

Rapport de stage Master2 RACOR

Sujet du stage:

**Gestion des identités
pour un Web socio-sémantique**

Nom des encadreurs :

Aurélien BENEL
aurelien.benel@utt.fr

Jean-Pierre CAHIER
jean-pierre.cahier@utt.fr

Réalisé par :

Rami EL SAWDA
rami.el_sawda@utt.fr

Juillet 2005

Remerciements

Je tiens tout d'abord à remercier profondément, professeur Manuel ZACKLAD, directeur du laboratoire Tech-CICO, pour m'avoir accueilli au sein de leur équipe.

Je tiens aussi à exprimer ma profonde reconnaissance à Monsieur Aurélien BENEL qui a dirigé mes travaux de recherche, pour ses conseils, sa patience et sa disponibilité. Je le remercie aussi pour son encadrement non seulement scientifique mais aussi humain. Il m'a permis de développer mes travaux de recherche toujours dans les meilleures conditions possibles.

Mes sincères remerciements vont aussi à Monsieur Jean-Pierre CAHIER pour sa disponibilité et pour avoir bien voulu juger mes travaux. Sa gentillesse et sa générosité scientifique nous ont accompagnées durant toute la période du stage.

Je remercie également tous les membres de l'équipe Tech-CICO pour leur sympathie et l'ambiance chaleureuse qui règne dans le laboratoire.

Résumé

Nous nous intéressons à la gestion des identités des sujets sur des modèles de connaissances. Notre but est d'étudier de manière prescriptive (gestion des droits d'accès) et descriptive (historique des modifications) des actions de ces sujets. Inspiré de l'identité dans les sciences humaines, et en identifiant quelques problèmes informatiques liés à la gestion des identités dans les systèmes d'information; nous avons proposé un modèle basé sur la métaphore du passeport. Nous supposons que ce modèle ait résolu certains problèmes identifiés.

Mots-clés : Travail coopératif, Approche sociologique, Ingénierie des connaissances documentaires, Systèmes d'information.

Sommaire

INTRODUCTION	4
Chapitre 1	5
Etat de l'art	5
1.1 Constitution de l'identité en sciences humaines	5
1.2 Quelques notions reliées à l'identité numérique.....	8
1.3 Quelques problèmes liés à la gestion des identités dans Unix.....	10
1.4 Quelques problèmes de la gestion des identités dans LDAP.....	10
1.5 L'importance des rôles dans la gestion des identités	11
1.6 Introduction au Web Socio-Sémantique	11
1.7 Gestion des acteurs et des rôles dans le web socio- sémantique	13
Chapitre 2	15
Travail effectué :	15
Conception du modèle de la gestion des identités	15
2.1 Éléments coopérateurs dans la gestion des identités	15
2.1.1 Les autorités de confiance.....	16
2.1.2 La gestion de stratégie.....	16
2.1.3 La gestion des sanctions.....	16
2.2 Le modèle proposé.....	16
2.2.1 Le passeport.....	18
2.2.2 Le Groupe.....	20
2.2.3 Le visa	20
2.2.4 Marque de passage	22
Conclusion	23
Bibliographie	24

INTRODUCTION

L'évolution actuelle de la "société de l'information" vers une "société de la connaissance", les besoins en gestion des connaissances dans les organisations ou communautés suscite une recherche profonde et évolutive au sein de l'ingénierie des connaissances.

L'ingénierie des connaissances (IC) propose des concepts, méthodes et techniques permettant d'acquérir, de modéliser et de formaliser des connaissances pour les mobiliser dans l'activité individuelle ou collective au sein d'une organisation ou d'une communauté. Elles sont structurées, formalisées et opérationnalisées pour être intégrées dans le fonctionnement d'un système basé sur des connaissances.

L'IC intègre de plus en plus dans des acquis des disciplines telles que les sciences humaines et sociales, la sociologie, la psychologie et l'ergonomie cognitives, la terminologie et la linguistique de corpus, la gestion.

Dans ce cadre l'IC est concernée par les recherches en cours sur le Web socio sémantique, un système d'information pour la coopération destiné à des acteurs organisés en communautés et partageant des objectifs similaires.

Les outils de gestion de la structure des informations échangées et des rôles, des identités et des statuts, forment les différentes composantes d'un espace de coopération au sein du Web socio sémantique.

Mon stage de recherche s'inscrit dans le cadre de la gestion des identités pour le Web socio sémantique. Il s'agit d'étudier comment gérer les actions des sujets (personnes, communautés) en s'appuyant sur des modèles de connaissance. Nous allons nous intéresser aussi bien à une gestion prescriptive (gestion des droits d'accès) qu'à une gestion descriptive (historique des modifications).

Dans le but de résoudre cette problématique, je vais présenter les différents points abordés durant la période de mon stage.

Le premier chapitre représente une revue sur la question de l'identité dans les Sciences Humaines, ensuite un aperçu de l'identité numérique et une introduction de la gestion des acteurs et des rôles dans le Web socio sémantique. Le Chapitre 2 présente le modèle conçu à l'aide des exemples inspirés du système d'information d'une Université.

Chapitre 1

Etat de l'art

1.1 Constitution de l'identité en sciences humaines

1.1.1 Niveau de l'individu

Inspiré de la gestion des identités dans les sciences humaines, je vais présenter dans cette partie comment l'identité de l'individu est fondée ? Et quelles sont ses différentes identités ?

1.1.2 Comment peut-on définir le soi ?

Le soi peut se définir comme « un ensemble de caractéristiques (goûts, intérêts, qualités, défauts, etc.), de traits personnels (incluant les caractéristiques corporelles), des rôles et de valeurs, etc., que la personne s'attribue ». [1]

Le soi est aussi défini comme un « Système éminemment adaptatif, qui se défend, se corrige et s'améliore pour mieux s'adapter et même se dépasser ». [2] Jean-Claude Ruano-Borbalan, co-fondateur et directeur de publication du magazine Sciences Humaines, décrit comment se construit l'identité de l'individu « L'individu se socialise et construit son identité par étapes, au cours d'un long processus qui s'exprime fortement de la naissance à l'adolescence, et se poursuit jusqu'à l'âge adulte ». [3]

Ainsi on peut distinguer quatre dimensions de l'identité personnelle :

- une première est constituée par le désir de continuité du sujet qui appartient à un environnement, à une culture ou à un imaginaire.
- une deuxième montre une rupture d'identité par exemple la rupture entre l'identité de l'enfance et l'identité de l'adolescence.
- Une dimension sociologique montre à quelle échelle la pratique d'une action peut influencer sur l'identité de l'individu (par exemple l'identification religieuse est d'autant plus forte que l'on va plus régulièrement à la messe).
- Une dimension psychologique qui valorise le soi, l'auto justifie et la structure.

