# Contrôle d'accès basés sur les rôles, les groupes d'objets et le contexte : Étude de cas dans les Systèmes d'information et de Communication en Santé

Anas Abou El Kalam, Yves Deswarte

LAAS-CNRS — 7 avenue du Colonel Roche — 31077 Toulouse Cedex 4 — France
{anas.abouelkalam, yves.deswarte}@laas.fr.

## Introduction

Dans ce papier, nous traitons du problème du contrôle d'accès dans les systèmes d'information et de communication en santé (SICS). Le contrôle d'accès doit être basé sur un modèle qui doit couvrir la richesse des SICS, permettre leur interopérabilité, contribuer à contrer les menaces (accidentelles ou malveillantes) et prendre en compte toute amélioration ou changement dans la politique de sécurité (extensible et modulable). Ce modèle doit s'exprimer dans un langage de spécification à la fois simple et expressif.

La première partie de ce travail consiste à décrire les différents concepts utiles pour fournir un contrôle d'accès (CA) flexible et sur mesure. Nous proposons une solution dont l'originalité repose sur :

- L'introduction du concept de groupe d'objets qui servira essentiellement à :
  - structurer les objets passifs ;
  - faciliter et assouplir la spécification et la gestion de la politique de sécurité ;
  - incorporer une des facettes de la notion du contexte ;
  - résoudre certains des problèmes de l'application de politiques basées sur la notion de rôle aux SICS ;
- Le contexte qui est une notion générique très vague. Nous allons donc l'encadrer en identifiant quatre types de contextes : le contexte du rôle, le contexte de l'utilisateur, le contexte relié à un groupe d'objets et le contexte relatif à l'utilisation (l'objectif de l'utilisation).

Les concepts que nous allons définir vont servir à introduire les notions qui peuvent intervenir dans le contrôle d'accès comme : l'unité (de soins), le processus de soins ainsi que les différents types des dossiers médicaux. Dans un deuxième temps, nous proposons une extension du langage déontique qui nous servira, dans un troisième temps, à représenter, d'une manière à la fois simple, riche et flexible, les règles d'accès de notre système.

**Mots clés :** Politiques de sécurité, RBAC, TMAC, autorisation, contrôle d'accès,Systèmes d'informations médicales, logique déontique, UML.

## I. Concepts du contrôle d'accès

L'analyse des politiques de sécurité et des modèles existants que nous avons effectuée dans [1] nous permet de conclure que l'état de l'art actuel est insuffisant. En effet, le contrôle d'accès discrétionnaire (DAC) présente de graves inconvénients vis-à-vis des fuites d'informations et des chevaux de Troie, tandis que le contrôle d'accès obligatoire (MAC) [2] [3] [4] [5] est très rigide et mal adapté aux systèmes réellement répartis. Nous visons donc à réaliser un compromis entre MAC et DAC en

renforçant la sécurité des MAC et en maintenant la flexibilité des DAC. D'autre part, la nature distribuée et inter organisationnelle, la diversité des flux et la variété des objets et des sujets des systèmes d'information et de communication en santé (SICS) augmentent la complexité de ce système. L'étude de la fonction de sécurité ne peut être implémentée et mise en oeuvre que si les entités de notre spécification sont bien structurées. À cet égard, le concept de rôle permet de fournir une classification des sujets. Pour améliorer l'organisation, le nouveau concept nommé « groupe d'objets », permet de regrouper l'ensemble des objets passifs sur lesquels on réalise les mêmes opérations. Cette solution met donc en relation les objets à protéger et les opérations sur ces objets.

### *I.1 Le contrôle d'accès basé sur les rôles*

Une politique telle que tous les droits d'accès sont attribués aux utilisateurs en fonction du rôle qu'ils jouent dans le système d'information est appelée politique par rôle (voir [6] [7] [8]). Un rôle désigne une entité intermédiaire entre utilisateurs et privilèges. Ces derniers ne sont plus associés, d'une façon directe aux utilisateurs mais à travers des rôles. Les deux relations {Rôle, Privilège} (figure 1) et {Utilisateur, Rôle} définissent les privilèges accordées à chaque utilisateur.

| | Dossier Administratif | Examen | Dossier Clinique | Dossier Financier | Rapport Infirmier | Prescription |
|---|---|---|---|---|---|---|
| Secrétaire | R W | - - | - - | R W | - - | - - |
| Infirmière | - - | R W | - - | - - | R W | R - |
| Médecin traitant | R - | R W | R W | - - | R - | R W |
| Pharmacien | R - | - - | - - | R W | - - | R - |
| Patient | R W | R - | R - | R - | R - | R - |

Figure 1 : exemple simplifié de table 'Rôle – Privilège' qui ne considère que les opérations d'écriture « W » et de lecture « R »

La notion de rôle permet de faciliter l'administration de la politique de sécurité (l'intégration des utilisateurs, la gestion des permissions, la définition de nouveaux objectifs) et de gérer la complexité de gestion des droits d'accès (hiérarchie de rôles). Néanmoins, seul, ce concept semble insuffisant pour satisfaire tous nos besoins en terme de contrôle d'accès. L'un des problèmes de l'application du contrôle d'accès par rôles aux systèmes de santé est que tous les utilisateurs ayant le même rôle ont les mêmes privilèges (sur les mêmes objets passifs). Dans le domaine médical, cela pose un problème : la modélisation de la notion de « traiter un patient donné » met en relation un ensemble d'utilisateurs avec un ensemble de patients. Tous les utilisateurs ayant le même rôle ne traitent pas forcément les mêmes patients, et par conséquent, ils n'ont pas les mêmes privilèges. Par exemple, le seul fait d'être un médecin (avoir le rôle médecin) ne donne pas le droit d'accéder aux données privées des patients qu'il ne traite pas. Ainsi les privilèges du même rôle « médecin », différent d'une instance (Médecin X traitant un patient M) à une autre (Médecin Y traitant un patient N). Dans ce cas, l'instance X du rôle médecin possède des privilèges sur le patient M (et aucun privilège sur N), alors que l'instance Y du même rôle médecin possède des privilèges sur le patient N (et aucun privilège sur M).

Ainsi, les privilèges doivent être attribués, non seulement selon le rôle du professionnel de santé, mais aussi selon :

- la relation de soin existante entre le professionnel de santé et le patient,
- l'implication du professionnel de santé (au moment de la requête) dans le processus de soins,
- d'autres informations contextuelles comme le lieu, le temps, l'urgence [1], l'exclusion mutuelle entre rôles, la délégation et de la séparation des intérêts, etc.

Afin d'offrir un contrôle d'accès plus adapté, le concept de groupe d'objets, que nous introduirons dans la section suivante, permet de compléter la notion de rôle, de résoudre les problèmes cités

précédemment et de réduire considérablement la complexité des systèmes d'information et de communication en santé.

### *I.2 Concept de groupe d'objets*

La construction des groupes d'objets passifs se fait en trois étapes :

**Première étape** : selon une vue logique, effectuer des regroupements d'objets passifs (dossiers des patients traités par un médecin donné, ressources d'une unité de soins, données d'urgence, données administratives des patients hospitalisés à l'hôpital de Rangeuil, équipements, locaux). Dans UNIX par exemple, les fichiers qui appartiennent au même groupe ont le même identifiant GID. Dans les SICS, la construction des groupes doit posséder une sémantique. Ils sont associés à un hôpital, à un département, à une unité, à un projet, à une tâche dans le processus de soins. Par exemple, nous pouvons considérer les fichiers des patients ainsi que les ressources d'une unité de soins ( ou d'une équipe ou d'un médecin) comme deux groupes d'objets associés à cette unité de soins (ou à l'équipe ou au médecin).

