Transaction de données sensibles au sein d'un Système Multi-Agent Hippocratique

L. Crépin[a,c] crepin@imag.fr
Y. Demazeau[a] Yves.Demazeau@imag.fr
O. Boissier[b] boissier@emse.fr
F. Jacquenet[c] jacquene@univ-st-etienne.fr

[a]Laboratoire d'Informatique de Grenoble, UMR 5217, CNRS

[b]Centre G2I
Ecole Nationale Supérieure des Mines de Saint-Etienne

[c]Laboratoire Hubert Curien, UMR 5516
Université Jean Monnet, Saint-Etienne, France

Résumé

L'évolution actuelle de l'informatique conduit à une multiplication des traitements automatiques des données qui transitent au sein des systèmes informatiques. Les données qui nous intéressent dans cet article sont les informations sensibles pour les utilisateurs ou les groupes d'utilisateurs. Un exemple typique est la circulation d'informations confidentielles concernant leur identité. Nous proposons une approche de ce problème, dans le cadre des systèmes multi-agents hippocratiques (HiMAS), modèle consistant à préserver le concept de privacy par une société d'agents. Dans ce contexte, nous présentons un protocole de communication d'informations sensibles permettant le respect de la sphère privée.

Mots-clés : *Sphère privée, transaction de données sensibles, confidentialité*

Abstract

The current evolution of Information Technology leads to the increase of automatic data processing over multiple information systems. The data we deal with concerns sensitive information about user or group of users. A typical example concerns the disclosure of confidential identity information. We propose an approach to this problem, in the context of Hippocratic Multi-Agent Systems (HiMAS), a model that preserves privacy using agency. In this context, we present a protocol of sensitive information communication that allows to preserve privacy.

Keywords: *privacy, sensitive data transaction, confidentiality*

1 Introduction

Au sein d'un système multi-agent (SMA), de nombreuses informations sensibles sont souvent amenées à transiter. Cet aspect des SMA n'a reçu que peu d'attention jusqu'à présent auprès des chercheurs du domaine. Le problème de la transmission d'informations sensibles au sein d'un SMA est d'autant plus présent dès lors qu'un utilisateur délègue ses informations sensibles à un agent autonome, les interactions étant essentielles dans les SMA.

Les Systèmes Multi-Agents Hippocratiques [7] prennent en compte la sensibilité des données. Ce modèle définit le concept de sphère privée pour la gestion de celles-ci ainsi que neuf principes à respecter pour s'assurer de leur protection. Dans cet article, nous nous intéressons à la protection des informations sensibles échangées lors des communications entre agents. Une telle communication est appelée transaction de données sensibles. Nous proposons ici un protocole de communication d'informations sensibles, inspiré de [24, 6], pour un HiMAS.

La prochaine section présente le modèle de Système Multi-Agent Hippocratique. La section 3 se consacre aux principes intervenant lors d'une transaction de données sensibles dans le but de définir notre protocole de communication d'informations sensibles. Finalement nous concluons et proposons quelques perspectives de travail.

2 Système Multi-agent Hippocratique (HiMAS)

Afin de présenter ce modèle, cette section aborde la sphère privée puis les neuf principes du modèle HiMAS et se termine par la sémantique de ceux-ci. Pour de plus amples informations sur cette section, le lecteur est invité à se référer à [7].

2.1 Sphère privée, consommateur et fournisseur

Nous avons défini la sphère privée comme l'ensemble des données estimées sensibles par agent ainsi que tous les éléments de gestion qui y sont associés [7]. Par exemple, dans notre contexte applicatif [9], ce type de données fait référence aux agendas que les utilisateurs délèguent aux agents.

A partir de nombreux travaux en sciences sociales, nous avons pu en définir les caractéristiques. Les droits de propriété de ce type d'information ne sont accordés qu'à l'agent concerné par cette information [22]. La sphère privée est également personnelle [10, 2], personnalisable [27, 26, 15] et elle dépend du contexte [3, 17].

Pour représenter les positionnements possibles d'un agent par rapport à la sphère privée, trois rôles ont été définis. Le rôle de **consommateur** caractérise l'agent qui demande l'information sensible, et celui de **fournisseur** décrit l'agent qui reçoit cette demande[1]. L'agent concerné par une information sensible incarne le rôle **sujet**.