1.1.3 L'identité se construit elle progressivement ?

Cité dans [4], Edmond Marc Lipiansky dans sa présentation de l'identité personnelle montre que l'enfant a pour identité de base son corps, il se

découvre à travers ses perceptions et ses actions et aussi dans son rapport des autres et grâce aux regards des autres.

« Avant même sa naissance, l'enfant existe déjà dans l'imaginaire et le discours de ses parents. Désiré ou non attendu, il prend très vite un contour plus ou moins précis à travers le sexe souhaité, le prénom choisi, qui à la fois l'individualisera et le situera dans une filiation et dans une caractérogie sommaire ». [1]

1.1.4 Existe-t-il plusieurs identités pour le même individu ?

L'individu appartient à plusieurs communautés (ethnie, nation, famille, groupe professionnel, tribu, sexe, classe sociale) et ceci explique le métissage de son identité.

Il existe donc en chaque personne plusieurs identités (réelles ou potentielles), les circonstances sociales ou historiques vont permettre à une identité de s'imposer par rapport à l'autre. [5]

L'identité se construit donc progressivement et durant cette construction tous les aspects cognitifs et sociaux rentrent en jeu.

La construction des identités se traduit par des formes identitaires distinctes qui sont «des moyens de représentation, des moyens pour construire des mondes, les identifier et pouvoir les négocier avec les autres dans la ville sociale ». [5]

	Continuité Biographique	Rupture Biographique
Identités reconnues par les institutions de travail	Identités d'entreprise	Identités de réseau
Identités non reconnues par les institutions de travail	Identités catégorielles	Identités « hors travail »

Tableau 1.1 : Les formes identitaires [5]

Comme nous le montre le tableau ci-dessus ; l'identité se construit soit en continuité soit en rupture avec son passé pour se reconstruire de nouveau et ceci continue tout le long de la vie.

Les formes identitaires *identités d'entreprise* et *identités catégorielles* sont construites à partir d'une continuité biographique. Par contre les deux autres formes *identités de réseau* ou *hors travail* sont construites à partir d'une rupture biographique.

Certaines formes telles que les *identités d'entreprise* et les *identités de réseau* sont aussi reconnues par les institutions de travail, d'autres ne le sont pas comme les identités catégorielles et hors travail.

Ce tableau montre bien que chaque personne peut changer de forme identitaire au cours de sa vie. Les formes identitaires représentent des moyens

indispensables pour construire des mondes, les identifier et pouvoir les négocier avec les autres dans la vie sociale. [5]

1.1.5 Comment définir l'identité du groupe ?

Comme l'identité est un processus de socialisation qui intervient tout au long de l'enfance, les valeurs de chacun résultent de normes inculquées de la famille, de l'école et des amis.[6]

Même s'il y'a socialisation de l'individu par le groupe, le sujet se différencie, s'individualise et tend à agir par ses projets sur son entourage social.

L'identité du groupe résulte des processus d'identification et de distinction par lequel ce groupe cherche à marquer sa position par rapport à d'autres groupes. [5]

Un groupe peut n'être qu'une collection d'individus ayant une caractéristique commune.

Par exemple les jeunes, les femmes forment des groupes sociaux ayant des caractéristiques communes.

Le sociologue américain Charles H. Cooley cité dans [1] définit deux types de groupes : *Groupe primaire* et *groupe secondaire*.

Le groupe primaire est un groupe stable caractérisé par une vie commune, des relations personnelles et intimes entre ses membres.

Le groupe secondaire est un groupe dont les liens entre ses individus sont liés par un contrat dont l'objectif est déterminé. Exemple : une entreprise, une administration, une association.

Une autre distinction existe aussi entre *groupe d'appartenance* et *groupe de référence*.

Le groupe d'appartenance est celui dont fait effectivement partie un individu.

Le groupe de référence est celui qui fournit à l'individu ses valeurs, ses normes et ses modèles d'attitude, d'opinion et de comportement.

Donc l'identité, c'est ce qui me distingue : je ne suis pas un autre, un autre n'est pas moi ; ne pouvant être confondu avec un autre, je peux être reconnu, je peux être considéré comme responsable, je peux m'engager, posséder, etc.

L'identité possède un rôle dans la coopération lorsqu'elle me permet d'échanger et d'appartenir : parce que j'existe à mes yeux et à ceux des autres, je peux échanger avec d'autres, en tant que sujet ; je peux me reconnaître et être reconnu comme membre d'un groupe, partageant une identité collective qui est plus que la somme des identités individuelles, mais qui a tout de même besoin d'elles. [6]

1.2 Quelques notions reliées à l'identité numérique

Alors que le monde dans lequel nous vivons étend ses frontières au-delà du monde physique pour intégrer un monde numérique en constante extension et transformation, se pose la question de l'impact de cette mutation sur l'identité des personnes.

Un même individu fera partie d'une multitude de cercles, se manifestera sous plusieurs identités plus ou moins fortes, plus ou moins reliées entre elles.

Et d'un point de vue plus global, il s'agira de rechercher des équilibres dynamiques entre :

- Ce qui est nécessaire pour que la confiance, donc l'échange, s'établissent, sachant que ce « nécessaire » est plus ou moins complexe selon l'objet ou les parties de l'échange ;
- Ce que désirent les individus, les groupes, les vendeurs, les pouvoirs, etc.

1.2.1 Microsoft autour du Passeport

Microsoft fournit des solutions techniques ainsi que des services pour gérer l'identité numérique à partir de la notion du passeport pour :

- permettre aux individus d'être authentifiés sans dire qui ils sont,
- faire communiquer des « îlots numériques » pour fournir aux utilisateurs des services plus intégrés, gérer des relations de confiance entre des acteurs différents qui fournissent tous des services personnalisés (par exemple le lien entre le remboursement par la Sécu et la mutuelle qui intervient ensuite).

1.2.2 La biométrie

La biométrie est une technique qui permet d'identifier des personnes à partir d'une ou de plusieurs de leurs caractéristiques personnelles, comportementales et /ou biologiques. (Exemple : empreintes digitales).

Les craintes vis à vis de la biométrie concernent d'une part la question de traçage et de la protection de la vie privée et d'autre part, la sécurité.

La biométrie est considérée comme une technologie particulièrement sûre, notamment contre l'usurpation d'identité cependant dans certains cas rares les pirates sont parvenus à déjouer des systèmes, notamment ceux qui se basent sur les empreintes digitales.

Le traçage concerne avant tout les bases de données destinées à l'identification ainsi que celles qui concernent les actions à propos desquelles l'identification a été réalisée. Il s'agit de savoir si les données collectées pour autoriser une action et l'accès à des locaux, etc. sont conservées, combien de temps, dans quelles conditions, etc.

