Amélioration de la politique de sécurité des systèmes DRM

introduction des notions du modèle Or-BAC dans le langage MPEG-21 REL

Mourad Rafi
École Mohammedia d'Ingénieurs, Univ. Mohammed V-Agdal, Av. Ibn Sina B.P. 765 Agdal Rabat, Maroc
rafimourad@gmail.com

Mohcine Eleuldj
École Mohammedia d'Ingénieurs, Univ. Mohammed V-Agdal, Av. Ibn Sina B.P. 765 Agdal Rabat, Maroc
eleuldj@emi.ac.ma

Résumé

Le DRM (Digital Rights Management) ou la gestion des droits numériques a pour rôle le contrôle d'accès et l'utilisation des contenus numériques produits par les détenteurs de droit d'auteur. Pour ce faire, un langage d'expression des droits est nécessaire. Le langage MPEG-21 REL est le standard adopté pour exprimer les licences. On propose dans cet article l'amélioration de la politique de sécurité des systèmes DRM et de l'expressivité du langage MPEG-21 REL par l'introduction de concepts inspirés du modèle de données Or-BAC (Organization Based Access Control). Cette amélioration sera illustrée par des exemples de scénarios d'usage.

Abstract

Digital Rights Management (DRM) allows controlling the access, the use and the diffusion of digital contents produced by the rights holders. With this intention, a right expression language is necessary. The MPEG-21 REL is a standardized language used to express the licenses. In this paper, we propose an improvement of the security policy and expressivity of MPEG-21 REL by introducing concepts based on the Or-BAC (Organization Based Access Control) data model. This improvement will be illustrated by some use cases.

Mots-clés

MPEG-21 REL, DRM, Or-RBAC, Licences, politique de sécurité

Keywords

MPEG-21 REL, DRM, Or-BAC, Licenses, security policy

1. Introduction

Les progrès récents des technologies numériques, particulièrement en ce qui concerne la vitesse et les capacités d'Internet, transforment les domaines de l'éducation, de la médecine, des services gouvernementaux, du commerce, du divertissement et des affaires. Les utilisateurs ne sont plus limités par le temps et les contraintes d'espace, ils peuvent accéder au contenu numérique par le biais des téléphones intelligents, PDA, téléphones mobiles, *etc.*
Placé au cœur de l'économie numérique, le DRM (*Digital Rights Management*) (Reihanah et Moti, 2006) (DRM, 2013), autrement dit la gestion des droits numériques (GDN), est appelé à répondre aux exigences de contrôle d'accès, de l'usage et de la diffusion de tout contenu numérique. Toutefois, le nombre accru d'usagers et la diversité d'accès aux ressources d'information rendent la gestion des droits numériques plus difficile.
Plusieurs études ont été consacrées au contrôle d'accès à base des méthodes *Role-Based* Access Control (RBAC) (Gavrila

et Barkley, 1996) (Ferraiolo, Sandhu *et al.*, 2001), afin de rendre possible la gestion d'un grand nombre d'utilisateurs, tout en assurant la sécurité et le contrôle d'usage.
Le RBAC traditionnel ne prend pas en compte l'adéquation des rôles et permissions de l'utilisateur avec son environnement et son contexte de travail, ni l'organisation dont il fait partie. Un mécanisme de contrôle d'accès aux contenus numériques doit être souple dans l'octroi des autorisations aux utilisateurs selon le contexte. Une combinaison des informations contextuelle et organisationnelle de l'utilisateur avec un mécanisme de type *Role-Based* Access Control permettra de doter les systèmes DRM des mécanismes d'octroi des rôles et permissions d'une façon dynamique et efficace. Ainsi, les systèmes DRM peuvent-ils ajuster dynamiquement, dans le temps et selon le contexte, les autorisations pour un contrôle plus approprié.
Àfin de satisfaire à ces exigences, il est nécessaire de spécifier les règles énonçant les conditions d'utilisation d'un contenu numérique et d'apporter les outils nécessaires. Ces règles sont souvent exprimées sous la forme d'une licence qui est une sorte de contrat entre un fournisseur d'une ressource numérique et un consommateur. Les langages d'expression des droits (Sans et Cuppens, 2004), en anglais *Rights Expressions Language* (REL), sont une partie intégrante des technologies des systèmes DRM. Parmi les langages les plus utilisés, on trouve les standards : MPEG 21 REL et ODRL.
MPEG 21 REL (The Moving Picture Experts Group, 2013) est adapté aux contenus numériques distribués et consommés par une grande variété des terminaux (PC, PDA, Mobile Phone,…) alors que le langage ODRL (2013) est adapté aux contenus numériques répartis et consommés par des terminaux mobiles (Mobile Phone, PDA, IPhone, *etc.*).
Une combinaison des méthodes de type *Role-Based* Access *Control* (RBAC) avec un langage d'expression de droits, en tenant compte du contexte organisationnel de l'utilisateur, apportera une solution aux défis de contrôle et gestion d'usage des contenus numériques.
La suite de cet article est organisée comme suit. La première partie expose les limites du modèle MPEG 21REL dans ses versions précédentes. Ensuite, nous présenterons un aperçu de nos premiers travaux d'amélioration de l'expressivité du modèle qui ont donné naissance à sa 2ème version. Par la suite, nous exposerons les travaux d'amélioration de la 2ème version, objet de cet article, par l'introduction de nouveaux concepts issus du modèle ORBAC.

2. Problématique

Dans le modèle de données de MPEG-21 (Burnett, 2006), la politique de sécurité s'exprime essentiellement à travers l'énumération des triplets {Objet, Sujet, Action}. À l'usage, une limite importante du modèle est apparue : la politique d'autorisation devient rapidement complexe à exprimer et à administrer. Il est en effet nécessaire d'énumérer les autorisations pour chaque sujet, action et objet. En particulier, lorsqu'un nouveau sujet ou objet est créé, il est nécessaire de mettre à jour la politique d'autorisation pour définir les nouvelles permissions associées à ce sujet ou cet objet. De nos jours, dans un système d'informations, des milliers de sujets interagissent avec des milliers d'objets. Pour pallier ce problème, un modèle nouveau a été envisagé permettant une expression plus structurée de la politique d'autorisation.
La solution a consisté au départ à adopter la notion de «rôle». Le contrôle d'accès à base de rôles est un modèle dans lequel chaque décision d'accès est fondée sur le rôle auquel l'utilisateur est attaché. Les utilisateurs exerçant des fonctions similaires peuvent être regroupés sous le même rôle. Un rôle, déterminé par une autorité centrale, associe à un sujet des autorisations d'accès à un ensemble objets. La modification des contrôles d'accès n'est pas nécessaire chaque fois qu'une personne rejoint ou quitte une organisation. Donc, l'introduction du concept «*Rôle*» facilite la gestion des droits et leurs affectations ainsi que le contrôle d'accès et d'usage des contenus numériques dans les systèmes DRMS (*Digital Rights Management Systems*) (Rafi et Eleuldj, 2007) (Rafi et Eleuldj, 2008a) (Rafi et Eleuldj, 2008b) (Reihanah et Moti, 2006) (Berrahou, Rafi *et al.*, 2010).
Dans ce sens, des travaux de recherches (Dwen-Ren, Wei-Yu *et al.*, 2009) (Danmei, Zhiyong *et al.*, 2010) (Chun-Te, Kun-De *et al.*, 2006) (Mei-Yu, Yi-Wei *et al.*, 2010) (Xianmin, 2011) ont été menés pour améliorer le contrôle d'accès aux systèmes DRM par l'introduction des concepts du modèle RBAC (*Role Based Access Control*). Le premier travail (Dwen-Ren, Wei-Yu *et al.*, 2009) consiste à combiner le contrôle d'accès à base de rôles avec les conditions d'usage qui sont mentionnées dans les licences de type *Creative Commons License* (2013). Le deuxième travail (Danmei, Zhiyong *et al.*, 2010) met l'accent sur le concept de hiérarchisation des rôles. Le troisième article (Chun-Te, Kun-De *et al.*, 2006) propose un système DRM basé sur RBAC avec des conditions et contraintes qui sont dynamiques. Les travaux (Mei-Yu *et al.,* 2010) et (Xianmin, 2011) utilisent le modèle RBAC pour la conception et le développement des applications fondées sur la gestion des droits numériques (DRM). Il faut noter que ces travaux ne concernent pas le standard en gestion des droits numériques : MPEG 21 (The Moving Picture Experts, 2013).