2.2 Les neuf principes d'un HiMAS

L'étude de plusieurs travaux portant sur la sphère privée nous ont permis d'en définir les problématiques et de proposer un modèle, que nous avons appelé HiMAS (Hippocratic Multi-Agent Systems) qui permet la gestion et la protection de la sphère privée.

Le modèle HiMAS est inspiré du concept des bases de données hippocratiques proposées par Agrawal *et al.* [1]. Pour préserver la sphère privée, un HiMAS doit répondre aux neuf principes suivants.

1. **Consentement :** Chaque transaction de données sensibles requiert le consentement du fournisseur (et du sujet s'il ne s'agit pas du même agent).
2. **Connaissance des objectifs :** Le fournisseur doit connaître les objectifs pour lesquels les données sensibles sont demandées. Ainsi, s'il le souhaite, il a la possibilité de calculer les conséquences de cet échange.
3. **Collecte minimale :** Le consommateur s'engage à ne collecter que la quantité minimale de données nécessaire à la réalisation d'un même ensemble d'objectifs.
4. **Utilisation minimale :** Le consommateur s'engage à n'utiliser les informations sensibles demandées que pour satisfaire les objectifs qu'il a spécifié et rien de plus.
5. **Diffusion minimale :** Le consommateur s'engage à ne diffuser les informations sensibles que si ses objectifs l'exigent et ce seulement aux agents qui interviennent dans la réalisation de ces objectifs.
6. **Rétention minimale :** Le consommateur s'engage à ne conserver les informations sensibles que pendant un certain laps de temps, fixé au plus petit délai qu'il estime requis pour la réalisation de ses objectifs.
7. **Sécurité :** Le système doit garantir la sécurité des informations sensibles pendant leur stockage et durant les transactions.
8. **Transparence :** Les informations sensibles transmises au consommateur doivent rester accessibles au sujet et/ou fournisseur.
9. **Conformité :** Chaque agent doit être capable de vérifier le respect des principes précédents et de prévenir tout comportement malicieux ou déviant.

2.3 Sémantique des principes d'un HiMAS

Afin de définir plus précisément les principes d'un HiMAS, nous avons décidé de les étudier sous un aspect sémantique et de déterminer les différents liens qui existent entre eux, figure 1. Cette étude commence par le regroupement des principes en trois groupes intervenant à différentes étapes dans le raisonnement des agents d'un HiMAS : ceux qui entrent en jeu lors de la transmission de données sensibles, ceux qui interviennent lors des interactions entre agents et finalement ceux qui sont en lien avec le système.

Intéressons nous dans un premier temps aux principes qui entrent en jeu lors d'une transaction de données sensibles. Dans un tel contexte, le fournisseur définit une **politique** et le consommateur une **préférence** afin que chaque agent puisse définir ses désirs sur les manipulations des informations sensibles.

La politique du consommateur et la préférence du fournisseur sont semblables à celles définies dans [24] : elles comportent les objectifs[2] de la transaction, la date de suppression des informations recueillies, une liste de diffusion et le format de l'information (les références requises).

[1] Cette vision centrée utilisateur est à l'opposé de celle centrée service en terme de consommateur et de fournisseur.

[2] Les objectifs se rapprochent de la notion de désir, comme par exemple le modèle BDI [4] ou encore [19].