1.2.3 L'anonymat

Il faut distinguer entre :

- des usages de vérification d'identité (ex. droits d'accès) pour lesquels l'anonymat est possible (on vérifie que la personne dispose d'un droit, mais on n'a pas nécessairement à savoir qui elle est)
- des usages destinés à identifier quelqu'un, par exemple en recherchant un individu dans une foule.

En ce qui concerne les mots de passe, si votre mot de passe est prêté, la personne qui se connecte avec votre mot de passe est masquée par votre identité, dans un cas identique il est difficile de s'assurer de la réelle identité de la personne. La biométrie semble être une bonne réponse à ce problème.

Les données de connexion : « je surfe donc je suis ». Cela ne concerne pas que la conservation des données d'usage par les fournisseurs d'accès (logs) ou l'adresse IP (qui identifie un abonné ou une machine et non une personne).

Selon Emmanuel Jud, il devient donc de plus en plus nécessaire de trouver les moyens de rendre possible un usage anonyme de l'Internet :

« Pour éviter le traçage et pour réduire les risques : le meilleur moyen de ne rien se faire voler est de ne rien laisser traîner. »

1.2.4 AAA (Authentication, authorization, and accounting)

Certification, autorisation, et comptabilité est un terme pour contrôler une structure intelligemment et accéder aux ressources de l'ordinateur, mettre en vigueur des politiques, vérifier l'usage, et prévoir l'information nécessaire pour facturer les services. Ces processus combinés sont considérés comme important pour la gestion de la sécurité dans un réseau.

L'authentification est le processus permettant de déterminer si une personne est-elle vraiment ce qu'elle prétend être grâce l'utilisation des mots de passes.

La faiblesse dans ce genre de système est que le mot de passe peut être volé ou oublié.

L'autorisation est l'action qui suit l'authentification qui donne l'accès ou non à l'utilisateur d'effectuer certaines tâches. Ce processus permet de déterminer à quelles ressources ou services un utilisateur peut accéder.

La comptabilité est utilisée pour contrôler l'autorisation, journaliser les fichiers logs et facturer l'utilisation de la ressource.

1.3 Quelques problèmes liés à la gestion des identités dans Unix

Dans le modèle Unix trois sujets l'utilisateur, le groupe et les autres permettent d'exécuter la plupart des commandes disponibles pour gérer des répertoires. [7]

La commande « chown » permet de changer « l'utilisateur » du fichier (à condition d'être exécutée par l'utilisateur de départ), dans ce cas ce dernier devient l'auteur du document. Cela reviendrait à dire que l'on peut falsifier un document. L'utilisateur d'un fichier serait à rapprocher du possesseur d'un document dans le monde réel. Il peut donc tout à fait céder ses droits de possession à un tiers.

Chaque utilisateur, pourra appartenir à plusieurs groupes. Dans l'exemple ci-dessous il est impossible par exemple de modéliser une fois pour toutes que chaque membre de « l'équipe Tech-CICO » est membre du « Laboratoire ISTIT » [7]

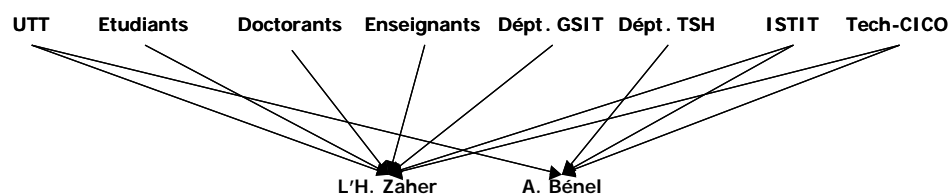


Figure1.1: Structuration des personnes en groupe dans Unix

Un autre reproche que l'on pourrait faire ; les verbes lire, écrire, exécuter sont utilisés pour les répertoires et pour les fichiers.

1.4 Quelques problèmes de la gestion des identités dans LDAP

Dans le modèle LDAP¹ (RFC 2253), le principe de multi appartenance des utilisateurs à plusieurs groupes est manière arborescente présente un certain nombre de problèmes. Tout d'abord, la structure arborescente empêche de définir un groupe à l'intersection de deux autres. Il sera par exemple impossible de modéliser le fait que l'ISTIT soit inclus à la fois dans le CNRS et l'UTT. De plus, pour des raisons architecturales, l'objet modélisant l'utilisateur ne peut être référencé dans un autre annuaire. Par exemple, l'utilisateur « L'Hédi Zaher » s'il est inscrit dans l'annuaire LDAP de l'UTT et dans celui du CNRS, sera modélisé par deux objets totalement distincts et indépendants. Dans le même exemple, il serait également impossible de chercher les « doctorants de Tech-CICO ». [7]

¹ LDAP : *Lightweight Directory Access Protocol*.

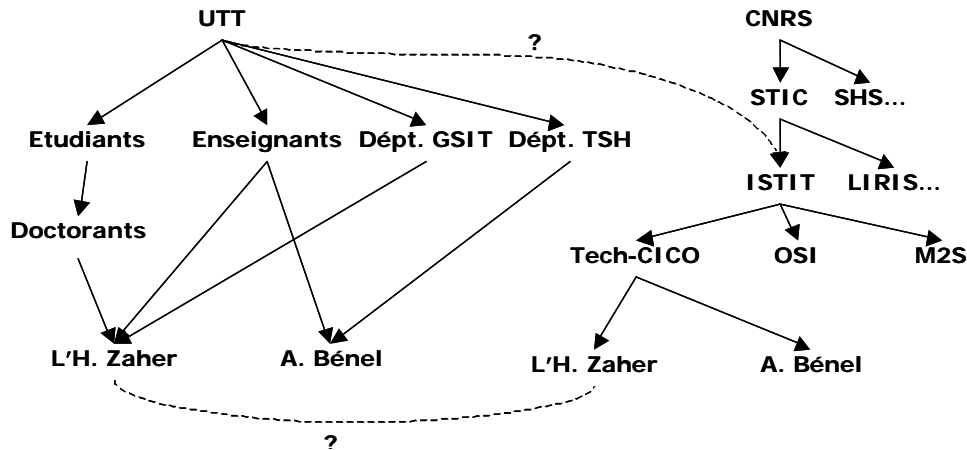


Figure 1.2 : Structuration des personnes et des groupes dans LDAP.

1.5 L'importance des rôles dans la gestion des identités

Comparons dans cette partie le rôle traditionnel par rapport au rôle tel qu'il est défini en sociologie :

Le rôle traditionnel est un ensemble de droits d'accès.