**Deuxième étape**: relier chaque groupe d'objets passifs avec les opérations effectuées sur les objets qui le constituent. Une des manières de réaliser ces deux premières étapes, est de regrouper les objets sur lesquels nous effectuons les mêmes opérations (figure 2). Ainsi, en jouant un rôle donné, l'utilisateur obtient des privilèges lui permettant de réaliser des opérations sur le groupe d'objets mentionné.

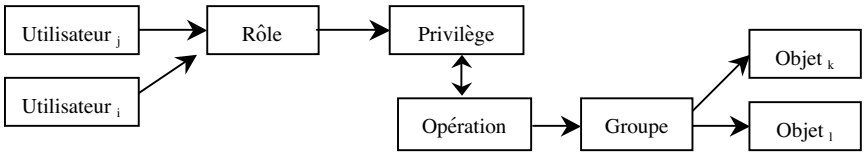



***Figure 2*** : les relations : (utilisateur, rôle, privilège) et (objet, groupe, opération)

Nous distinguons deux types d'opérations :

- *Opérations de bas niveau* : des opérations élémentaires du type : créer, lire, ajouter….
- *Opérations complexes* : une succession d'exécutions d'opérations élémentaires par un où plusieurs sujets sur un ou plusieurs objets (la réalisation d'une opération complexe exige l'existence de plusieurs privilèges associés à un ou plusieurs utilisateurs). Une opération de ce type peut donc être vues comme une **fonction** ou une méthode. Par exemple : l'opération « Prescrire : désigne l'ensemble des opérations de bas niveau : lire données (séjour hospitalier, feuille de thérapie, historique des médicaments, rapport infirmier, résultat tests) du patient ; créer/écrire/modifier feuille de thérapie » ; délégation, etc.

L'intérêt de cette séparation est que pour les opérations complexes, deux types de contrôles peuvent être effectués :

- contrôle au niveau des opérations élémentaires (de bas niveau) qui constituent l'opération complexe Par exemple : est ce que le médecin à le droit de lire les données de séjour hospitalier ?
- contrôle au niveau de l'opération complexe elle même (la fonction ou la méthode). Par exemple, est ce que le médecin à le droit d'invoquer la méthode « prescrire ».

**Troisième étape** : réduire la complexité et améliorer la structuration en reliant les groupes. Deux types de relations peuvent être distingués :

- Héritage (hiérarchie de groupes). Supposons, à titre d'exemple que nous construisons deux groupes : ressources de l'unité de soins cardiologie et ressources de l'unité de soins. Nous pouvons constater la relation d'héritage : ressource de l'unité de soins cardiologie ***est une*** ressource de l'unité de soins (première ligne de la figure 3) ; Le dossier clinique ***est une*** ressource clinique ; etc.
- Composition (agrégation). En notation UML [17], La figure 3 montre que : ressource de l'unité de soins chirurgicale « $C_5$ » ***est composée de*** deux salles « $C_{5,1}$ et $C_{5,2}$ », des postes ayant des adresses entre 192.168.1.0 et 192.168.1.9 et des dossiers de spécialité des patients ayant transité par cette unité ; Le dossier du patient ***est composé d***'une partie administrative (identité, adresse, age, sexe, coordonnées de mutuelle) et d'une partie médicale (ce que dit le patient, ce que constate le soignant « examens », ce qui est réalisé « protocoles, avis », ce qui est conclu « diagnostic traitement, délivrance de documents »).

Ces relations favorisent la propagation des valeurs d'attributs des sous-classes vers les super-classes, et les opérations sur l'agrégat vers les composants.

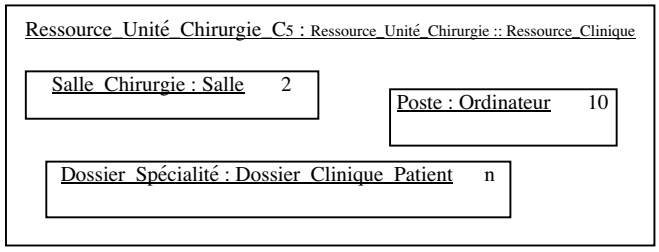



*Figure 3* : Objets composites de « Ressource de l'unité Chirurgicale $C_5$ ».

Selon une vision orientée objet, un groupe d'objets est une classe dont les objets instances possèdent des informations en communs (des attributs comme l'unité de rattachement) et des fonctions (méthodes) relatives à la sécurité, qui illustrent les opérations pouvant être exercées sur ces objets (sur les objets d'un groupe donné, un utilisateur réalise les mêmes opérations). Par exemple, un « médecin » (rôle) peut accéder aux « dossiers des patients de son unité » (groupe d'objets). Une action (Sujet, Objet, Opération) ne peut être autorisée que si l'ensemble des privilèges des rôles joués par l'utilisateur ainsi que le contexte, passé sous forme d'arguments d'invocation, permettent d'invoquer la méthode implémentant l'opération.

Pour résumer, nous remarquons qu'outre les raisons de structuration, les groupes d'objets sont construits de façon à établir le lien entre les professionnels de santé et les objets qu'ils manipulent, y compris les fichiers des patients qu'ils traitent. Dans la section suivante, nous expliquerons les notions concrètes qui présentent le cadre dans lequel ce lien est réalisé.

# II. Unité de soins, processus de soins, et accès aux dossiers médicaux

## *II.1 Notion d'unité*

Le système de santé peut être vu comme un ensemble de domaines qui interagissent entre eux : hôpitaux, cliniques, instituts de recherche, organismes payeurs, etc. l'hôpital est une structure associant plusieurs types d'unités : unités de soins, pharmacie, services administratifs médico-techniques et logistiques ([9 - Ch 11][10]). Chacune de ces unités a des fonctions et des ressources distinctes et est dotée d'une certaine autonomie. Suivant le même raisonnement, l'unité de soins, principal site d'accueil des patients, est définie comme étant une unité de lieu où est élaborée une stratégie thérapeutique, mise en œuvre par une équipe soignante (figure 4 et 5), en consommant des moyens (ressources) internes et

externes et susceptibles de fournir des prestations à d'autres unités. Il est donc essentiel de construire les groupes d'objets associés aux unités et de définir les droits d'accès, d'abord à l'équipe de l'unité, puis aux autres catégories d'utilisateurs qui interagissent avec l'unité.

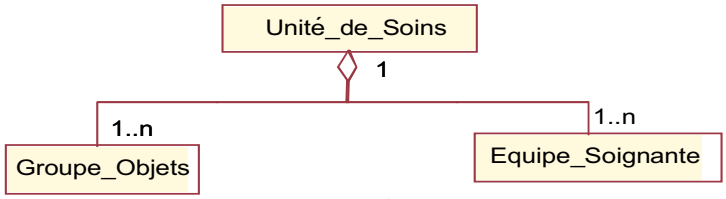



***Figure 4*** : Composition d'une unité (Notation UML : diagramme des classes)

### *II.2 Notion de processus de soins*

Une décision d'accès dépend du demandeur (rôle, attributs), mais aussi de l'utilisation prétendue des données. Cette utilisation est caractérisée par l'objectif de l'utilisation (voir III.3.4) ou par l'activité enregistrée dans le serveur et associant un certain nombre d'utilisateurs pour la réalisation d'un projet de soins ou d'une tâche globale. En effet, l'hôpital ne peut correctement fonctionner que s'il existe une coopération entre ces unités afin de traiter au mieux les patients. Conformément à la réalité, c'est le processus de soins qui assure la communication entre les unités de soins qui interagissent pour accomplir la fonction de soin ainsi que les fonctions subordonnées (figure 6). Par exemple, dans le cadre du processus soins en cours, le médecin X ($sujet_1$ de l'$unité_i$) ré alise un scanographe ($objet_1$) sur le patient ($objet_2$) et partage/envoie le résultat ($objet_3$) aux médecins Y de l'$unité_j$.