Notre équipe a mené des travaux d'amélioration de la politique de contrôle d'accès en enrichissant et en mettant à niveau le modèle de données du «standard» MPEG 21 qui traite de la question de la gestion des DRM. L'idée consistait à intégrer les concepts du modèle RBAC (rôle, temporisation, *etc.*) dans le modèle MPEG 21, permettant ainsi d'enrichir le langage d'expression des droits correspondants par de nouveaux droits et règles. La nouvelle version a été baptisée «MPEG 21 REL amélioré» (Rafi, Eleuldj *et al.*, 2009). Pour la suite de l'article, cette version sera désignée par «MPEG 21 REL V2.0».

Avec le développement des applications de gestion de droits numériques (DRM *i.e. Digital Right Management*), il faut être capable de spécifier des conditions à satisfaire tout au long de la chaine de distribution et de consommation des contenus numériques.

Ainsi, tout langage d'expression des droits numériques qui espère suivre le rythme avec lequel les systèmes DRMS évoluent, doit être extensible et permettre de traiter des besoins en nouvelles règles et nouveaux droits d'usage. Par ailleurs, ces mêmes systèmes DRMS doivent mettre en place des politiques de contrôle d'accès et d'usage qui s'adaptent aux «contextes» de travail.

Donc, face au nombre croissant d'accès à accorder par les systèmes DRMS, nous devons arriver à élaborer un système d'autorisations qui ne soit pas statique. Il doit dépendre de conditions qui, si elles sont satisfaites, permettent d'activer dynamiquement les autorisations. Dans ce cas, nous parlons souvent «d'autorisations contextuelles». Ainsi, les autorisations peuvent-elles dépendre de contextes temporels (par exemple permission pendant les heures de travail), de contextes géographiques (par exemple, permission à l'intérieur de l'enceinte sécurisée de l'entreprise), de contextes provisionnels (permission si d'autres actions ont été réalisées au préalable, comme dans le cas d'un *workflow*). D'autres types de contextes peuvent également être définis.

Le modèle Or-BAC (Abou El Kalam, El Baida *et al.*, 2003 a) (Sandhu et Coyne, 1996), en plus de généraliser les modèles à base de rôles, offre la possibilité d'exprimer des autorisations contextuelles et ajoute une dimension organisationnelle à la politique. Une organisation est une entité qui a la charge de gérer un ensemble de règles de sécurité : obligations, permissions, interdictions. Les opérations du système sont appelées actions. Un sujet est une entité active du système pouvant réaliser des actions au sein de ce même système. Par opposition aux sujets, les objets sont les entités non actives du système (soumises aux opérations des sujets).

Dans cet article, nous utiliserons Or-BAC (*Organisation Based Access Control*) comme modèle de politique de contrôle d'accès pour les Systèmes DRM. Ce modèle reprend les concepts de rôle, d'activité, de vue et d'organisation qui sont des concepts issus des modèles R-BAC (*Role-Based Access Control*), T-BAC (*Task-Based Access Control*) (Thomas et Sandhu, 1997), V-BAC (*View-Based Access Control*) et T-MAC (*Team-Based Access Control*) (Roshan et Thomas, 1997). Nous étudierons ainsi les adaptations du standard MPEG 21 REL aux spécifications du modèle ORBAC (ORBAC, 2013).

Dans la suite, nous présenterons d'abord le modèle de données du standard MPEG-21 puis le résultat de notre précédente recherche qui consistait à y introduire des concepts du modèle RBAC et qui a abouti à MPEG-21 REL V2. Nous aborderons ensuite les adaptations et les améliorations apportées au modèle par l'introduction des concepts du modèle OrBAC.

3. Introduction de la gestion de rôle dans MPEG 21 REL

3.1. Le standard MPEG 21 REL

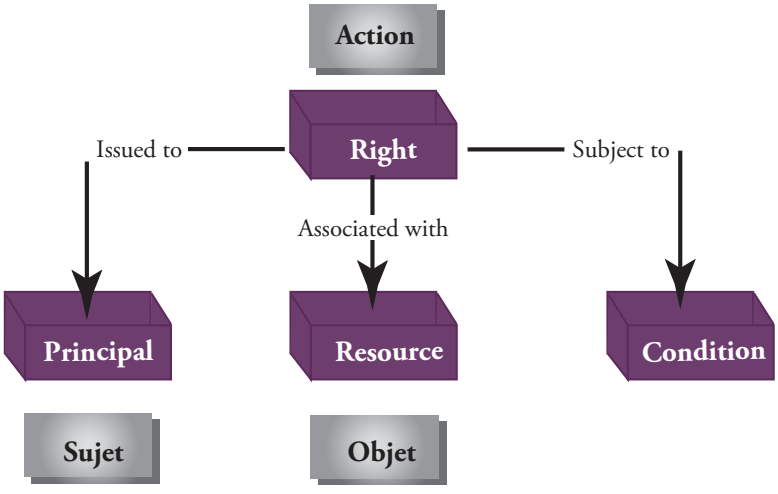

figure 1. Modèle de données MPEG-21 REL [18]

Selon la définition du standard MPEG-21 pour les DRM, «un ***sujet*** a la permission de faire une certaine ***action*** sur une ***ressource*** sous une certaine condition.»
Le contrôle d'accès à des contenus numériques et les conditions de leur usage sont exprimés à travers un ensemble d'autorisations via le langage d'expression des droits : MPEG-21 REL. Ainsi, l'approche utilisée se décline-t-elle en termes de sujet, objet (ressource) et privilège (action, droit ou permission) comme le résume la figure 1.
Pour illustrer ce modèle, nous présentons l'exemple suivant : «Karima» a le droit de «consulter» le fichier «SampleBook» durant «une semaine». Le fichier de licence **Karima.xml** correspondant est écrit selon MPEG-21 REL en figure 2.

```
<License>
  <grant>
    <keyHolder licensePartId="Karima">
    </keyHolder>
    <mx:play/>
    <digitalResource>
    <nonSecureIndirect URL="http://www.contentguard.com/sampleBook.spd"/>
    </digitalResource>
    <validityInterval>
      <notBefore>2012-12-17T23:59:59</notBefore>
      <notAfter>2012-12-24T23:59:59</notAfter>
    </validityInterval>
  </grant>
</License>
```

figure 2. fichier Karima.xml de licence selon MPEG-21 REL

Le tableau 1 décrit les balises constituant la licence Karima.xml.