Le rôle en sociologie possède quatre caractéristiques : [7]

- La *position* dans la hiérarchie, dans une logique de différenciation et de responsabilité (cependant les règles et les appartenances sont dynamiques),
- La *fonction*, l'organigramme étant toujours un peu adapté suivant les circonstances (plus ou moins inconsciemment),
- Le *comportement* correspondant à « l'interprétation du rôle » dans la tâche,
- La *sanction* vis-à-vis d'un écart entre le comportement et l'attente qu'en avait le groupe : sanction négative (exclusion...) ou positive (acceptation passagère, reconnaissance du nouveau rôle).

1.6 Introduction au Web Socio-Sémantique

Le Web socio-sémantique fédère ainsi les Web sémantique, social, et cognitivement sémantique. Il se base sur les sciences humaines et sociales et la compréhension de l'activité coopérative pour modéliser et représenter les connaissances de communautés.

Le Web socio-sémantique est un système d'information pour la coopération. [8]

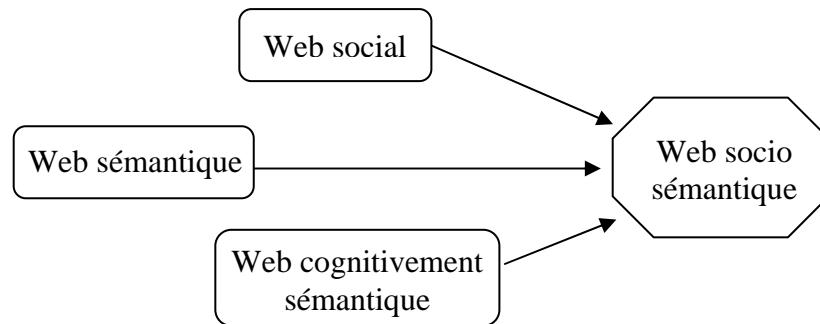


Figure 1.3 : Le Web socio-sémantique comme fédérateur [8]

Le web sémantique:

La thématique du Web *sémantique* repose sur la question du *sens* et de sa *construction*.

Le Web sémantique – imaginé au sein du W3C par Tim-Berners Lee – fut d’abord présenté comme étant une extension du Web courant dans laquelle l’information se donne un sens bien défini permettant aux ordinateurs et aux hommes de mieux travailler en coopération [9].

Il a pour but de permettre aux :

- Machines de comprendre les humains.
- Machines de comprendre les machines.
- Humains de comprendre les humains à travers des machines.

Le web social :

C’est l’ensemble des applications du Web qui visent essentiellement à fournir des espaces de rencontre accroissant la conscience mutuelle entre les partenaires (mutual awarness) dans les interactions distantes (forum, chat, messagerie instantanées, etc.).

Le web cognitivement sémantique :

Permet de guider la recherche et la navigation d’un acteur humain à l’aide des indexations. Le Web Cognitivement Sémantique visait à intégrer dans les recherches et les pratiques de développement des applications du Web Sémantique l’ensemble des activités de conception initiale des représentations, de maintenance au fil de l’eau (au fur et à mesure que les connaissances évoluent) et d’évaluation de la pertinence des résultats des requêtes.

Tout en prolongeant cette perspective, le Web Socio-Sémantique (W2S) se positionne vis-à-vis du « Web Social ». Le W2S vise lui à soutenir des activités de coopération plus structurées dans lesquelles les interactions s’appuient également sur des informations ou des documents partagés par un collectif poursuivant, au moins pour un temps, des objectifs communs. Vis-à-vis de ces objectifs, il doit contribuer à la construction d’une représentation structurée tant du domaine que du collectif.

Les applications du W2S doivent permettre aux acteurs de remodeler voire de construire la structure des espaces de coopération dans lesquels se déroulent leurs interactions, espaces qui prennent la forme d'un réseau de liens entre des applicatifs et des ressources nécessaires à la conduite de leur activité. [8]

1.7 Gestion des acteurs et des rôles dans le web socio-sémantique

Tech-CICO a développé un ensemble de concepts adapté aux applications du W2S qui est modélisé par un modèle générique appelé Hyper Topic ; un modèle de description de connaissances basé sur les graphes et un langage de représentation de connaissances adapté à l'approche Web socio-sémantique.

Ce modèle inclut les concepts de Point de Vue, de Thèmes, d'Entités, de Ressources et d'Association.

Les Points de vue dans Hyper Topic sont des "descripteurs de mise en situation" [8] ancrant les entités, les thèmes, et l'organisation de leurs associations dans une conception / perception d'une sous-communauté d'acteurs.

Un Thème est un concept, un critère ou d'une propriété caractérisant les autres thèmes et les entités qui lui sont hiérarchiquement liés.

L'entité permet la distinction entre l'objet décrit d'une part et ses caractéristiques et les ressources documentaires qui lui sont attachées d'une autre part.

Les ressources correspondent à des documents, des sections de pages Web, des fichiers multimédia, des informations issues de bases de données ou des documents bureautiques mis sur le Web. Ils contiennent des informations en rapport avec l'entité à laquelle les ressources se rattachent.

Hyper Topic définit un nombre de types recommandés d'association tels que Inclut, Est-un-sous-thème-de, Traite-de, a-pour-(nom_attribut) etc.

Hyper Topic V2 introduit la représentation de l'activité et des acteurs ainsi que leurs rôles respectifs en plus de la représentation du domaine.

Les différents composants mis en oeuvre sont organisés et hiérarchisés via leurs associations dans trois dimensions. [10]

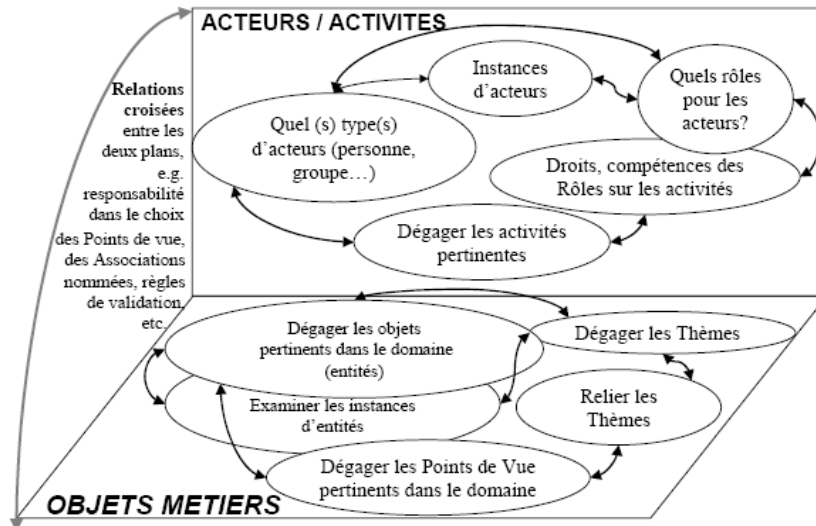


Figure 1.4 : Structuration des acteurs et des rôles dans Hyper Topic [10]

- le plan Métier et Domaine, où sont organisés les objets du problème traité par la représentation, et où ils subissent les différentes activités coopératives des acteurs ainsi que leurs actions.
- le plan Acteurs / Rôles ou est représentée l'organisation sociale de la communauté hôte de l'activité coopérative.
- le plan Activité, représentant les actions aussi bien système (servant à la régulation, à l'organisation et à la distribution de rôles), opérationnelles qu'argumentatives dans la coopération [10].