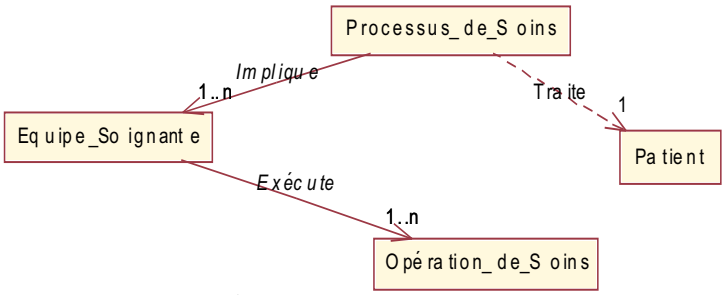



***Figure 6*** : Collaboration des unités dans un processus de soins (Notation UML : diagramme des classes)

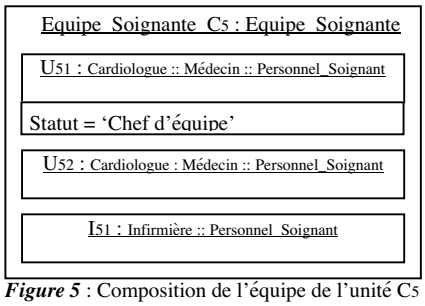



***Figure 5*** : Composition de l'équipe de l'unité C5

### *II.3 Différents types de dossiers médicaux*

Toute l'activité de l'unité de soins est organisée autour du patient. Le dossier du patient n'apparaît à un acteur de l'unité de soins que sous l'angle des besoins de sa tâche au sein de l'organisation. Chaque acteur ne sera donc concerné que par certaines informations du dossier. Nous citons : le dossier hospitalier, le dossier de spécialité, le dossier partageable, le dossier biologique, le dossier clinique, le dossier de transmission, le dossier minimum européen, le dossier d'archives [10]. Nous restreindrons notre étude aux dossiers suivants :

- Dossier partageable : ce dossier est dynamique (en cours d'élaboration). Il comprend l'histoire médicale actuelle du patient (les problèmes actifs) ainsi que les résultats provisoires et les avis temporaires. Il est le support, permettant aux professionnels de santé participant à un processus de soins, de communiquer les informations nécessaires.

- Dossier de spécialité : ce dossier est très spécifique à l'unité de soins. Sa constitution tient compte du plan de travail et des contraintes de l'unité à laquelle il appartient. Il existe une grande variabilité dans son contenu et dans la façon dont il est utilisé.

- Dossier archive : Contrairement au dossier partageable qui est dynamique, le dossier archive est stable. L'archivage implique un stockage de masse qui nécessite des mises à jour continuelles en relation avec les évolutions technologiques. Le dossier archive est alimenté par les résumés des dossiers partageables après fermeture de chaque processus de soins. En effet, le règlement des archives hospitalières impose des délais de conservation très longs : 70 ans pour les dossiers de pédiatrie, de neurologie, de stomatologie et de maladies "chroniques", illimités lorsqu'il s'agit de maladies héréditaires. Ce dossier comprend, outre l'identification du patient, des informations cliniques de synthèse, permettant de caractériser le type du séjour, les pathologies diagnostiquées, les traitements, la modalité de sortie et la façon dont le suivi de ce patient sera effectué. Ces données (ou une partie) sont souvent conservées chiffrées. À ne pas confondre avec les dossiers (anonymisés) utilisés dans le cadre du programme de médicalisation des systèmes d'information[1] « PMSI» [12].

Cette variété des parties et types des dossiers médicaux influence le contrôle d'accès. En effet, lorsque le patient se rend chez son médecin traitant, ce dernier ouvre un processus de soins (nommé parfois épisode de soins). Matériellement, cet épisode est figuré par le dossier partageable. Si le processus de soins est clôturé, un résumé du dossier partageable met à jour le dossier archive. En revanche, si durant le processus de soins, le patient est hospitalisé, il est traité dans le cadre d'un processus de soins où différentes équipes collaborent. Le dossier partageable ainsi que le dossier archive sont accessibles à l'ensemble des équipes du processus tandis que chacune des équipes possède un dossier de spécialité non accessible aux autres, et donc gérés localement au niveau des unités. Par ailleurs, le médecin traitant (psychologue, gynécologue) est le seul à posséder une partie privée (commentaire) où il met les données intimes que le patient ne veut pas partager avec une tierce personne. Cette partie n'est donc accessible que par le médecin et son patient (figure 7).

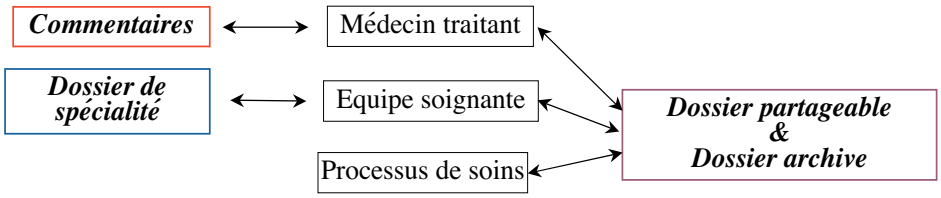



Figure 7 : Accès des différents types d'utilisateurs aux différents types de dossiers

# III. Notion de contexte

## *III.1 Vision générale sur le contexte*

Dans notre modèle, en plus des rôles et des groupes d'objets, nous tenons compte du contexte dans lequel la requête d'accès est faite. D'une manière générale, le contrôle d'accès basé sur le contexte peut être vu comme des réponses aux questions : qui, quand, pourquoi, où et comment ? posées pour chacune des entités, groupes, opérations et rôles du système [19] :

*Qui* : qui a le droit de travailler sur quel fichier (ou partie de fichier et/ou patient). Par exemple, le professionnel de soin engagé dans certains soins est autorisé à accéder à certaines informations. Accès limité à un utilisateur, rôle, agent ou équipe de soins. Qui peut déléguer, nommer, désigner ?

[1] Dans le cadre du PMSI, tout établissement de santé rend compte de son activité au moyen de résumés de séjour (RSS) pour les hospitalisations de court-séjour, et au moyen de résumés hebdomadaires (RHS) pour les séjours en soins de suite ou de réadaptation

*Quand* : Quand l'utilisateur a-t-il le droit d'accéder à une information ? Quand l'information est-elle disponible ?

*Où* : D'où l'accès aux informations est-il possible ?

*Comment* ? Comment accéder aux informations ? Comment l'information est-elle disponible ?

*Pourquoi* ? Pour quelles raisons les informations doivent-elles être disponibles : raison (but/objectif) de l'utilisation (fins scientifiques, épidémiologiques, médico-économique) ? quel est le processus concerné (soin du diabète, soin de grossesse, recherche, administration) ?

### *III.2 Types du contexte*

Le contexte est une notion générique dont l'utilisation peut parfois prêter à confusion. Le but de cette section est de le définir d'une manière précise. Par exemple, le lieu (variable contextuelle) peut être associé au rôle sous forme de contrainte (d'où le rôle peut-il être joué ?). Néanmoins, dans la réalité, les unités de soins possèdent, chacune, un ensemble d'unités mobiles (d'ordinateurs portables) que les Professionnels de santé qui y sont affectés utilisent simultanément (indépendamment de leurs rôles). En gros, quatre catégories de contexte peuvent être identifiées.