MPEG 21	Balises correspondantes	Description
Sujet	<keyHolder licensePartId="Karima"> </keyHolder>	Karima est déclarée come sujet
Action	<mx:play/>	Karima a le droit de «lire» le document
Objet	<digitalResource>...</digitalResource>	Déclaration du document que Karima a le droit de lire
Condition	<validityInterval> <notBefore>..... </notBefore> <notAfter> ..... </notAfter> </validityInterval>	La période durant laquelle Karima peut lire le document

Tableau 1. Description des balises de la licence

3.2. Aperçu de MPEG 21 REL V2

L'idée consistait à intégrer les concepts du RBAC (rôle, temporisation) dans le modèle MPEG 21. Baptisée initialement «MPEG 21 REL Amélioré» (Rafi et Eleuldj, 2009), cette version est désignée par «MPEG 21 REL V2.0» dans la suite de cet article.
Un rôle est un concept organisationnel : des rôles sont affectés aux utilisateurs conformément à la fonction attribuée à ces utilisateurs dans l'organisation. Le principe de base du modèle TRBAC (Bertino, Bonatti *et al.*, 2001), ou généralement le modèle RBAC, est de considérer que les autorisations sont directement associées aux rôles et non aux sujets. Ce sont donc les rôles qui reçoivent des autorisations pour réaliser des actions sur des objets et non pas les sujets ou les groupes de sujets qui reçoivent des autorisations comme c'est défini dans le modèle de base de MPEG-21REL.

3.2.1. Principes directeurs de la version 2 du modèle MPEG 21

Un autre concept introduit par le modèle TRBAC est celui de *session*. Pour pouvoir réaliser une action sur un objet, un utilisateur doit d'abord créer une session et, dans cette session, activer un rôle qui a reçu l'autorisation de réaliser cette action sur cet objet. Si un tel rôle existe et si cet utilisateur a été affecté à ce rôle, alors cet utilisateur aura la permission de réaliser cette action sur cet objet une fois ce rôle activé.
Lorsqu'un nouveau sujet est créé dans le Système d'Information (SI), il suffit d'affecter des rôles prédéfinis au sujet pour que ce sujet puisse accéder au SI conformément aux permissions accordées à cet ensemble de rôles.
Dans le cas général, n'importe quel ensemble de rôles peut être affecté à un utilisateur et un utilisateur peut activer dans une session n'importe quel sous-ensemble des rôles qui lui ont été affectés.
Le modèle TRBAC introduit la notion de *contrainte* (de rôle) pour spécifier des politiques d'autorisation incluant des situations plus restrictives. Ainsi, une contrainte de séparation *statique* spécifie que certains rôles, par exemple médecin et infirmier, ne peuvent pas être simultanément affectés à un utilisateur. Une contrainte de séparation *dynamique* spécifie que, même si certains rôles peuvent être affectés à un même utilisateur, par exemple médecin libéral et chirurgien, ces rôles ne peuvent pas être activés simultanément dans une même session.
Dans TRBAC, il est également possible d'organiser les rôles de façon hiérarchique. Les rôles héritent les autorisations des autres rôles qui leur sont hiérarchiquement inférieurs. Lorsqu'un rôle r1 est hiérarchiquement supérieur à un rôle r2, on dit que r1 est un rôle senior de r2.
Par l'introduction des notions de Rôle et Session du modèle TRBAC dans le modèle MPEG 21 REL (figure 1), la gestion de la politique d'autorisation s'en trouve simplifiée puisqu'il n'est plus nécessaire de mettre à jour une politique d'autorisation à chaque fois qu'un nouveau sujet est créé ou qu'un nouvel objet ou une nouvelle action sont introduits.

3.2.2. Notion de «rôle»

Dans l'exemple de la figure 3, nous introduisons les nouvelles balises <Role> et </Role> dans la licence karima.xml définie en figure 2. Dans cette licence, ces deux balises délimitent les droits qu'un utilisateur a acquis. C'est une couche entre un utilisateur (Karima) et ses droits sur un contenu numérique. Si Karima a deux rôles, alors le fichier de licence aura la forme suivante (figure 3).

```
<License>
  <grant>
     <keyHolder licensePartId="Karima"> </keyHolder>
  <Role id=1> …. </Role>
  <Role id=2> …. </Role>
  </grant>
</License>
```

figure 3. fichier Karima.xml de licence selon MPEG-21 REL V2.0 avec plusieurs rôles

La description d'un rôle est présentée en figure 4.

```
<Role id=1>
  <mx:play/>
  <digitalResource>
  <nonSecureIndirect URL="http://www.contentguard.com/sampleBook.spd"/>
  </digitalResource>
  <validityInterval>
    <notBefore>2012-12-17T23:59:59</notBefore>
    <notAfter>2012-12-24T23:59:59</notAfter>
  </validityInterval>
</Role>
```

figure 4. Balise rôle du fichier Karima.xml de licence selon MPEG-21 REL V2.0

3.2.3. Contraintes sur le «rôle»

Nous présenterons les notions de «contrainte dynamique du rôle» et de «temporisation des rôles» par des exemples. Pour la notion de la «contrainte dynamique du rôle», nous considérons le cas d'un chirurgien anesthésiste. Durant une opération chirurgicale, un médecin chirurgien ne peut pas jouer en même temps le rôle chirurgien et celui

d'anesthésiste. Ceci implique que la même personne peut cumuler plusieurs rôles, mais que ceux-ci ne sont pas actifs en même temps. Un rôle, une fois activé, désactive le second. Dans cet exemple, nous introduirons la valeur «**Disable**» pour les nouvelles balises **<Dynamic constraint Role>** et **</ Dynamic constraint Role>.**
La notion de «temporisation des rôles» spécifie que le médecin a un rôle de chirurgien qui commence à partir 08:00 am et qui se termine à minuit du 17/12/2012. Les balises utilisées sont: **<Role validityInterval>** et </**Role validityInterval>** et les valeurs possibles sont NotAfter et NotBefore.

```
<Role id= Chirurgien >
< Dynamic constraint Role > Disable Role id= Anesthésiste </ Dynamic constraint Role>
  <Role validityInterval>
    <notBefore>2012-12-17T08:00:0</notBefore>
    <notAfter>2012-12-17T23:59:59</notAfter>
  </Role validityInterval>
</Role id= Chirurgien >
```

figure 5. Temporisation de rôle du fichier Karima.xml de licence selon MPEG-21 REL V2

Nous avons présenté les résultats de nos travaux précédents qui consistaient à introduire des concepts du modèle RBAC dans le standard MPEG 21. Nous analyserons, dans la suite, de nouvelles pistes pour améliorer l'expressivité du modèle MPEG 21 et pour renforcer le contrôle d'accès aux systèmes DRM.