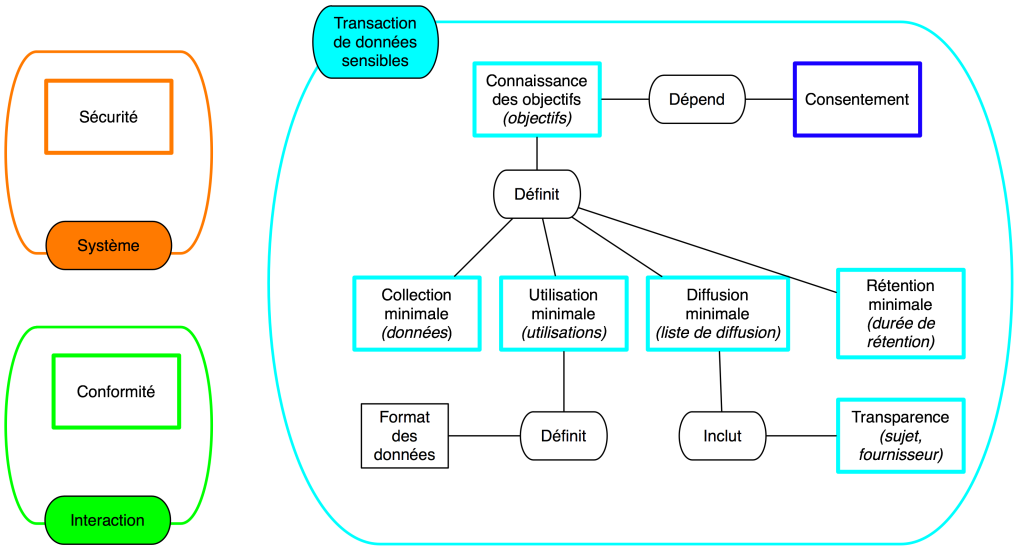

FIG. 1 – Graphe conceptuel de la sémantique des neuf principes d'un HiMAS

Afin de pouvoir mettre en correspondance une politique et une préférence, une transaction de données sensibles regroupe les informations sensibles à transmettre, mais également la politique et le consentement du fournisseur.

Sept des neuf principes des HiMAS entrent en jeu pour réaliser une transaction de données sensibles (figure 1) :

- **2. Connaissance des objectifs** : Le consommateur demande des informations sensibles à un fournisseur afin de réaliser certaines tâches qui lui sont requises. Ces tâches permettent de définir les objectifs du consommateur qui peut alors les transmettre au fournisseur.
- **3. Collection minimale** : Une fois que le consommateur a défini ses objectifs, il peut alors sélectionner les informations sensibles dont il a besoin pour réaliser ses objectifs.
- **4. Utilisation minimale** : Les objectifs étant définis, le consommateur peut déterminer les utilisations possibles des données recueillies.
- **5. Diffusion minimale** : La spécification des objectifs permet au consommateur de déterminer quels sont les agents qui peuvent recevoir les informations sensibles recueillies.
- **6. Rétention minimale** : La spécification des objectifs définit combien de temps le consommateur va pouvoir garder en mémoire les informations sensibles.
- **8. Transparence** : La transparence implique que le fournisseur et/ou le sujet appartiennent à la liste de diffusion.
- **1. Consentement** : La mise en correspondance entre une politique et une préférence représente le principe du consentement, établi après le respect des précédents principes.

Dans un deuxième temps, nous avons étudié les principes qui sont en relation avec les interactions. Ces interactions permettent la définition du principe **9. Conformité**.

Le dernier principe **7. Sécurité** ne concerne pas directement le raisonnement des agents d'un HiMAS. Ce principe intervient lors de la conception du système multi-agent et ne fait donc pas partie de la formalisation présentée dans ce document car il est indépendant du raisonnement des agent d'un HiMAS.

Dans cet article, nous souhaitons nous focaliser sur la problématique de la transaction de données sensibles dans un HiMAS. La section suivante présente ainsi une description des principes intervenant lors d'une telle transaction, nous amenant ainsi à définir notre protocole de communication d'informations sensibles.

3 Principes liés à une transaction de données sensibles

Les principes qui nous intéressent ici permettent aux agents de définir leur politique et leur préférence pour une transaction de données sensibles. Cette vision des principes requiert d'étudier préalablement les travaux existants sur les politiques portant sur des politiques, les méta-politiques. Ces principes ne s'appliquant qu'aux transactions de données sensibles, nous proposons de formaliser un protocole de communication d'informations sensibles s'appuyant sur des

méta-politiques pour décrire formellement ces principes et les implanter au sein d'un HiMAS.

Nous proposons de définir ces méta-politiques dans un dictionnaire qui définit les principes à respecter lors d'une transaction de données sensibles en guidant la conception d'une politique et d'une préférence à un niveau méta. Un dictionnaire applicatif est également considéré afin d'inclure les éléments contextuels pour le raisonnement des agents. Ces derniers construisent alors leur préférence et leur politique, et donc une transaction de données sensibles, en se référant au dictionnaire applicatif.