#### III.3.1 Contexte du rôle

En général, le contexte du rôle précise des valeurs que doivent prendre certaines variables contextuelles avant d'autoriser à un utilisateur de jouer un rôle donné. Par exemple :

- l'instant d'accès : le rôle médecin de salle est valide pendant les heures de travail tandis que le rôle médecin de nuit est valide la nuit [13];
- l'exclusion mutuelle entre rôles : elle peut être statique « un utilisateur ne peut jamais jouer les deux rôles ; par exemple, dans le même établissement, être personnel soignant et comptable », comme elle peut être dynamique « l'utilisateur ne peut pas jouer les deux rôles simultanément. Par exemple, médecin à l'hôpital et médecin travaillant pour une société d'assurance » ;

#### III.3.2 Contexte objet

Comme pour les rôles, les objet (ou les groupe d'objets passifs) ont des attributs contextuels spécifiques. Par exemple :

- La durée de conservation des données de neurologie, de maladies héréditaires, etc. ;
- le lieu : les dossiers de spécialités de chacune des unités sont gérés localement dans les ordinateurs de cette unité. Ainsi, les accès à ce type de dossier ne peut se faire que localement.

Selon l'organisation, les règles de priorité ainsi que les formalités (urgence, grève) peuvent être associées aux unités, comme elles peuvent être associées aux opérations d'accès.

#### III.3.3 Attributs d'utilisateurs

Les attributs décrivent des caractéristiques du genre : autorisations spécifiques, délégation à d'autres utilisateurs, droits temporaires, etc. Ces attributs sont parfois nécessaires pour l'exécution de certaines actions (dans des situations spécifiques). Dans les SICS par exemple :

- informations sur des qualifications : une spécialité avec une certaine expérience ; affiliation à un corps de santé régional, national ou international ;

- connaissances spécifiques : la capacité de pratiquer des consultations spécifiques (traitement à base de plantes, acuponcture) ou à utiliser certains types d'appareils (ultrason, rayon X, scanographe, prothèse dentaire) ;

- permissions particulières : le droit de travailler pour une autorité donnée ou pour une société d'assurance ; l'appartenance à un Ordre/chambre, etc.

Nous pouvons parfois considérer ces attributs comme particularités décrivant de nouveaux rôles (puisque en fin de compte, ces attributs donnent droit à d'autres permissions, et inversement, le rôle peuvent être implémentés comme des attributs des utilisateurs). Néanmoins, nous préférons les considérer comme attributs d'utilisateurs pour deux raisons : leur nature temporaire et non définitive ; elles doivent souvent être couplés avec certains rôles avant de déduire les privilèges de l'utilisateur.

### III.3.4 Objectif d'utilisation

Les ressources des SICS peuvent être invoquées par différents utilisateurs et pour différentes raisons. Il faut surtout réaliser un compromis entre le respect du **moindre privilège**[2] et la **flexibilité**[3] du contrôle d'accès, de façon à favoriser l'intérêt des patients. Les obligations éthiques et déontologiques affirment que les données ne peuvent être exploitées que pour les raisons pour lesquelles elles ont été collectées. Les privilèges d'une utilisation pour des fins épidémiologiques, différentes de ceux dont la finalité est commerciale et/ou de recherche et/ou statistique. Certaines utilisations nécessitent le consentement du patient, d'autres, parfois plus urgentes, tiennent compte de l'objectif[4] mentionné et accordent l'accès avec une responsabilité plus élevée. Pour illustrer cette notion, nous citons les exemples suivants :

- Afin de favoriser la flexibilité, on peut éditer une règle qui autorise au médecin qui a déjà traité (au passé) un patient de réaccéder à son fichier, à condition qu'il spécifie l'objectif derrière cette utilisation : « révision du diagnostic, vérification ». Cet objectif sera le point essentiel de l'autorisation et déclenchera automatiquement un audit de haut niveau (traçabilité) ou même l'envoi d'une notification au patient.

- Dans un cas d'urgence, certains rôles peuvent déclarer l'objectif « traitement d'urgence » et s'accorder des privilèges en assumant leur responsabilité. L'accès sera validé par des valeurs que prendront certaines variables de l'environnement (service des urgences ; patient touché dans un organe vital ; et/ou manque de personnel).

- Autoriser l'accès aux données des patients, à un centre hospitalier universitaire, à d'autres institutions de santé ou à certains partenaires pour des sujets de recherche ou d'aide au diagnostique. Selon le but mentionné (et le rôle), le système n'autorisera l'accès qu'aux données anonymes et/ou ordonnera le consentement du patient et/ou de sa famille et/ou du médecin traitant.

- Les règles de priorités peuvent tenir compte, entre autres, de l'objectif de l'utilisation. Par exemple dans une unité de soin, l'objectif « urgence » sera favorisé par rapport à l'objectif « paiement ».

Pour résumer, le but de l'objectif de l'utilisation est d'assurer la flexibilité tout en déterminant la responsabilité de l'utilisateur et en servant d'argument en cas d'abus de pouvoir ou de conflit.

---

[2] Ne donner accès qu'aux utilisateurs autorisés et seulement aux ressources dont ils ont besoin pour accomplir leurs tâches

[3] Ne pas laisser hypothéquer les bénéfices potentiels par des limites qui seraient destinées plus à verrouiller qu'à sécuriser le système.

[4] La notion d'objectif d'utilisation a été utilisé dans [14] « en anglais : *purpose* » mais son utilisation est différente de la nôtre.

# IV. Représentation en logique déontique

### *V.1 Intérêt d'une approche formelle*

Le choix d'une approche formelle est justifié par les points suivants :

- Lever l'ambiguïté et le manque de précision souvent rencontrés lors de l'utilisation du langage naturel ;
- Possibilité de manipuler la spécification par des transformations mathématiques et avec l'assistance des outils de preuve ;
- Vérification de la consistance interne des objectifs de sécurité ainsi que la cohérence et la complétude de la politique de sécurité ;
- Validation, détection des conflits, preuve formelle, contrôle statistique….

La logique déontique fournie les notions de permission « $\mathbf{P}$ », d'obligation « $\mathbf{O}$ » et d'interdiction « $\mathbf{F}$[5] ».

### *V.2 Extension du langage déontique*

Le langage déontique [20] est adéquat pour la représentation des règles de sécurité. Néanmoins, la nécessité de détailler toutes les propositions atomiques nécessaires pour construire la spécification ainsi que toutes les formules associées peut introduire une certaine lourdeur. Ce problème est d'autant plus complexe car le système de santé est très riche en termes d'entités et de scénarios. Dans le but de faciliter la tâche de spécification et de profiter de la hiérarchie des classes (rôles et groupes), nous nous inspirons de l'extension fournie dans [15] [16]. Cette extension, *purement syntaxique* et dont l'intérêt réside dans la possibilité de *structurer les propositions* atomiques, considère le langage $L(\Pi)$ désigné par l'ensemble des formules $f$ construis par les règles : $f := A \mid \neg f \mid f \vee f \mid f \wedge f \mid f \rightarrow f \mid f \leftrightarrow f \mid \mathbf{O}_f \mid \mathbf{P}_f \mid \mathbf{F}_f$. Avec : $A$ un élément de $\Pi$, et $\Pi$ un ensemble d'ensembles finis, ordonné par la relation d'ordre partiel d'inclusion. Par ailleurs, afin de faciliter la construction des éléments de $\Pi$, nous utilisons le produit cardinal défini par : $E \times R = \{ (e,r) / e \in E , r \in R \}$.