4. MPEG 21 REL V3

Selon les études (Abou El Kalam, El Baida *et al.*, 2003 b) et sur le site officiel ORBAC (2013), le modèle TRBAC ou d'une façon générale le modèle RBAC présente des inconvénients: le concept de permission est primitif et le concept de hiérarchie de rôles est quelque peu ambigu. Il est en général incorrect de considérer que la hiérarchie de rôles correspond à la hiérarchie organisationnelle. Par ailleurs, la distinction entre le concept de rôle et celui de groupe est floue. Le modèle Or-BAC propose de clarifier ces points.

4.1. Apport du sous-modèle OR-BAC

Le modèle Or-BAC est composé de trois parties:

- La partie supérieure concerne la politique abstraite, composée des concepts de rôle, de vue, d'activité et de contexte, communs à l'ensemble des organisations. La relation entre ces concepts génériques permet de définir des permissions abstraites.
- La partie inférieure concerne la politique concrète, composée des concepts de sujet, d'action et d'objet qui sont propres à chaque organisation et desquels sont dérivées les permissions concrètes.
- La partie intermédiaire joue le rôle de médiateur entre les parties supérieures et les parties inférieures. Partant de la politique abstraite, elle instancie une politique concrète en terme d'objets et d'actions concrets.

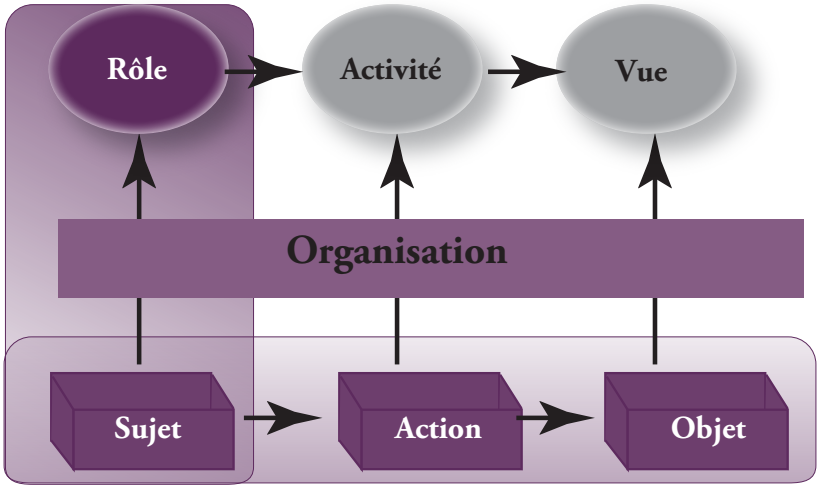

figure 6. Modèle MPEG 21 REL V3

4.2. Modèle de données MPEG 21 REL V3

L'introduction, dans le modèle de données MPEG 21 REL V2, des concepts clés du modèle Or-BAC à savoir la Vue, l'Activité et l'Organisation donnera naissance à la version 3 (figure 7).

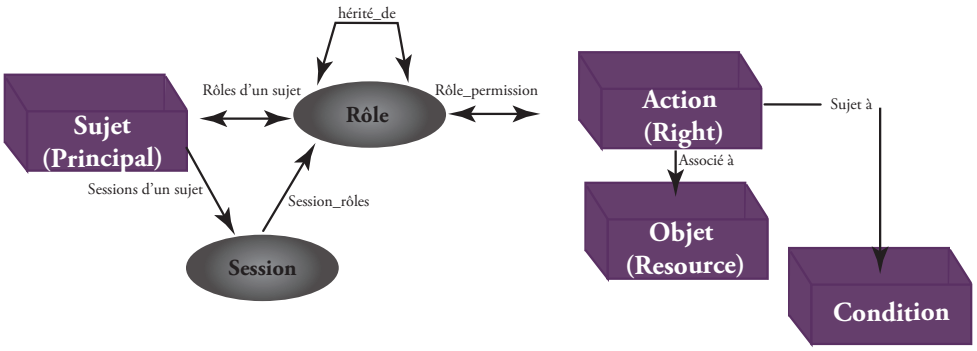

figure 7. Modèle de données MPEG 21 REL V2.0

Les éléments Sujet, Action, Objet et Rôle sont les éléments qui constituent le modèle MPEG21 REL dans sa version V2. Les concepts Activité, Vue et Organisation sont les concepts introduits pour enrichir la version V2 donnant lieu à la version MPEG 21 REL V3.
Les rôles, les activités et les vues sont les représentations abstraites des sujets, actions et objets. Cette relation signifie que l'organisation donne la permission à un rôle de réaliser une activité sur une vue.
La modélisation en UML de ces concepts est présentée en figure 8.