Chapitre 2

Travail effectué :

Conception du modèle de la gestion des identités

Dans le premier chapitre après avoir défini le rôle de la gestion des identités dans le Web Socio Sémantique, et avoir montré comment les sociologues définissent l'identité et comment le monde de l'informatique gère l'accès aux ressources, ce chapitre présente le modèle que nous avons conçu à partir d'un rapprochement entre ces deux mondes. Nous faisons l'hypothèse que ce modèle peut apporter un nouveau changement au sein de la gestion des identités pour une gestion dynamique et décentralisée de l'identité des sujets connaissants.

2.1 Éléments coopérateurs dans la gestion des identités

Notre modèle est basé sur la métaphore du passeport, du visa et de la marque de passage. Quatre éléments rentrent en jeu pour coopérer et assurer la gestion des identités.

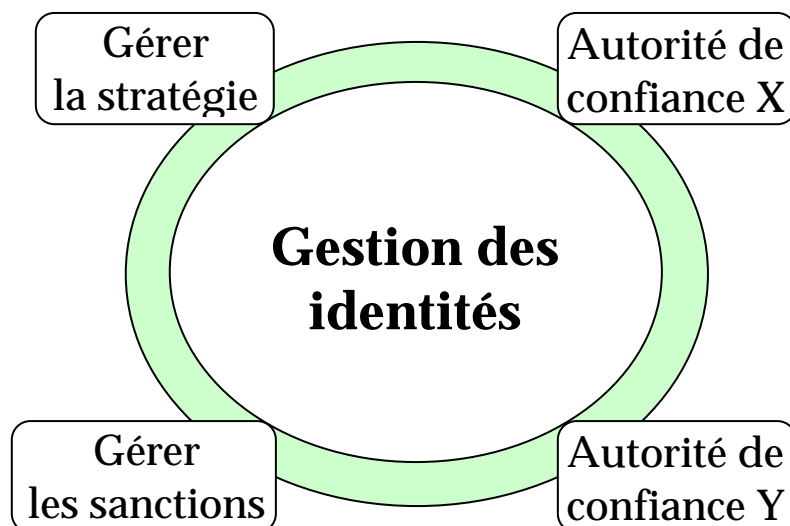


Figure 2.1: Les éléments de coopération dans ce modèle

2.1.1 Les autorités de confiance

L'autorité de confiance x (AC x) est un tiers de confiance dont la responsabilité est essentiellement analogue à celle d'un bureau chargé de l'émission des passeports dans un gouvernement.

L'autorité de confiance y (AC y) est un tiers de confiance dont la responsabilité est de délivrer les droits d'accès, analogue à l'émission des visas.

2.1.2 La gestion de stratégie

La gestion de la stratégie des identités sert à créer une stratégie d'attribution des droits d'accès, à la modifier et à la supprimer. Ceci est nécessaire au cas où des entreprises signent, suppriment ou modifient des accords entre elles. Par exemple il se peut que deux entreprises signent un nouvel contrat entre elles et donc de nouvelles règles d'attribution des droits doivent être établies entre elles pour faciliter par exemple l'échange des informations.

2.1.3 La gestion des sanctions

La gestion des sanctions sert à identifier l'intrusion des droits attribués, à définir des sanctions du titulaire d'un passeport ou d'un visa, à sanctionner les sujets en cas d'intrusion des droits d'accès et à vérifier aussi s'ils ont bien été sanctionnés.

2.2 Le modèle proposé

Réellement l'application de notre modèle nécessite la mise en place de trois serveurs ; HyperTopic Server, HyperPasseport Server et HyperGroup Server qui s'échangent continuellement des informations.

HyperTopic Server gère l'ensemble des droits d'accès attribués à travers du visa, la stratégie d'attribution des droits, et les sanctions.

HyperPassport Server gère la délivrance et la validité du passeport.

HyperGroup Server s'occupe des groupes de sujets. Comme nous l'avons vu dans l'état de l'art, le groupe joue un rôle important dans la gestion des identités et assure une coopération entre les sujets pour aboutir à un but commun ou réaliser une tâche commune.

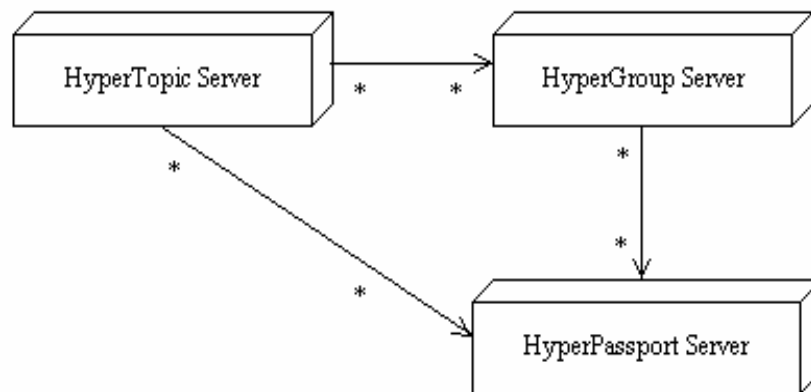


Figure 2.2: Les différents serveurs impliqués dans la gestion des identités

Nous allons modéliser à l'aide d'un diagramme de classe UML la relation entre les différentes entités qui rentrent dans la gestion des identités. Ce modèle est composé de trois packages : HyperTopic, HyperGroup et HyperPassport et de huit classes liés par des relations d'association, d'agrégation et de généralisation.