Nous considérons l'ensemble $\Phi_\Pi$ constitué par les ensembles terminaux de $\Pi$, qui ne contiennent pas d'autres éléments (ensembles) et constituent donc la base de la hiérarchie définie par la relation d'inclusion : $\Phi_\Pi = \{E \in \Pi / (\forall R \in \Pi , \ R \not\subset E)\}$. Ainsi, une formule de $L(\Pi)$ correspond à une notation synthétique de plusieurs formules de $L(\Phi_\Pi)$ qui sont celles que l'on peut obtenir en remplaçant dans « $f$ » toutes les occurrences d'ensembles non terminaux de $\Pi$ par leur contenu, jusqu'à obtenir uniquement les éléments de $\Phi_\Pi$. Par exemple, la formule $\mathbf{P}(A \vee B)$ de $L(\Pi)$ sera exprimée, en $L(\Phi_\Pi)$ par l'ensemble des formules : $\{\mathbf{P}(q \vee r) / q \in A; r \in B\}$, ce qui signifie que si $\mathbf{P}(A \vee B)$ est vrai dans un monde $w$, toutes les formules $\mathbf{P}(q \vee r)$ telles que $q \in A$ et $r \in B$ sont vraies dans $w$.

Cette extension va nous faciliter la spécification en nous permettant d'abord, de définir progressivement et hiérarchiquement les différentes propositions atomiques du langage grâce aux différents ensembles « rôles et groupes d'objets », et ensuite d'utiliser directement ces ensembles pour rédiger les formules logiques décrivant la politique de sécurité. Si le même ensemble apparaît plusieurs fois dans la même formule, il désigne le même élément. Par exemple la formule

---

[5] $\mathbf{F}p = \mathbf{O}\neg p$ *et* $\mathbf{P}p = \neg\mathbf{O}\neg p = \neg\mathbf{F}p$

de $L(\Pi)$: $A \wedge B \vee C \wedge B$ désigne dans $L(\Phi_\Pi)$ $\forall p \in A\ \forall q \in B\ \forall r \in C\ p \wedge q \vee r \wedge q$. Par contre, si nous voulons désigner deux éléments distincts dans « $B$», la formule de $L(\Pi)$ sera : $A \wedge B \vee C \wedge \beta$ de façon à ce que « $\beta$ » représentera une copie de « $B$».

La sémantique associée à l'extension ainsi définie est la sémantique de Kripke avec une petite modification au niveau de la relation d'accessibilité. Un modèle de Kripke est un triplet $\langle W,R,V \rangle$ où $W$ est un ensemble de mondes possibles $w$; $R$ est une relation d'accessibilité et la fonction $V : W \times \Phi_\Pi \rightarrow \{ Vrai , Faux \}$ qui donne pour chaque monde $w \in W$ la valeur de vérité $V$ ( $w$ , $A$ ) de l'ensemble $A$. Une Formule du type « F$p$» (il est interdit que p) indique qu'aucun des mondes accessibles dans le modèle ne doit permettre de conclure que $p$ est vraie dans ce monde. La formule « P$p$» (il est permis que p) au contraire, signifie qu'à partir de n'importe quel des mondes, on doit pouvoir atteindre un monde dans lequel $p$ est vraie.

# V. Exemple de spécification en logique

### *VI.1 Éléments de base*

Nous nous intéressons aux principaux éléments de description utilisés pour définir les objectifs et les règles de sécurité de la spécification. La première étape consiste donc à construire $\Pi$ en énumérant les sujets et les objets, les rôles et les groupes d'objets, les permissions et les opérations, mais également en utilisant le produit cardinal pour établir les associations (utilisateurs, rôle, équipe) « désignant les rôles que l'utilisateur peut jouer dans chacune de ses équipes », (objet, groupe), hiérarchie de rôles et de groupes. Dans le cas général, tous les éléments de structuration doivent être instanciés, (il faut définir toutes les instances des utilisateurs, des machines, des rôles).

#### VI.1.1 Entités

*a) ROLES*

- *Organisationnels* : patient, tuteur, médecin traitant, médecin de consultation, médecin de salle, médecin de garde, médecin du département d'information médicale (DIM), médecin chef de l'hôpital, chef de service, interne, résident, infirmière, cadre infirmier, aide-soignante, employé d'accueil, secrétaire médicale, chercheur, agent de santé publique. Ces rôles doivent être instanciés, autrement dit, il faut définir des relations du type : $P1 \times Patient , P2 \times Patient$, $M1 \times Médecin$, $S1 \times SecrétareMédicale$, ….

- *Abstraits* : personnel soignant, personnel paramédical, personnel de pharmacie, personnel de laboratoire.

*b) OPERATIONS*

- *De bas niveau* : créer, lire, ajouter « append », modifier « update », copier/télécharger/importer, supprimer, insérer carte, fournir, accéder.

- *De haut niveau* : collecter des données de diagnostique, demander des examens indispensables ou complémentaires, poser diagnostique, prescrire, consulter, rédiger, chiffrer, anonymiser, transmettre/exporter, valider/signer, imprimer ainsi que toutes les délégation possibles.

*c) CLASSES D'OBJETS*

Types de dossiers médicaux

- Dossier partageable (en cours d'élaborations)

- Dossier médical archivé : ce dossier est composé des résumés : cliniques, infirmiers, psychiatriques, gériatriques, financiers et sociaux.
- Dossier médical anonymisé : résumés de séjour (RSS) ; résumés hebdomadaires (RHS).

Classes d'autres documents

- Accord du tuteur
- consentement du patient

*d) OBJECTIFS D'UTILISATION*

Recherche scientifique, soins, révision du diagnostique, aide au diagnostique, non-commercial, urgence (vie du patient en danger, manque de personnel, grève), prévention, évaluation médico-économique.

*e) UNITES*

- Urgences : $UR_1$, $UR_2$, …
- Consultations externes $CE_1$, $CE_2$, $CE_3$, …
- Départements spécialisés : Médecine ($M_1$, $M_2$), Chirurgie ($C_1$, $C_5$), Gynécologie ($G_1$), Pédiatrie ($P_1$), Anesthésie ($A_1$, $A_3$), Radiologie ($R_1$, $R_2$), Réadaptation.

*f) GROUPES D'OBJETS*

- Selon le type des données : données cliniques, données d'urgences (nom du médecin traitant, groupe sanguin, temps du facteur K, allergies), données d'identité (nom, prénom, sexe, date de naissance, numéro de téléphone, lieu de travail, nationalité), données paramédicales, données financières, données statistiques.
- Matériel, médicament, postes de travail, salles, etc.
- Données et ressources propres à l'hôpital et à chacune des unités et services.

### VI.1.2 Associations

$AU \subseteq User \times Rôle$ est une relation plusieurs à plusieurs associant les utilisateurs aux rôles ;

$AE \subseteq User \times Equipe$ (plusieurs à plusieurs) désigne l'appartenance des utilisateurs aux équipes ;

$AU_{(R,E)} = \{(u,r,e) / u \in User, r \in Rôle, e \in Equipe\}$ les rôles qu'un utilisateur peut jouer dans une équipe ;

$AO \subseteq Objet \times Groupe$ (plusieurs à plusieurs) désigne l'appartenance des objets aux groupes ;

$AU_S \subseteq Equipe \times Groupe \times Unité\_Soins$ Associant les équipes et les groupes d'objets aux unités de soins;

Hiérarchie de rôles : $HR \subseteq Rôle \times Rôle$ ; Hiérarchie de groupes : $HG_R \subseteq Groupe \times Groupe$

Entre groupe d'objets et opérations : $AO_p \subseteq \texttt{Opération} \times Groupe$ ;

Le processus de soins réuni un ensemble d'équipes et donne, à chacune des équipes, le droit de réaliser certaines opérations sur certains groupes d'objets : $Aproc \subseteq (\texttt{Opération}^* \times Equipe \times Groupe)^*$

Exemples d'associations exprimées dans $L(\Phi_\Pi)$ :

( $U_{01}$, *Médecin_de_Nuit* , $U_{R4}$ ), instance de la relation $U \times R \times U_S$ : l'utilisateur ayant comme identifiant « U01 » et jouant le rôle « médecin de nuit » au seins de l'unité de soins d'urgence « UR4 ».