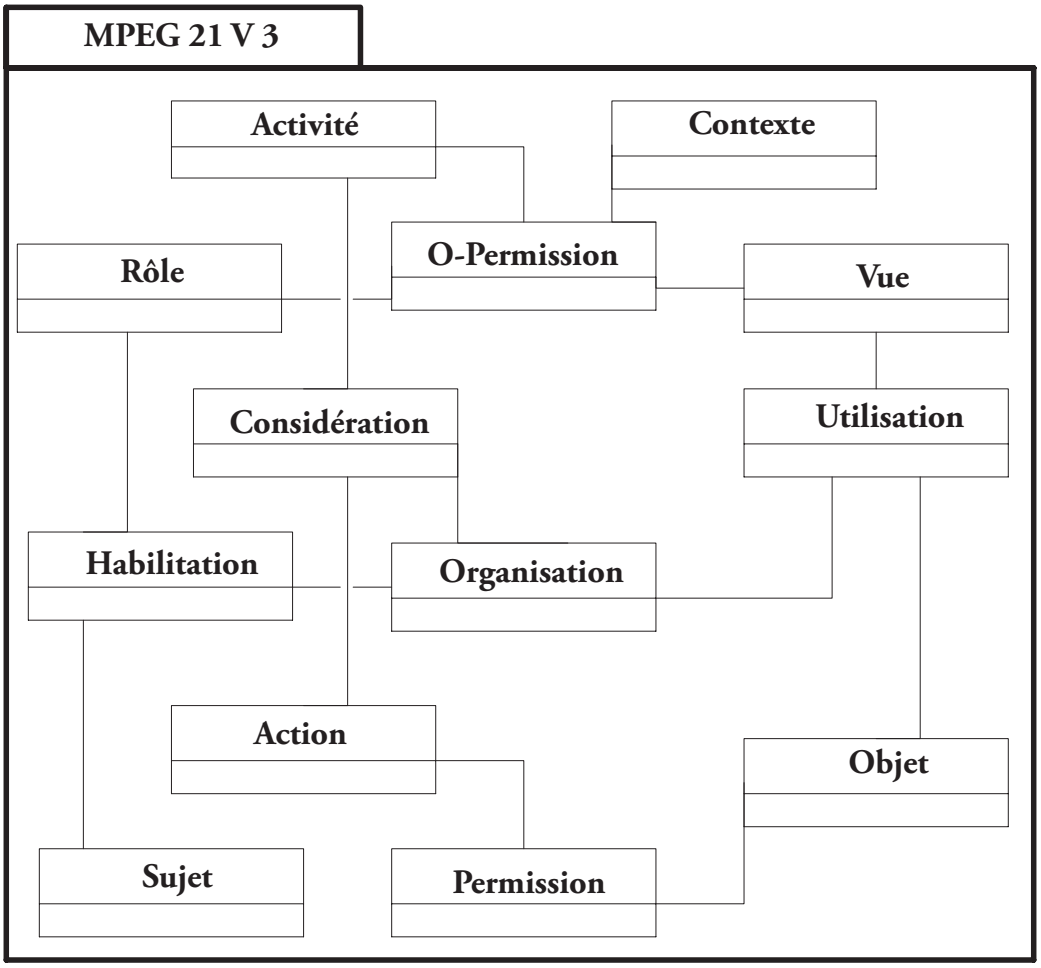

figure 8. Représentation UML du Modèle MPEG 21 REL V3

4.2.1. Les sujets et les rôles

L'entité Sujet est utilisée différemment selon les modèles de sécurité (Abou El Kalam, El Baida *et al.*, 2003 b) et sur le site officiel ORBAC (2013). Dans le modèle Or-BAC, un sujet peut être soit une entité active, c'est-à-dire un utilisateur, soit une organisation. Par exemple, «Jean», «Marie», «Pierre» peuvent être des sujets, tout comme les organisations «département informatique de l'Ecole Mohammedia des ingénieurs (EMI)», «le service des achats de l'Entreprise «Compagnie»». Donc, l'entité Rôle est utilisée pour structurer le lien entre les sujets et les organisations. Dans le domaine médical, les rôles «cardiologue», «Infirmier» ou «Chef de département» sont joués par des utilisateurs alors que les rôles «Département Cardiologie» ou «service de réanimation» sont assumés par des organisations. Comme les sujets jouent des rôles dans des organisations, une relation entre ces entités a été introduite : la relation «Habilite» (Abou El Kalam, *El Baida et al.*, 2003 b) (ORBAC, 2013). Si org est une organisation, s est un sujet et r est un rôle, alors Habilite(org, s, r) signifie que org habilite le sujet s à jouer le rôle r.
Exemple :

- Habilite(Hopital_Souissi, Adil, cardiologue) : «l'Hopital_Souissi habilite Adil à jouer le rôle cardiologue»
- Habilite(Hopital_Souissi, SU, Unité_des_soins_intensifs) : «l'Hopital_Souissi habilite le service SU (Service des urgences), à jouer le rôle chargé de l'Unité_des_soins_intensifs».
-

4.2.2. Les objets et les vues

Dans notre modèle, l'entité Objet (figure 7) représente principalement les entités non actives comme les fichiers, les courriers électroniques, les formulaires imprimés (Abou El Kalam, El Baida *et al.*, 2003 b) (ORBAC, 2013). Dans le domaine médical, nous aurons ainsi à considérer des objets comme les dossiers administratifs, les dossiers médicaux et les dossiers chirurgicaux des patients.
Les rôles nous permettent de structurer les sujets et de faciliter la mise à jour de la politique de sécurité quand un nouvel utilisateur est ajouté.
Dans la mesure où il est également nécessaire de structurer les objets et d'ajouter de nouveaux objets au système, nous considérons qu'une entité comparable au rôle pour les sujets est nécessaire pour les objets. Nous l'appelons : entité Vue. De manière intuitive, une vue correspond, comme dans les bases de données relationnelles, à un ensemble d'objets qui satisfait une propriété commune. Par exemple dans un système de fichier administratif, la vue «dossiers administratifs» correspond à l'ensemble des dossiers administratifs des patients, alors que la vue «dossiers médicaux» correspond aux dossiers médicaux des patients.
Dans la mesure où les vues caractérisent la manière dont les objets sont utilisés dans l'organisation, une relation intitulée «Utilise» lie ces trois entités. Si org est une organisation, o est un objet et v est une vue, alors Utilise(org, o, v) signifie que org utilise l'objet o dans la vue v.
Exemple :

- Utilise (Hôpital Souissi, fichier_Medical_1.doc, dossier_médical) : «L'hôpital Souissi utilise fichier_Medical.doc comme un dossier médical» ;
- Utilise (Hôpital Souissi, FM2.rtf, dossier_inscription) : «L'hôpital Souissi utilise FM2.rtf comme un dossier médical».

4.3. Les actions et les activités

Les politiques de sécurité spécifient les accès autorisés aux entités passives par des entités actives et régulent les actions opérées sur le système (Abou El Kalam, El Baida *et al.*, 2003 b) (ORBAC, 2013). Dans notre modèle, l'entité Action englobe principalement les actions informatiques comme «lire», «écrire», «envoyer», etc. De la même manière que dans 4.1 et 4.2 où les rôles et les vues sont des abstractions des sujets et des objets, nous définissons une nouvelle entité utilisée comme abstraction des actions : l'entité Activité.
Ainsi, les rôles associent-ils des sujets qui remplissent les mêmes fonctions, les vues regroupent des objets qui satisfont à une propriété commune et par analogie les activités correspondent à des actions qui ont un objectif commun. Dans la mesure où des organisations différentes peuvent considérer qu'une même action est employée à la réalisation d'activités différentes, la relation «Considère» sera utilisée pour associer les entités Organisation, Action et Activité. Plus précisément, si org est une organisation, α est une action et a est une activité, alors Considère (org, α, a) signifie que l'organisation org considère l'action α comme faisant partie de l'activité a.
Exemple :

- Considère (Hôpital_Souissi, lire, consultation) : «l'Hôpital_Souissi considère «lire» comme une consultation» ;
- Considère (Hôpital_Souissi, select, consultation) : «l'Hôpital_Souissi considère «select» comme une consultation».

4.4. Les balises du langage MPEG 21 REL V3

Le Tableau 2 décrit les balises constituant une licence selon le nouveau modèle MPEG 21 REL V3. Un utilisateur entre dans le système avec un rôle dans lequel il peut faire appel à une activité sur une vue donnée. Dans le cas où il fait appel à une activité qui est interdite pour son rôle courant, on peut l'obliger à s'authentifier pour entrer avec un nouveau rôle dans lequel l'activité demandée est autorisée. Le schéma XML du nouveau modèle est présenté dans la figure 14.