Ces dictionnaires doivent être communs aux agents d'un HiMAS afin que chaque agent fonde son raisonnement sur un même vocabulaire et une même sémantique. Nous choisissons de modéliser ces deux dictionnaires comme étant extérieurs aux agents et consultables par l'ensemble de ces derniers. De cette manière, les modifications apportées aux dictionnaires ne posent pas de problème de propagation et requièrent uniquement l'intervention d'une seule entité de contrôle.

Le protocole de communication d'informations sensibles que nous proposons est résumé dans la figure 2. L'avantage d'un tel procédé vient de la possibilité de vérifier les contraintes exprimées dans les principes d'un HiMAS grâce aux dictionnaires.

Nous commençons par présenter un panorama des principaux travaux existant dans le domaine des méta-politiques. Nous présentons ensuite une formalisation du protocole que nous proposons ainsi que des pistes d'implantation en étudiant d'abord le niveau méta, puis le niveau applicatif et finalement le niveau agent.

3.1 Méta-politiques

Cette section présente brièvement les principaux travaux qui existent sur les méta-politiques dans le but d'en fournir une vision générale. Les méta-politiques sont une spécialisation des méta-connaissances introduites par Pitrat [18] : elles portent sur des connaissances représentant uniquement des politiques de sécurité.

Les méta-politiques sont une notion introduite par Hosmer dans [12, 13]. Ces articles décrivent des politiques qui portent sur des politiques. Ces méta-politiques permettent de définir des règles de coordination sur les politiques de sécurité d'un système.

Les travaux de Kühnhauser [14] utilisent les méta-politiques pour l'interface de politiques complexes coexistantes et pour la coopération et la résolution de conflits entre politiques.

Les méta-politiques dans le système PONDER [16, 23] sont utilisés pour décrire les politiques de sécurité et résoudre les conflits.

Les méta-politiques ont en général pour objectif de gérer l'ensemble des politiques de sécurité d'un système en garantissant leur définition et la détection de conflits.

Les principes des HiMAS définissent des lignes directrices pour le raisonnement des agents et donc pour leur politique et préférence. Ainsi ces principes représentent des méta-politiques pour le comportement des agents en relation avec la communication et les manipulations des informations sensibles.

Cependant, dans notre cas d'étude[3], la notion de politique n'est pas la même que dans les travaux portant sur la sécurité. Les principes d'un HiMAS permettent aux agents de raisonner sur un ensemble de contraintes sur leur comportement et non de gérer l'ensemble des politiques des agents.

Cette différence nous amène à représenter autrement les principes d'un HiMAS. Sachant que la sphère privée est contextuelle, ces principes doivent donner une définition formelle et générique des lignes directrices de comportement que les agents prennent en compte lors d'une transaction de données sensibles. Afin de permettre aux agents de raisonner sur ces principes, nous les définissons dans un dictionnaire sous forme de graphe conceptuel [20] où chaque concept représente l'élément majeur d'un principe relié sémantiquement à un autre par une relation binaire, voir figure 1.

3.2 Niveau méta

Pour décrire les principes d'un HiMAS, nous nous sommes intéressés aux relations sémantiques qui existent entre eux, figure 1. Le principe central lors du raisonnement relatif à la transaction de données sensibles est **2. Connaissance des objectifs**. Ce principe permet aux agents de définir la durée de rétention, la collection de données, la liste de diffusion incluant le principe de transparence, les différentes utilisations possibles ainsi que le format de la donnée demandée (liste des références requises). A

[3] Le respect de la sphère privée au sein de systèmes multi-agents.