$(U_2, Médecin\_Chef, Hôpital\_de\_Rangueil)$ : U2 joue le rôle médecin chef de l'hôpital de Rangueil.

### *VI.2 Règles de fonctionnement*

Le but de la spécification des règles de fonctionnement et des règles de sécurité est de définir les différents flux d'informations et les contrôles de sécurité. Cette étape doit s'appuyer sur les éléments structurants définis précédemment (rôles, groupe, contexte) tout en les raffinant et en précisant leur contenu. Il ne s'agit de représenter que le fonctionnement (activation des rôles, enchaînement des actions) pertinent vis-à-vis de la sécurité afin de pouvoir ultérieurement déterminer l'impact sur les objectifs de sécurité. La description se fait dans le langage $L(\Pi)$, par le biais des différents opérateurs de la logique propositionnelle. Au niveau de la sémantique, les règles de fonctionnement définissent la structure interne des mondes de Kripke associé à la spécification. Ce sont en effet, des axiomes ne contenant pas des opérateurs modaux. Ils n'ont donc aucun impact sur les caractéristiques de la relation $R$ entre les mondes du modèle. En revanche, chaque monde est tel qu'il constitue un état de fait compatible avec les règles de fonctionnement. Ainsi, si nous avons défini une règle du type $q \Rightarrow r$, tout monde « $w$ » où « $q$ » est vraie, « $r$ » le sera aussi.

***Activation des rôles***

Les règles d'activation des rôles sont de types : ***Si*** *condition* ***alors*** *l'utilisateur a le droit de jouer le rôle*. La règle $(\texttt{Fournir} \times User \times Certificat\_de\_Santé) \vee (\texttt{Se\_Loguer} \times User \times CPS) \rightarrow User \times PS$ signifie que si un utilisateur (user) possède un certificat délivré par une autorité de santé ou s'il se logue pas sa carte professionnelle de santé (CPS), il a le droit de jouer le rôle professionnel de santé (PS). Les opérations « `Fournir` » et « `se Loguer` » sont des propositions atomiques.

***Hiérarchie de rôles***

La structure hiérarchique de la figure est représentée par les règles suivantes :

$Médecin \vee Personnel\_Infirmier \vee Aide\_Signante \rightarrow Personnel\_Soignant$

$P\_Soignant \vee Personnel\_Paramédical \vee P\_Administratif \vee P\_Hôtelier \rightarrow Professionnel\_Santé$

$Personnel\_Pharmacie \vee Personnel\_Laboratoire\_Analyses\_Médicales \rightarrow Personnel\_Paramédical$

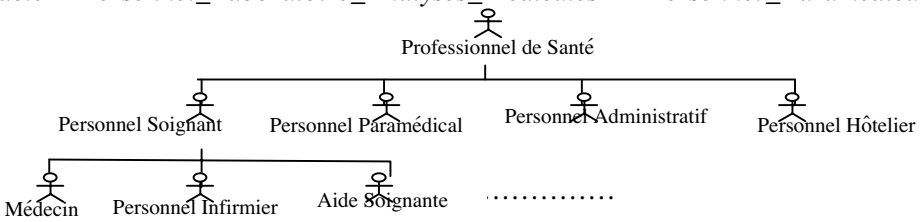



***Figure 8 :*** Hiérarchie de rôles

***Contexte de rôles***

$\texttt{Se\_Loguer} \times (User \times Médecin) \times Nuit \rightarrow User \times Médecin\_de\_Nuit \wedge \neg(User \times Médecin\_de\_Salle)$ signifie que si, pendant la nuit, l'utilisateur se logue avec le rôle médecin, il a le droit de jouer le rôle médecin de nuit et il n'a pas le droit de jouer le rôle médecin de salle (exclusion mutuelle).

### *VI.3 Objectifs de sécurité*

Les objectifs de sécurité sont exprimés en utilisant les opérateurs modaux. Ces opérateurs permettent de modifier les propriétés de la relation d'accessibilité $R$ entre les différents mondes du modèle. Ils indiquent si deux mondes doivent être accessibles l'un depuis l'autre. Par exemple, la formule $\mathbf{P}p$ indique qu'à partir de n'importe quel monde, on doit pouvoir atteindre un monde dans lequel $p$ est vraie ; la formule $\mathbf{F}p$ signifie qu'aucun des mondes accessibles dans le modèle ne doit permettre de conclure que $p$ est vraie dans ce modèle. Dans notre système, nous pouvons identifier des objectifs de sécurité du type :

1. $\mathbf{F}(\texttt{Prescrire} \times \textit{Pharmacien} \times \textit{Médicament})$
2. $\mathbf{P}(\texttt{L}\textit{ire} \times \textit{Pharmacien} \times \textit{Dossier\_Farmaceutique})$
3. $\mathbf{P}(\texttt{Accès} \times \textit{Agent\_Assurance} \times \textit{Donnée\_Financières})$
4. $\mathbf{P}(\texttt{Modifier} \times \textit{Agent\_Santé\_Publique} \times \textit{Donnée\_Statistique})$
5. $\mathbf{F}((\texttt{Modifier} \vee \texttt{Copier}) \times \textit{Médecin\_Consultation} \times \textit{Dossier} \times \textit{Patient})$
6. $\mathbf{P}(\texttt{Accès} \times \textit{Chercheur} \times \textit{Donnée\_Statistique}) \wedge \mathbf{P}(\texttt{Accès} \times \textit{Chercheur} \times (\textit{Donnée\_Médical} \wedge \neg \textit{Identité})$
7. $F(\textit{Transmettre} \times (\textit{Données} \times \textit{Patient})) \wedge (\textit{Destination} \times \textit{Liste\_Noire})$

Les deux premiers objectifs autorisent au pharmacien de lire le dossier pharmaceutique sans pouvoir prescrire des médicaments. Le troisième (resp. quatrième) objectif autorise aux agents des services payeurs (resp. de santé publique) d'accéder aux données financières (resp. statistiques). Le cinquième interdit au médecin de consultation de modifier ou de copier les dossiers des patients. Le sixième objectif autorise aux chercheurs des institues médicaux d'accèder aux données statistiques (médico-économiques) et aux données anonymes. Le dernier objectif interdit la transmission des données personnelles aux pays figurants dans une liste noire (les pays ne disposant pas d'une législation de protection des données).

### *VI.4 Règles de sécurité*

Du point de vue formel, une règle de sécurité est une formule modale dont les différentes clauses ne sont pas toutes des formules modales, par exemple $r \rightarrow \mathbf{P}q$. Dans ce cas, la règle précise une relation logique entre l'état existant dans un monde et les règles déontiques qui s'appliquent.