MPEG 21 REL V3	Balises correspondantes
Sujet	`<keyHolder licensePartId=«Farid»> </keyHolder>`
Action	`<mx:play/>`
Objet	`<digitalResource> ….. </digitalResource>`
Condition	`<validityInterval> <notBefore> .... </notBefore> <notAfter> .... </notAfter> </validityInterval>`
Activité	`<Activity> .... </Activity>`
Organisation	`<Organisation> .... </Organisation>`
Vue	`<View> .... </View>`

Tableau 2 : Description des balises de la licence selon la MPEG 21 REL V3

4.5. Processus d'interprétation des licences dans le nouveau modèle MPEG 21 REL V3.0

Le *workflow* utilisé dans MPEG-21 REL V3.0 est illustré par la figure 16.

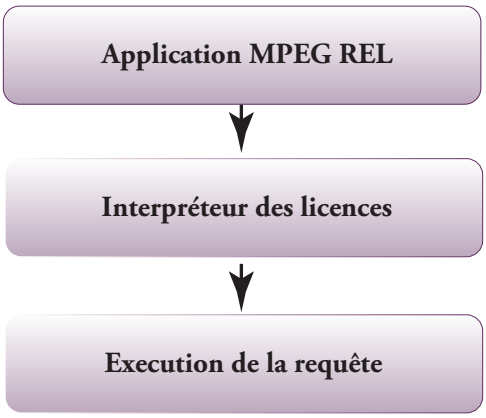

figure 9. Workflow d'interprétation des licences

Avant l'exécution de la requête de l'utilisateur, l'application MPEG 21 REL enclenche le module d'interprétation. Dès que l'interpréteur de la licence valide la requête, les droits de l'utilisateur sont activés concernant ce contenu numérique.

5. Validation par un exemple d'une organisation

5.1. Licences MPEG 21 REL V3

Pour valider le modèle MPEG 21 REL V 3, nous adopterons comme cadre organisationnel à étudier le modèle de l'Université Mohammed V (figure 10), composé des Facultés de Sciences et d'Économie ainsi que de l'École Mohammedia d'Ingénieurs. Nous focaliserons sur l'Ecole Mohammedia d'Ingénieurs (EMI).

Nous introduirons les notions : Activités, Rôles, Vues du modèle d'accès d'Or-BAC. Notre objectif n'est pas de couvrir le modèle organisationnel présenté en figure 10, mais d'étudier la faisabilité par des exemples.
Prenons le cas de Farid, un étudiant qui souhaite lire le document électronique Cours_UML.pdf proposé par la bibliothèque numérique de l'École EMI :

- la relation entre les sujets et les rôles est modélisée par Habilite (EMI, Farid, Etudiant) qui signifie que «l'école EMI habilite Farid pour exercer le rôle étudiant».
- la relation entre les objets et les vues est traduite par Utilise (EMI, Cours_UML.pdf, Programme_Scolaire_Informatique) *i.e.* «L'EMI utilise Cours_UML.pdf comme programme scolaire pour l'informatique
- la relation entre les actions et les activités est modélisée par Considère (Bibliothèque_Numérique_EMI, lire, consultation) *i.e.* «La bibliothèque numérique de l'EMI considère lire comme une consultation».

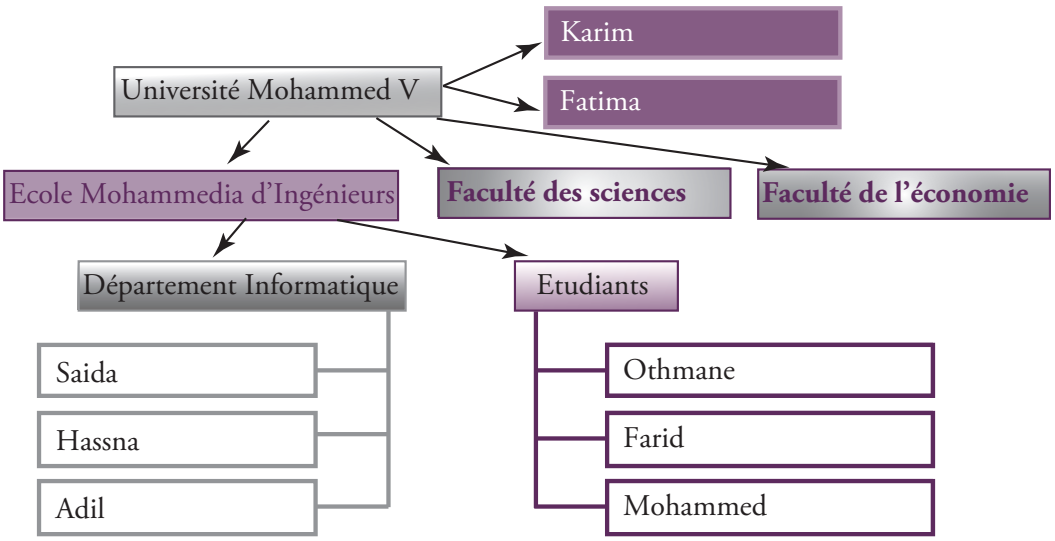

Figure 10. Cas de l'Université Mohammed V

La structure de la licence du nouveau modèle MPEG-21 REL V3.0 après l'introduction des notions (organisation, vue, activité) du modèle Or-BAC est comme suit (figure 11).

```
<License>
<Organization id=Ecole_Mohammedia_d_Ingénieurs>
<grant>
<keyHolder licensePartId="Farid">
</keyHolder>
<Role id=Etudiant>
  <Activity id= Consultation>
  <mx:Lire/>
  </Activity>
  <View id= Programme_Scolaire_Informatique>
<digitalResource>
  <nonSecureIndirect
    URL="http://www.emi.ac.ma/bibliotheque_numérique/Cours_UML.pdf"/>
  </digitalResource>
  </View>
  <validityInterval>
    <notBefore>2008-12-17T23:59:59</notBefore>
    <notAfter>2008-12-24T23:59:59</notAfter>
  </validityInterval>
</Role>
</grant>
</Organization>
</License>
```

figure 11. La licence selon le nouveau modèle MPEG-21 REL V3.0

Dans cet exemple, l'utilisateur «Farid» peut entrer dans le système avec un rôle «Role Etudiant» grâce auquel il peut exécuter l'activité «consultation» sur la vue «Programme_Scolaire_Informatique». Le tableau 3 décrit et présente les balises constituant la licence.

MPEG 21	Balises correspondantes	Description
Sujet	`<keyHolder licensePartId="Farid"> </keyHolder>`	On déclare Karima come sujet
Action	`<mx:play/>`	Karima a le droit de «lire» le document
Objet	`<digitalResource> ... </digitalResource>`	Déclaration du document dont Karima a le droit de lire
Condition	`<validityInterval> <notBefore> ….. </notBefore> <notAfter> ….. </notAfter> </validityInterval>`	La période dans laquelle Karima peut lire le document
Activité	`<Activity> .... </Activity>`	Les balises délimitant le concept «Activité»
Organisation	`<Organisation> .... </Organisation>`	Les balises délimitant le concept «Organisation»
Vue	`<View> .... </View>`	Les balises délimitant le concept «Vue»

Tableau 3. Description des balises de la licence selon la MPEG 21 REL V3

5.2. Processus d'interprétation des licences

La figure 12 donne un aperçu du processus d'évaluation d'une requête utilisateur pour le nouveau modèle MPEG-21 REL V3.0.