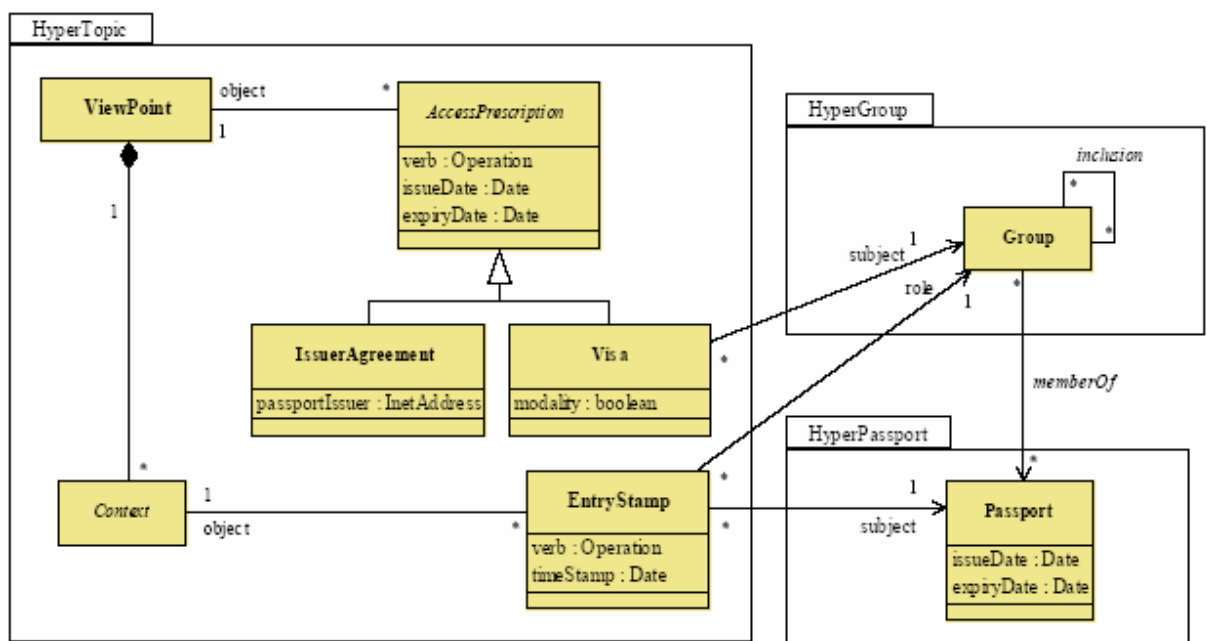


Figure 2.3: Modèle proposé pour la gestion des identités

Nous allons lister ses principales caractéristiques et ensuite le détailler par des exemples inspirés du système d'information d'une Université.

2.2.1 Le passeport

Le passeport est un document authentique, émis par une autorité de confiance (entreprise, société, etc.), pour l'autorité des autres qui certifie que son détenteur est bien la personne qu'elle prétend être. C'est le "document d'identité" de la personne. Toute société ou entreprise ayant confiance en l'autorité d'un bureau de passeports d'une autre société ou entreprise honorera les passeports des ressortissants de cette société. Tout comme un passeport, l'identité électronique de l'utilisateur d'un réseau, émise par une AC, est une preuve que cet utilisateur est connu de l'AC. Par conséquent, grâce au mécanisme de confiance entre les tiers, quiconque a confiance en l'AC, peut avoir confiance en l'identité de l'utilisateur. Les stratégies de gestion sont d'une importance primordiale pour déterminer le degré de confiance qu'on peut avoir dans les AC.

Pour prendre un exemple, chaque personne voulant accéder à un projet que nous désignons par *ViewPoint* (un ensemble de projets dans des contextes différents) doit posséder un passeport pour y accéder seulement si l'autorité lui ayant délivré le passeport, a confiance en l'autorité qui s'occupe de ce point de vue. Ce passeport est délivré par l'autorité de confiance de l'Université.

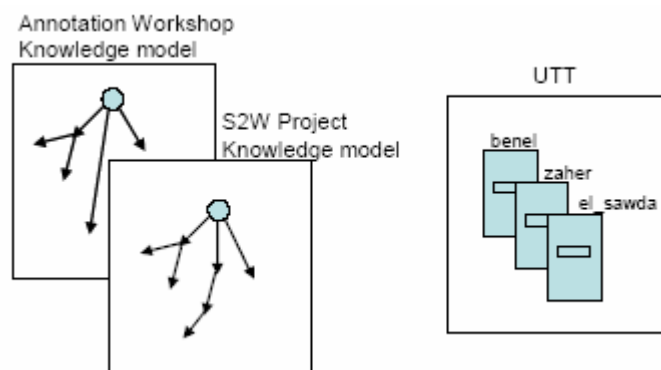


Figure 2.4: Représentation du passeport et du point de vue

Le passeport doit porter une date d'issue (issue date) et une date d'expiration (expiry date). Ces attributs servent à indiquer la durée de validité du passeport que nous supposons des éléments importants dans la gestion des identités.

Une personne peut avoir plusieurs passeports émis par différentes autorités de confiance. Comme exemple, on peut avoir un passeport pour accéder à un compte pour le travail et un autre passeport pour accéder à un compte personnel.

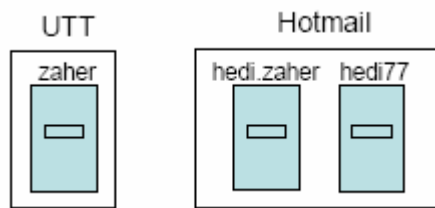


Figure 2.5: Plusieurs passeports pour une même personne

Le passeport est une marque de confiance temporaire, il doit être renouvelé régulièrement afin d'éviter qu'il ne soit utilisé illégalement par les autres en cas de perte.

Par exemple l'université peut avoir confiance en un étudiant tant que ce dernier continue ses études dans celle-ci, car l'administration peut toujours prendre des mesures disciplinaires en cas de problème avec l'étudiant. Mais si l'étudiant a terminé ses études, il n'est plus possible de le sanctionner. Pour éviter ce type de problème, son compte ne serait pas renouvelé s'il ne se réinscrit pas dans l'Université.

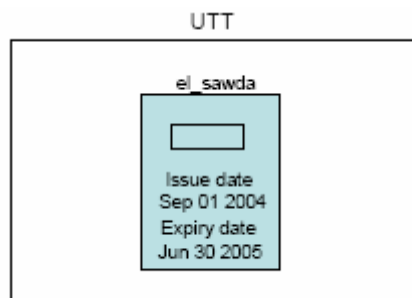


Figure 2.6: Durée de validité du passeport

Le passeport seul suffit (ceci dépend des frontières et de l'AC ayant délivré ce passeport). Mais dans ce cas des contrôles peuvent être effectués et des sanctions négatives sont appliquées.

Prenons l'exemple de l'Université qui fournit un droit d'accès de lecture en ligne de quelques magazines chers à ses étudiants et à tous ses employés. Ceci implique que le seul fait d'avoir un passeport de l'Université nous donne le droit de lire ces magazines.