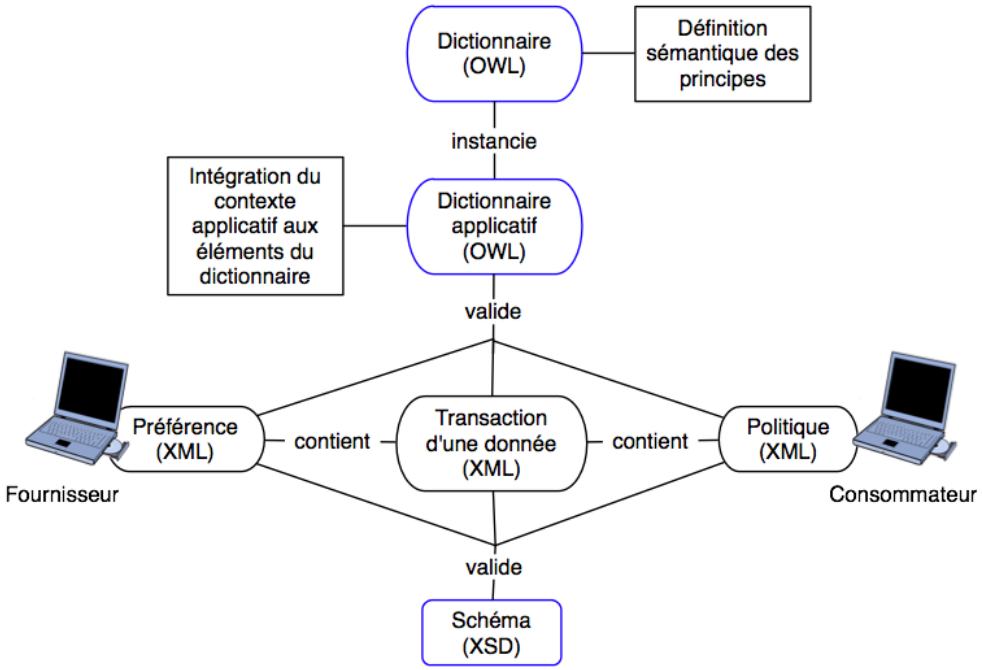

FIG. 2 – Protocole de communication d'informations sensibles

partir de la connaissance des objectifs, le fournisseur est également apte à donner ou non son consentement.

$\forall x\ objectifs(x)$	$\rightarrow\ \exists y\ définit(x,y) \wedge données(y)$
$\forall x\ objectifs(x)$	$\rightarrow\ \exists y\ définit(x,y) \wedge utilisations(y)$
$\forall x\ objectifs(x)$	$\rightarrow\ \exists y\ définit(x,y) \wedge listeDiffusion(y)$
$\forall x\ objectifs(x)$	$\rightarrow\ \exists y\ définit(x,y) \wedge duréeRétention(y)$
$\forall y\ utilisations(y)$	$\rightarrow\ \exists z\ définit(y,z) \wedge format(z)$
$\forall y\ listeDiffusion(y)$	$\rightarrow\ \exists z\ inclut(y,z) \wedge sujet(z)$
$\forall y\ listeDiffusion(y)$	$\rightarrow\ \exists z\ inclut(y,z) \wedge fournisseur(z)$
$\forall w\ consentement(w)$	$\rightarrow\ \exists x\ dépend(w,x) \wedge objectifs(x)$

TAB. 1 – Formalisation des principes.

Chaque principe et la notion de format de données représentent un concept relié à un autre selon un lien sémantique. Afin d'obtenir une définition formelle, nous utilisons un fragment de la logique existentiel, positif et conjonctif du premier ordre afin de ne pas obtenir d'informations logique contradictoires. Nous représentons ainsi chacun de ces concepts par un prédicat atomique et chaque relation par un prédicat binaire. La description formelle du graphe conceptuel de la figure 1 est décrite dans le tableau 1.

L'implantation de ce graphe conceptuel se fait par le biais d'une ontologie définie en OWL [25], figure 3. Ce procédé permet de définir les principes comme un ensemble de classes instanciables (*Objectifs* pour le principe **2. Connaissance des objectifs**, *Données* pour **3. Collecte minimale**, *Utilisations* pour **4. Utilisation minimale**, *ListeDiffusion* pour **5. Diffusion minimale** et *DuréeRétention* pour **6. Rétention minimale**) reliées par les relations sémantiques (*définit*, *inclut*).

3.3 Niveau applicatif

Les principes d'un HiMAS définissent à un niveau méta les différentes relations entre les principes que les agent doivent appliquer pour préserver la sphère privée. Ce niveau méta est à mettre en relation avec le contexte applicatif du HiMAS du fait de la contextualité de la sphère privée.