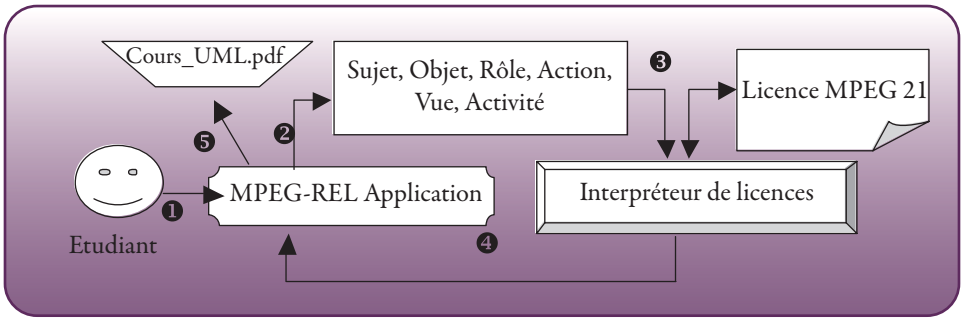

figure 12. Processus d'interprétation

Le processus d'interprétation de la licence est exécuté comme suit, selon cinq étapes :

1. L'étudiant demande la lecture du document électronique. Par exemple, Hamid souhaite lire le document Cours_UML.pdf. L'application de gestion/lecture MPEG REL formalise la requête à soumettre au module Interpréteur. Dans notre cas, l'application MPEG REL formalise la requête suivante : le sujet Hamid active le Rôle Etudiant pour lire qui est une Action à exécuter en relation avec l'Activité Consultation de l'Objet Cours_UML.pdf, sous la Vue Programme_Scolaire_Informatique.
2. L'application MPEG REL appelle l'interpréteur en lui passant la requête.
3. L'interpréteur de la licence valide la licence afin de s'assurer qu'il n'a pas été altéré ou modifié. Ensuite, l'interpréteur vérifie les éléments de la requête.
4. L'application MPEG REL reçoit la validation de la licence de la part de l'interpréteur.
5. L'application MPEG REL permet à l'Etudiant d'effectuer l'action demandée sur le contenu numérique Cours_UML.pdf

Ainsi, nous avons validé le modèle MPEG 21 V3 par l'étude du cadre organisationnel de l'Université Mohammed V, en particulier le cas de l'École Mohammedia d'Ingénieurs. Cette étude applique et illustre les notions d'organisation, de vue et d'activité. Elle montre comment le standard MPEG 21 a été enrichi pour plus d'expressivité, ce qui permettra de traiter des cas plus complexes.

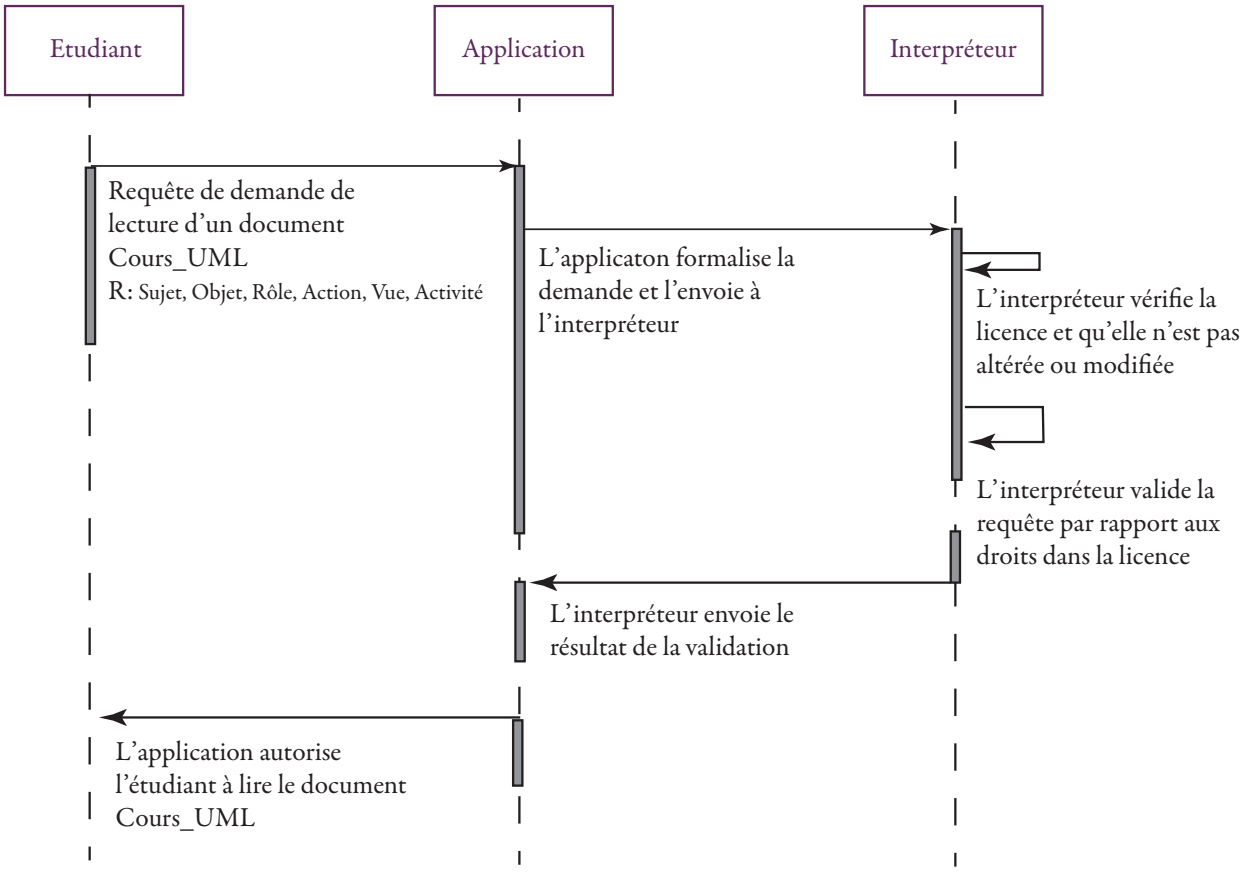

figure 13. Diagramme de séquence d'interprétation

6. Conclusion

Dans cet article, nous avons présenté le nouveau modèle de données de MPEG-21REL V3.0 fondé sur l'approche *Organization-Based* Access Control (Or-BAC). Une combinaison des méthodes de type Or-BAC avec un langage d'expression de droits adaptés au contexte de l'utilisateur permet de doter les systèmes DRM des mécanismes d'octroi des rôles et des permissions, d'une façon dynamique et efficace. Ainsi, les systèmes DRM peuvent-il ajuster dynamiquement, dans le temps et selon le contexte, les autorisations les plus appropriées et par conséquent ils feront face au nombre accru d'usagers ayant des accès variables aux contenus numériques.
Par ce travail, nous avons amélioré la politique de sécurité, le contrôle d'accès et le contrôle d'usage des contenus numériques dans les systèmes DRMS et aussi l'expressivité du standard MPEG-21 REL.
L'application au cas d'une école d'ingénieurs nous a permis de confronter notre modèle à un système réel et de valider notre approche.
Comme perspectives de ce travail, nous prévoyons le développement et la standardisation des notions et des concepts issus de MPEG 21 V3 ainsi que le formalisation du concept de «contexte». Par la suite, il faudrait prendre en compte la notion de règles de délégation et de transfert de droits : par exemple, un médecin a la permission d'autoriser un infirmier à consulter le dossier médical d'un patient.
Une application de démonstration du modèle MPEG 21 version 3 est à envisager, en appliquant le modèle sur des cas plus complexes.