Figure 2.7: Les frontières du passeport

2.2.2 Le Groupe

Le groupe est créé de lui-même sans l'intervention de l'autorité de confiance d'origine ni de l'autorité de confiance qui le reçoit. Chaque membre du groupe possède un passeport (donc plusieurs passeports dans le même groupe). Ce même passeport peut lui être utile pour être membre dans d'autres groupes.

Par exemple les étudiants se mettent en groupe librement pour travailler à des projets ensemble ou même pour effectuer des activités sportives sans aucune intervention de l'administration de l'université. El_Sawda possède un passeport lui permettant d'être membre du groupe « Students » et membre d'un groupe travaillant un projet sur le Web Socio Sémantique « S2W Taskforce »

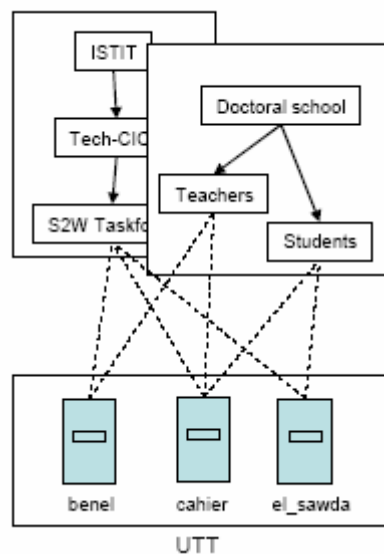


Figure 2.8 : Un même passeport dans plusieurs groupes

2.2.3 Le visa

Le passeport est délivré par une autorité de confiance, il sert à identifier une identité pour authentifier son propriétaire quant au visa, il est délivré par une autre autorité de confiance (AC y), attribue des permissions au propriétaire du passeport. Dans certains cas le passeport seul peut suffire. Ces deux types d'identification sont complémentaires.

Quand un visa est fourni à un groupe, l'autorité ayant délivré le visa accepte le groupe tel qu'il est listé. Par exemple, un enseignant peut donner accès à ses cours en donnant le visa pour un groupe défini par l'école doctorale.

Sur chaque visa est écrit l'opération que son propriétaire a le droit faire (Read, Write) et la modalité (positive + ou négative -)

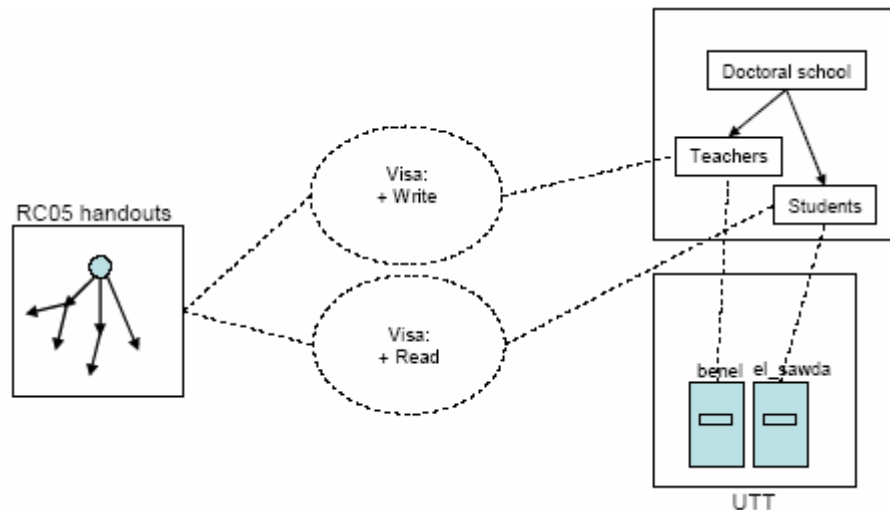


Figure 2.9: Visa de groupe

Le visa est aussi une marque de confiance temporaire. Comme exemple, on ne doit pas laisser accéder les étudiants aux solutions des exercices de l'année précédente tant que les étudiants n'ont pas suivi le cours et essayé de résoudre les exercices.

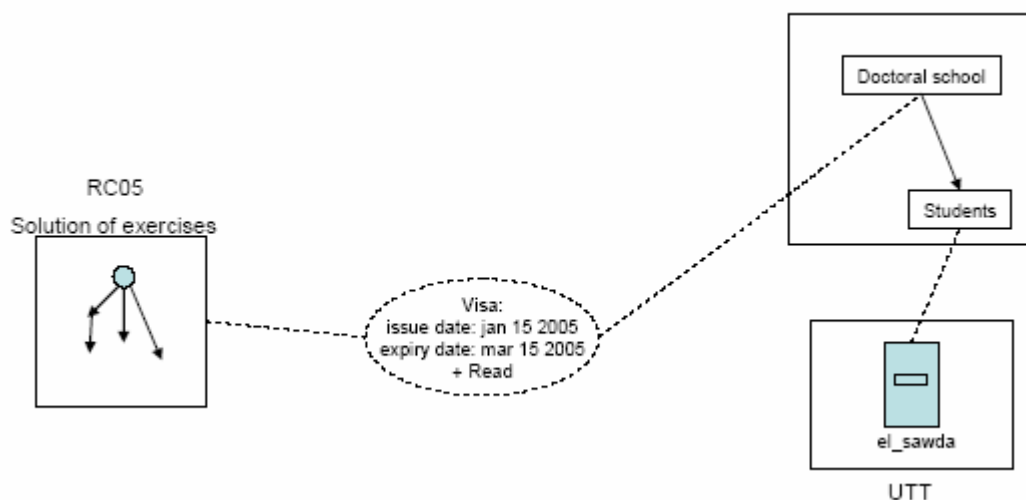


Figure 2.10: Visa comme marque de confiance temporaire

Un membre du groupe peut accéder avec deux rôles différents au même point de vue, chaque accès a aussi *une marque d'entrée* et *une opération*.

L'historique du visa est aussi pris en compte. En lisant l'historique, l'autorité de confiance peut être informée qui sont les étudiants qui ont été autorisé à lire les rapports administratifs (+ Read), et même savoir si le représentant des étudiants est maintenant impliqué avec un droit d'écriture (+ Write) sur ces rapports.

