passage de l'un vers l'autre n'est pas évident à déterminer, d'abord parce que les deux modèles ne se situent pas au même niveau d'abstraction et ensuite l'expressivité d'OrBAC au travers de ces différentes entités de structuration se perd dans un codage XACML. Cela s'apparenterait un peu à la génération d'un pré-codage d'un programme exprimé dans un langage évolué. Ce qui fait de XACML un bon candidat pour une pré-compilation d'une modélisation OrBAC. Un profil XACML accompagné de recommandations pour les éléments non directement transposables sans une modification de la grammaire XACML a été élaboré. Il a servi à l'expression de la politique de contrôle d'accès aux documents patient partagés dont certains aspects de la modélisation ont été présentés dans cet article.

Remerciements

A Isabelle Gibaud et Joseph Berthiaud du SIB (Syndicat Interhospitalier de Bretagne) pour les discussions intéressantes que nous avons pu avoir avec eux, à Sylvain Gombault pour l'intérêt qu'il a porté à cette étude, à Thierry Sans pour ses conseils sur les aspects profil XACML, à Monique Nguyen et Cédric Obejero pour leur contribution.

7. Bibliographie

- [Abo 03] ABOU EL KALAM A., BAIDA R. E., BALBIANI P., BENFERHAT S., CUPPENS F., DESWARTE Y., MIÈGE A., SAUREL C., TROUessin G., « Organization Based Access Control », *Policy'03*, juin2003.
- [ARM 03] ARMSTRONG M., « An introduction to XACML », *GIAC Security Essentials*, juin2003.
- [BEZ 98] BEZNOSOV K., « Requirements for access control : US Healthcare domain », *RBAC '98 : Proceedings of the third ACM workshop on Role-based access control*, New York, NY, USA, 1998, ACM Press, page 43.
- [CUP 03] CUPPENS F., MIÈGE A., « Modelling Contexts in the Or-BAC Model », *ACSAC '03 : Proceedings of the 19th Annual Computer Security Applications Conference*, IEEE Computer Society, 2003, page 416.
- [CUP 04a] CUPPENS F., CUPPENS-BOULAHIA N., MIÈGE A., « Hiérarchies d'héritage dans le modèle Or-BAC : application dans un environnement réseau », *Journées SSTIC*, juin2004.
- [CUP 04b] CUPPENS F., MIÈGE A., « Or-BAC (Organization Based Access Control) », *DRUIDE*, mai2004.
- [FAY 01] FAYAD A., JAJODIA S., FAATZ D., DOSHI V., « Going beyond MAC and DAC using mobile policies », *Sec '01 : Proceedings of the 16th international conference on Information security : Trusted information*, 2001, p. 245–260.
- [FER 01] FERRAILOLO D. F., SANDHU R., GAVRILA S., KUHN D. R., CHANDRAMOULI R., « Proposed NIST Standard for Role-Based Access Control », *ACM Transactions on Information and System Security*, vol. 4, août2001, p. 224-274.
- [JOFa] « Code de Déontologie Médicale, Article R1112-2 », Code de la Santé Publique, Journal Officiel.
- [JOFb] « Code de Déontologie Médicale, R.4127-1 à R.4127-112 », Code de la Santé Publique, Journal Officiel.
- [JOF02] « Loi du 4 mars 2002 », Code de la Santé Publique, 2002, Journal Officiel.
- [SAN 96] SANDHU R. S., COYNE E. J., FEINSTEIN H. L., YOUMAN C. E., « Role-Based Access Control Models », *Computer*, vol. 29, n° 2, 1996, p. 38–47, IEEE Computer Society Press.
- [SAN 02] SANDHU R., OH S., « A Model for Role Administration Using Organization Structure Roles », 2002, page 8.
- [TAD 02] TADONKI P. D., « Sécurité dans les applications de télémédecine », Thèse de doctorat, Université de Yaoundé 1, septembre2002.