7. Références

Abou El Kalam, A., El Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miège, A., Saurel, C., Trouessin, G. (2003 a). Organization Based Access Control. *In 4th IEEE International Workshop on Policies for Distributed Systems and Networks (Policy'03)*.

Abou El Kalam, A., El Baida, R. *et al.* (2003 b). Or-BAC : un modèle de contrôle d'accès basé sur les organisations. *Cahiers francophones de la recherche en sécurité de l›information. II,30-43.*

Berrahou, A., Rafi, M., Eleuldj, M. (2010). DRMS Co-design by F4MS. *International Journal of Computer Science Issues - IJCSI'10. 7,2*.

Bertino, E., Bonatti, P.A., Ferrari, E. (2001). A temporal role based access control model. *Proceedings of the 5th ACM workshop on Role-based access control*. 4, 3, 191-233.

Burnett, Ian S. (2006). The MPEG-21 Book. Wiley.

Chun-Te, C., Kun-De, L., Ying-Chieh, W., Kun-Lin, L. (2006). An Approach of Digital Rights Management for E-Museum with Enforce Context Constraints in RBAC Environments. 2006 IEEE International Conference on Systems, Man, and Cybernetics, Taipei, Taiwan.

Danmei, N., Zhiyong, Z. Lili, Z. (2010). A DRM System for Home Network Based on RBAC and License. 2010 Fourth International Conference on Genetic and Evolutionary Computing.

Dwen-Ren, T., Wei-Yu, C, Liang, H., Hu, C. (2009). Role-Based Access Control of Digital Right Management. fifth International Joint Conference on INC, IMS and IDC.

Ferraiolo, D. F, Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R. (2001). Proposed NIST Standard for Role-Based Access Control. ACM Transactions on Information and System Security. 4,3, 222-274.

Gavrila, S.-I., Barkley, J.-F. (1996). Formal Specification for Role Based Access Control User/Role and Role/Role Relationship Management. Third ACM Workshop on Role-Based Access Control, 22-23 Octobre, 81-90.

Mei-Yu, W., Yi-Wei, C., Chih-Kun, K. (2010). Design and implementation of a context and Role-Based Access Control model for digital content. 2010 IEEE- IET International Conference on Frontier Computing. Theory, Technologies and Applications.

Rafi, M., Eleuldj, M. (2007). Digital Right Management. 7ème Conférence Internationale sur les NOuvelles TEchnologies de la REpartition NOTERE'07.

Rafi, M., Eleuldj, M., Guennoun, Z. (2008a). Digital Rights Management Adaptable Architecture. The 3rd IEEE International Conference on Information & Communication Technologies: from Theory to Applications - ICTTA'08, Damas, Syrie

Rafi, M., Eleuldj, M., Diouri, O. (2008b). Digital Rights Management- A developpement of media player. Scientific Research Outlook & Technology Developpement in the Arab World (SRO5), Conference of Information and Communication Technologies, Fes.

Rafi, M., Eleuldj, M., Guennoun, Z. (2009). Improvement of MPEG-21 Right Expression Language. The Seventh ACS/IEEE International Conference on Computer Systems and applications - AICCSA'09. Rabat

Roshan, K., Thomas, R. (1997). TMAC: A primitive for Applying RBAC in collaborative environment. 2nd ACM Workshop on RBAC, Fairfax, Virginia, USA: 6-7 novembre, 13-19.

Reihanah, S., Moti, Y. (2006). Digital Rights Management: Technologies, Issues, Challenges and Systems, Springer.

Sans, T., Cuppens, F. (2004). Vers une Formalisation des Langages de DRM. 1er atelier INFORSID. Sécurité des Systèmes d'Information (SSI 2004). Biarritz, France.

Thomas, R., Sandhu, R. (1997). Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. 11th IfiP Working Conference on Database Security, Lake Tahoe, California, USA.

DRM (2013) DRM white papers **http://www.contentguard.com/what-we-do/drmwhitepapers.html**.

The Moving Picture Experts (2013) MPEG-21 REL. The Moving Picture Experts Group website. http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm.

ORBAC (2013) Site web officiel du modèle ORBAC. **http://www.orbac.org**.

Xianmin, W. (2011). Design and Implementation of Rights Management System Based on RBAC Model. 2011 IEEE International Conference on Computer and Management (CAMAN).

Sandhu, R., Coyne, E.J., Feinstein, H.L., Youman, C.E. (1996). Role-based Access Control Models. In IEEE Computer, 29,2,38–47.

Creative Commons License (2013). Site web officiel de l'organisation Creative Commons License. http://creativecommons.org/about.

ODRL (2013) Site web officiel de l'initiative Open Digital Rights Language (ODRL). **http://www.w3.org/community/odrl/**.

8. Annexe : Schéma XML de la nouvelle licence MPEG-21 REL

```
<?xml version="1.0"encoding="utf-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2000/10/XMLSchema">
<xsd:element name="License">
  <xsd:element name="Organization">
    <xsd:element name="Grant">
      <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="keyHolder License">
      <xsd:attribute name="PartId" type="xsd:string"/>
      </xsd:element>
      </xsd:sequence>
      </xsd:complexType>
      <xsd:element name="Role" minOccurs="1" maxOccurs="unbounded"/>
        <xsd:complexType>
        <xsd:sequence>
          <xsd:element name="Activity"/>
            <xsd:complexType>
            <xsd:sequence>
            <xsd:element name="Right"/>
            </xsd:sequence>
            </xsd:complexType>
          <xsd:element name="View"/>
            <xsd:complexType>
            <xsd:sequence>
            <xsd:element name="digital Resource"/>
              <xsd:complexType>
              <xsd:element name="nonSecureIndirect">
              <xsd:attribute name="URI" type="xsd:string"/>
              </xsd:element>
              </xsd:complexType>
            </xsd:sequence>
            </xsd:complexType>
        </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="RoleValidityInterval"/>
        <xsd:complexType>
        <xsd:sequence>
          <xsd:element name="notBefor" type="xsd:Date"/>
          <xsd:element name="notAfter" type="xsd:Date"/>
        </xsd:sequence>
        </xsd:complexType>
      <xsd:attribute name="id" type="xsd:String"/>
      <xsd:element name="RoleStaticConstraint" type="xsd:string"/>
      <xsd:element name="RoleDynamicConstraint" type="xsd:string"/>
      <xsd:element name="RoleTotalActiveDuration" type="xsd:string"/>
</xsd:Grant>
</xsd:Organization>
</xsd:License>
</xsd:schema>
```