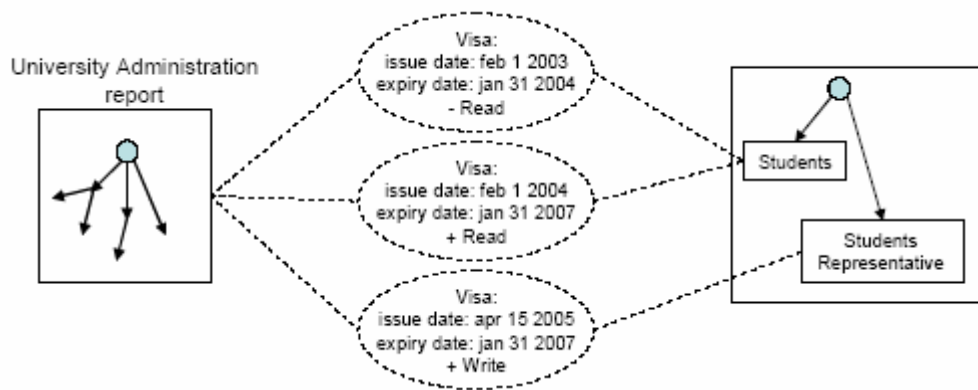


Figure 2.11: L'historique du visa

Comme le montre la figure ci-dessus, une modalité positive ou négative aussi bien pour les sujets que pour les groupes est indiquée sur le visa. Par exemple accès autorisés (+ Read) ou interdit (- Read) pour les groupes des étudiants (Students).

2.2.4 Marque de passage

Les marques de passage (Entry Stamp) servent à indiquer le droit d'accès du sujet (Read ou Write) et la date d'exécution de ces droits. Cette marque est adhérente au passeport et ne peut exister sans ce dernier.

Une marque de passage décrit les accès. Sur n'importe quelle marque, les données sont loin d'être plus précises que sur le visa (quel bordure, quel jour, quelle personne, dans quel groupe). L'historique des marques de passage est enregistré aussi.

Dans notre exemple, on suppose qu'une même personne a le droit de lire une partie du cours RC05 avec deux rôles différents. Si cette personne n'a pas eu de visa, le responsable du cours sera notifié et pourrait lui donner un visa positif ou négatif.

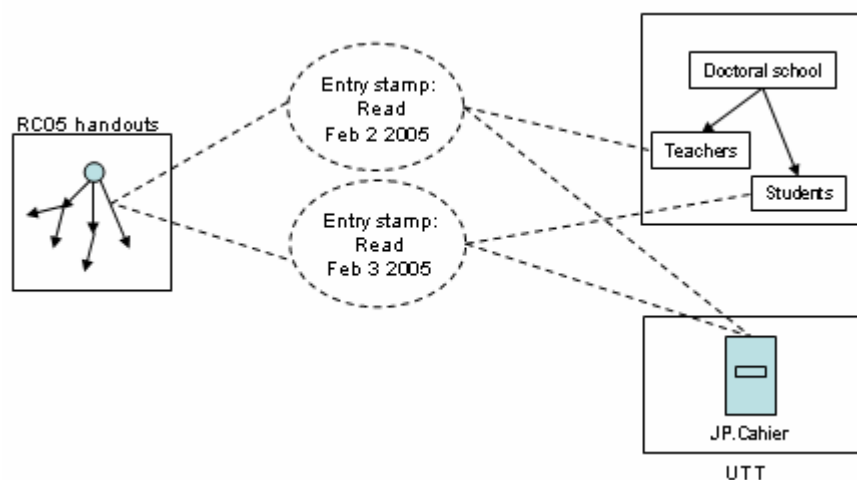


Figure 2.12: Description temporaire de l'accès avec la marque de passage

Conclusion

Nous nous sommes intéressés à question de la gestion des identités pour un Web Socio Sémantique, c'est-à-dire à la manière de gérer l'action de sujets connaissant (personnes, communautés) sur des modèles de connaissance. Notre but était non seulement *prescriptif* (gestion des accès) mais également *descriptif* (historique des modifications).

A partir d'un survol sur la question de l'identité en sciences humaines et identification de quelques problèmes théoriques et pratiques dans les modèles informatiques couramment utilisés (tous issus plus ou moins directement des premiers systèmes d'exploitation) nous avons proposé un modèle basé sur la métaphore du passeport dans lequel la structuration des sujets (tout comme celle des objets) est plurielle et dynamique et la gestion des droits d'accès est décentralisée.

Au-delà des ajustements du modèle (voire des modifications plus profondes) qui suivront nécessairement les premières expérimentations, s'ouvre un certain nombre de perspectives. La première concerne l'habilitation et la délégation des droits d'accès.

Un modèle de confiance distribué doit être implémenté pour fournir des fonctionnalités de délégations de privilèges. La décentralisation de la gestion des privilèges est donc nécessaire pour avoir un champ d'action plus large. Les privilèges du propriétaire d'un passeport peuvent être transmis à un autre. La seconde concerne une meilleure gestion de l'historique des droits d'accès dans le cadre de la gestion des identités dans le W2S.

Bibliographie

- [1] LECOMTE, J. Le Soi de l'enfance à l'âge adulte In : HALPERN, C. RUANO-BORBALAN, J.-C. *L'identité : l'individu, le groupe, la société*, 1998 p.33.
- [2] MARTINOT, D. Le Soi, les approches psychosociales In : HALPERN, C. RUANO-BORBALAN, J.-C. *L'identité : l'individu, le groupe, la société*, 1998 p.6.
- [3] RUANO-BORBALAN, J.-C. *L'identité : l'individu, le groupe, la société*, Auxerre, 1998, p 27.
- [4] LIPIANSKY, E.-M. Les fondements de l'identité In : HALPERN, C. RUANO-BORBALAN, J.-C. In : HALPERN, C. RUANO-BORBALAN, J.-C. *L'identité : l'individu, le groupe, la société*, 1998 p.41.
- [5] DORTIER, J.-F. L'individu dispersé et ses identités multiples In : HALPERN, C. RUANO-BORBALAN, J.-C. *L'identité : l'individu, le groupe, la société*, 1998, p 51-56.
- [6] LIPIANSKY, E.-M. Comment se forme l'identité des groupes In : HALPERN, C. RUANO-BORBALAN, J.-C. *L'identité : l'individu, le groupe, la société*, 1998, p 143.
- [7] ZAHER, H. BENEL, A. EL SAWDA, R. CAHIER J.-P. ZACKLAD, M. Identities Management for a Socio-Semantic Web, COOP 2005.
- [8] ZACKLAD, M. CAHIER, Jean-Pierre. PETARD, Xavier. Du Web Cognitivement Sémantique au Web Socio Sémantique, *Journée « Web Sémantique et SHS » du 7 mai 2003*, <http://www.lalic.paris4.sorbonne.fr/stic/as5.html>.
- [9] BERNERS-LEE, T. HENDLER, J. LASSILA, O. The Semantic Web Scientific American, May 2001, Feature article.
- [10] CAHIER, Jean-Pierre. ZACKLAD, Manuel. MONCEAUX, Anne : "Une application du Web socio-sémantique à la définition d'un annuaire métier en ingénierie", 15ème journées francophones d'Ingénierie de Connaissance, Lyon, 2004