1. $\textit{Personnel\_Soignant} \times \textit{Urgence} \rightarrow \mathbf{P}\left(\texttt{Accèder} \times \textit{PS} \times \textit{Données\_Nominatives}\right) \wedge \mathbf{O}\left(\texttt{Activer} \times \textit{Système} \times \textit{Audit}\right)$
2. $\textit{Dossier} \times \textit{Patient} \rightarrow \mathbf{P}\left(\texttt{Lire} \times \textit{Patient} \times \textit{Dossier}\right)$
3. $\textit{Personnel\_Soignant} \times \textit{Unité\_Soins} \rightarrow \mathbf{P}\left(\texttt{Accès} \times \textit{Personnel\_Soignant} \times \left(\textit{Dossier\_Spécialité} \times \textit{Unité\_Soins}\right)\right)$
4. $\texttt{Transmettre} \times \textit{Biologiste} \times \textit{Résultat} \rightarrow \mathbf{O}\left[\texttt{Chiffrer} \times \textit{Système} \times \left((\textit{Identité} \times \textit{Patient}) \wedge (\textit{Identité} \times \textit{Médecin}) \wedge (\textit{Code} \times \textit{Laboratoire})\right)\right]$
5. $\mathbf{P}\left(\texttt{Opération\_de\_soin} \times \textit{User}\right) \rightarrow \textit{User} \times \textit{Personnel\_Soignant}$
6. $\mathbf{P}\left(\texttt{Transmettre} \times \textit{User} \times \textit{RSA} \times (\textit{Direction\_Hôp} \vee \textit{Agence\_Régionale} \vee \textit{Assurance} \vee \textit{Ministère})\right) \rightarrow \textit{User} \times \textit{Méd\_DIM}$
7. $\mathbf{P}\left(\texttt{Rédiger} \times \textit{User} \times \textit{Rapport\_Infirmier}\right) \rightarrow \textit{User} \times \textit{Personnel\_Infirmier}$
8. $(\textit{Dossier} \times \textit{Patient}) \wedge (\textit{User} \times \textit{Méd\_Trait}) \rightarrow \mathbf{P}((\texttt{Poser\_Diag} \wedge \texttt{Demander\_Test} \wedge \texttt{Prescrire}) \times \textit{User} \times \textit{Dossier})$
9. $\textit{Utilisateur} \times \textit{Médecin} \times \textit{Réviser\_Diagnostic} \rightarrow \textit{Utilisateur} \times \textit{Traitement\_antécédent} \wedge O(\textit{Lancer} \times \textit{Audit})$

10. $(Dossier \times Patient) \wedge (Patient \times Tuteur) \wedge (Patient \times Consentement) \rightarrow \mathbf{P}(\texttt{Lire} \times Tuteur \times Dossier)$

11. $User \times Med\_Trait \times Patient \rightarrow \mathbf{P}(\texttt{Désigner} \times User \times (User^{1} \times Méd\_Consult \times Patient))$

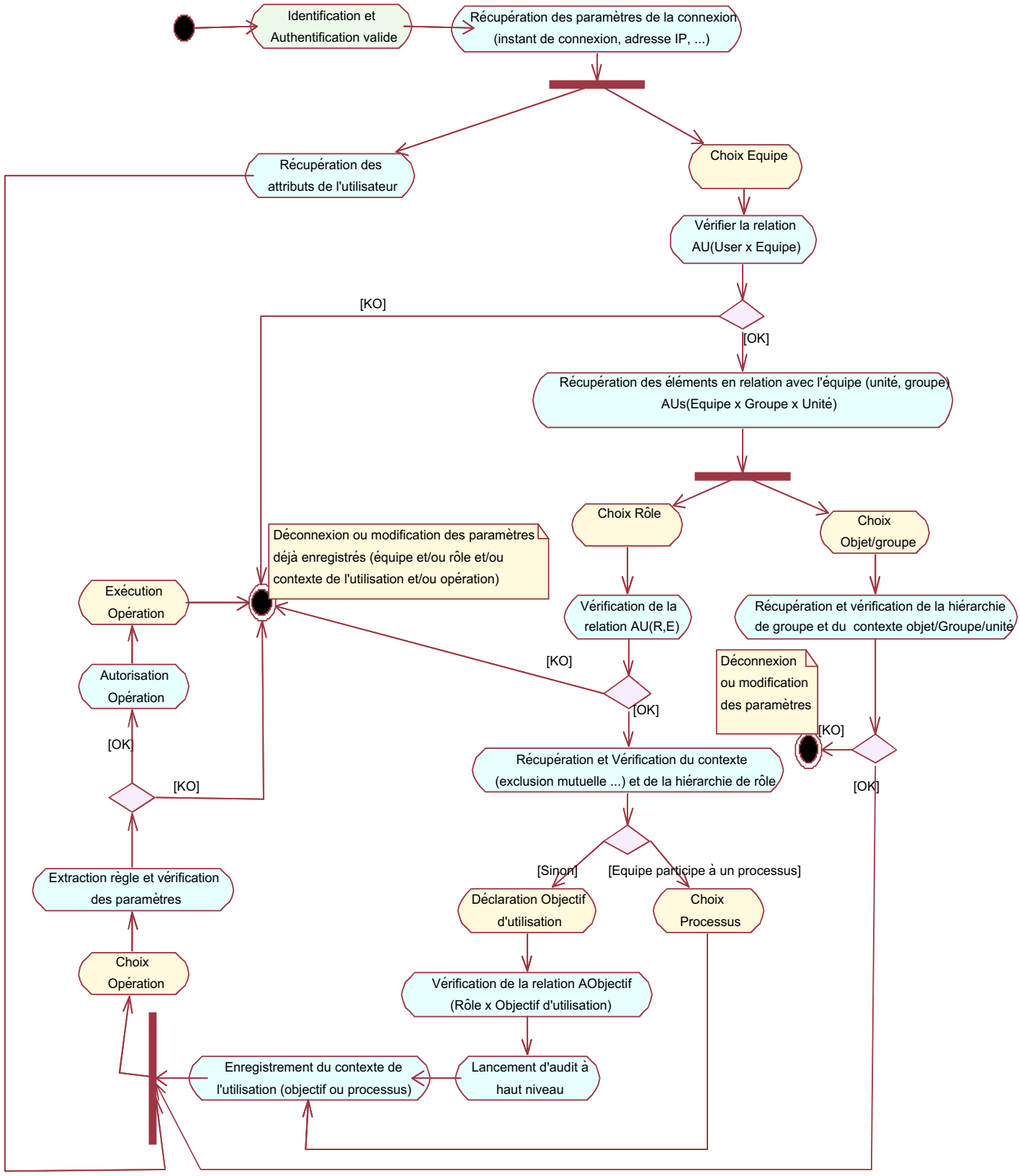
La première règle exprime le fait qu'en cas d'urgence, un professionnel soignant a le droit d'accéder aux données nominatives. En parallèle, le système enregistrera les paramètres de l'accès dans le fichier d'audit. La deuxième règle donne au patient la permission de lire son dossier. La troisième signifie que si un professionnel soignant travaille dans une unité de soins, il a le droit d'accéder aux dossiers de spécialités de cette unité. La quatrième oblige le système de chiffrer (au moins) l'identité du patient, celle du médecin et le code du laboratoire avant toute transmission des résultats biologiques. La cinquième exprime que tout personnel soignant a le droit d'effectuer des opérations de soins. La sixième explique les principales missions du médecin responsable du Département d'Information médicale (Méd_DIM) : transmission des résumés de sortie anonymes (RSA) à la direction de l'établissement ainsi qu'aux Agences régionales d'hospitalisation, aux directions régionales des affaires sanitaires et sociales, aux Caisses régionales d'Assurance Maladie et au ministère de la santé.

## VI. Scénario

L'utilisateur commence par s'identifier et s'authentifier. Le système récupère ses attributs et lui propose de choisir une équipe. Une fois l'équipe choisie, le système récupère le contexte de l'équipe et son unité de rattachement. En fonction de ces paramètres, le système lui demande de choisir l'objet (ou le groupe d'objet) sur lequel il veut effectuer des opérations, ainsi que le (s) rôle (s) qu'il veut jouer (parmi les rôles qu'ils peut jouer dans l'équipe choisie). À ce niveau, un contrôle du contexte du rôle (exclusion mutuelle) est effectué. Le système propose à l'utilisateur, de choisir le processus de soins ou de déclarer, dans des cas particuliers et bien définis, un objectif d'utilisation. Les processus de soins possibles sont ceux enregistrés dans le serveur et auxquels son équipe participe (voir figure 8 : diagramme d'activités en notation UML).

## Conclusion

Nous avons présenté un modèle se basant sur une utilisation croisée des rôles et des groupes d'objets comme étant deux moyens de structuration assez flexible qui se complètent pour supporter la richesse des SICS. De la même manière que le rôle lie les utilisateurs aux privilèges, les groupes d'objets permettent d'établir une relation entre les opérations et les objets à protéger. Nous avons également cadré la notion de contexte afin de permettre un contrôle d'accès respectant le principe du moindre privilège tout en garantissant une flexibilité favorisant le profit des patients. Dans la dernière partie de notre papier, nous avons proposé un scénario d'accès ainsi qu'une liste significative mais non exhaustive des règles de sécurité, règles de fonctionnement et objectifs de sécurité, exprimés par une extension du langage déontique. Dans nos perspectives, nous envisageons d'enrichir notre politique et l'améliorer afin de satisfaire les besoins de sécurité élevés, et plus précisément de couvrir la propriété de disponibilité, avant de définir des méthodes de raisonnement automatique sur ses concepts et de passer à l'expérimentation.


Identification et Authentification valide
Récupération des paramètres de la connexion (instant de connexion, adresse IP, ...)
Récupération des attributs de l'utilisateur
Choix Equipe
Vérifier la relation AU(User x Equipe)
[KO]
[OK]
Récupération des éléments en relation avec l'équipe (unité, groupe) AUs(Equipe x Groupe x Unité)
Choix Rôle
Choix Objet/groupe
Déconnexion ou modification des paramètres déjà enregistrés (équipe et/ou rôle et/ou contexte de l'utilisation et/ou opération)
Exécution Opération
Vérification de la relation AU(R,E)
Récupération et vérification de la hiérarchie de groupe et du contexte objet/Groupe/unité
[KO]
[OK]
Autorisation Opération
Déconnexion ou modification des paramètres
[KO]
[OK]
[OK]
[KO]
Récupération et Vérification du contexte (exclusion mutuelle ...) et de la hiérarchie de rôle
Extraction règle et vérification des paramètres
[Sinon]
[Equipe participe à un processus]
Déclaration Objectif d'utilisation
Choix Processus
Choix Opération
Vérification de la relation AObjectif (Rôle x Objectif d'utilisation)
Enregistrement du contexte de l'utilisation (objectif ou processus)
Lancement d'audit à haut niveau

## Remerciements

Cette étude est partiellement soutenue par le Réseau National de Recherche en Télécommunications (RNRT) dans le cadre du projet MP6 (*Modèles et Politiques de Sécurité pour les Systèmes d'Informations et de Communications en Santé et Social*), dont les partenaires sont : Ernst & Young Audit, ENST-Bretagne, ETIAM, France Telecom R&D, LAAS-CNRS, MasterSecuritY, ONERA-DTIM, Supélec-Rennes, UPS-IRIT. Elle entre également dans le cadre des travaux du projet « Sécurité Informatique » de FéRIA, la Fédération de Recherche en Informatique et Automatique de Toulouse. Les auteurs remercient en particulier Philippe Balbiani pour sa contribution.

## Références

[1] Abou El Kalam A., "Politiques de sécurité pour les systèmes d'informations médicales", *Journées Doctorales en Informatique et Réseaux (JDIR)*, Toulouse, France, 4-6 Mars 2002, pp 201-210.

[2] D.E.Bell, L.J.LaPadula, *Secure Computer Systems : Unified Exposition and Multics Interpretation*,The MITRE corporation TechnicalReport, ESD-TR-73-306, 1975.

[3] K.J.Biba, *Integrity Consideration for Secure Computer Systems*, The MITRE Corporation, TechnicalReport, ESD-TR-76-372 & MTR-3153, 1977.

[4] D.Clark, D.Wilson, "A comparison of Commercial and Military Computer Security Policies", *IEEESymposium on Security and Privacy*, Oakland, California, April 27-29, 1987, pp.184-194.

[5] D.Brewer, M.Nash, "The Chinese Wall security policy", *IEEE Symposium on Security and Privacy,Oakland, California*, May 1-3, 1989, pp 206-214.

[6] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, "Role-Based Access Control Models", *IEEEComputer*, vol.29, pp.38-47, February, 1996.

[7] S.H.v.Solms et al. ; "The management of computer security profiles using a role-oriented approach",*Computer & Security*, vol.13, n°8, pp. 673-680,1994.

[8] Roshan K.Thomas, "TMAC : A primitive for Applying RBAC in collaborative environement", *2nd ACM, Workshop on RBAC*, FairFax, Virginia, USA, November 6-7, 1997.

[9] Degoulet P., Fieschi M., "*Traitement de l'information médicale - Méthodes et applications hospitalières*", Springer-Verlag France.

[10] P. Degoulet, J.-C. Stéphan, A. Venot et P.-J. Yvon, "*Informatique et Gestion des Unités de Soins - Informatique et Santé - Volume 1*", Springer-Verlag France, juin 1989.

Disponible à : http://www.cybermed.jussieu.fr/Broussais/InforMed/InforSante/Volume1/Volume1.html

[11] Mohr D.N., Carpenter P.C., Claus P.L., Hagen P.T., Karsell P.R., Van Scay R.E. "Implementing an Electronic Medical Record : Paper's last Hurrah", 995, pp 157-161.

[12] Riandey B., "Appariements sécurisés et statistique publique", Séminaire de la société Française de Statistique, 28 Février 2001.

Disponible à : www.sfds.asso.fr/groupes/CRappariements.PDF

[13] M. Willikens, S. Feriti, M. Masera, "A Context-related autorisation and access control method based on RBAC", *ACM Symposium on Access Control Models and Technologies, (SACMAT'02)*, California, U.S.A. June 3-4, 2002.

[14] P. Bonatti, E. Damiani, S. di Vimercati, P. Samarati, "An access Control Model for data archives", IFIP TC11 in 16th International Conference on Information Security (IFIP/SEC'01), Paris, France, June 11-13, 2001.

[15] R. Ortalo, "A Flaxible Method for Information System Security Policy Specification", in *5th European Symposium on Research in Computer Security (ESORICS 98)*, Louvain-La-Neuve, Belgique, September 16-18, 1998, Springer-Verlag, pp 67-84.

[16] R. Ortalo, Y. Deswarte, "Management of Information System Security Specification and Assessment", in *14th InternationalConference on Advanced Science and Thechnology (ICAST'98)*, Naperville, Illinois, USA, Appril 3-4 1998, pp 207-221.

[17] G. Booch, J. Rumbaugh, I.Jacobson, "*The Unified Modeling Language User Guide*", 1999, Addison Wesley, ISBN 0-201-57168-4.

[19] La norme Européenne CEN/TC 251 : prENV 13606-3: Health informatics – Electronic, 17 décembre1999.

[20] B.F. Chellas, "*Modal Logic : An Introduction*", 295p., Cambridge University Press, 1980, ISBN 0-521-29515-7.