Le dictionnaire au niveau méta définit un vocabulaire pour le dictionnaire applicatif. Ce dernier instancie le dictionnaire du niveau méta en donnant toutes les valeurs possibles aux classes

```
<rdf:RDF>
  <rdfs:Class rdf:ID="Liste-diffusion"/>
  <rdfs:Class rdf:ID="Objectifs"/>
  <rdfs:Class rdf:ID="Données"/>
  <rdfs:Class rdf:ID="Durées"/>
  <rdfs:Class rdf:ID="Utilisation-possible"/>
 <owl:TransitiveProperty rdf:ID="définit">
    <rdfs:domain rdf:resource="#Objectifs"/>
    <rdf:type rdf:resource="owl#ObjectProperty"/>
    <rdfs:range>
     <owl:Class>
       <owl:unionOf rdf:parseType="Collection">
        <rdfs:Class rdf:about="#Durée-rétention"/>
        <rdfs:Class rdf:about="#Utilisations"/>
        <rdfs:Class rdf:about="#Données"/>
        <rdfs:Class rdf:about="#Liste-diffusion"/>
       </owl:unionOf>
     </owl:Class>
    </rdfs:range>
  </owl:TransitiveProperty>
</rdf:RDF>
```

FIG. 3 – Exemple d'implantation du dictionnaire au niveau méta

selon le contexte applicatif et en mettant en relation ses valeurs.

Nous considérons la gestion d'agendas distribués [9] comme contexte applicatif permettant d'illustrer notre proposition. Chaque utilisateur est représenté par un agent ayant en charge son emploi du temps qui peuvent être partagés avec les autres agents. Si les agents ne les partagent pas, un système de négociation est alors nécessaire pour fixer un rendez-vous.

Nous avons choisi un cas simple de transaction de données sensibles : fixer un rendez-vous de groupe. Nous considérons les créneaux de temps libres et occupés des agendas comme les informations sensibles.

Fixer un rendez-vous de groupe. Dans cet exemple, un consommateur veut fixer un rendez-vous avec un fournisseur et d'autres agents (groupe G) dans une période donnée (un intervalle de temps borné par deux créneaux de temps). La figure 4 illustre ce cas d'étude. Nous considérons ici que le fournisseur incarne également le rôle de sujet.

Pour fixer un tel rendez-vous, nous définissons les contraintes suivantes pour les agents :
- Les données sensibles que le consommateur peut collecter sont les créneaux libres pour une période donnée.
- Les données sensibles peuvent être fournies avec toutes les références que le fournisseur permet de diffuser.
- Les données recueillies par le consommateur ne peuvent pas être conservées en mémoire au-delà d'une date donnée.
- Le consommateur peut diffuser ces informations sensibles aux agents du groupe G et il doit en garantir l'accès au fournisseur.
- Les utilisations possibles des informations sensibles dans le contexte de la détermination d'un rendez-vous de groupe sont de stocker les informations recueillies, de les utiliser pour négocier un rendez-vous avec le fournisseur et de partager ces informations avec les agents du groupe G.

Le dictionnaire applicatif s'implante en instanciant les classes de la figure 3 avec les valeurs fournies dans la figure 4. Pour notre exemple, la classe *Objectifs* s'instancie par la valeur "fixer-rdv-groupeG" et cette valeur définit les valeurs "créneaux-libres", "négocier, stocker, diffuser", "date-donnée" et "agent-fournisseur, groupe G" pour les classes *Données*, *Utilisations*, *Durée-Rétention* et *ListeDiffusion*.

Ces deux dictionnaires définissent les sept principes d'un HiMAS liés au raisonnement des agents lors d'une transaction de données sensibles. Ils représentent le vocabulaire contextuel nécessaire aux agents pour se comprendre et envisager les différents impacts d'une transaction de données sensibles.

A partir des dictionnaires, le consommateur (resp. fournisseur) peut établir sa politique (resp. préférence) en respectant les contraintes imposées par les principes d'un HiMAS. Ce respect est assuré par le biais de la définition des liens sémantiques qui existent entre les concepts des principes d'un HiMAS.

3.4 Niveau agent

Nous nous s'intéressons ici à l'utilisation que peuvent faire les agents d'un HiMAS des deux dictionnaires présentés précédemment.

Nous définissons maintenant un protocole de communication pour les informations sensibles. Celui-ci est fondé sur ces deux dictionnaires et il spécifie la façon dont se déroulent les transactions de données au sein d'un HiMAS.

Lors d'une transaction de données sensibles, le consommateur (resp. fournisseur) construit sa politique (resp. préférence) en fonction de ses besoins et selon le dictionnaire applicatif (figure 2). Avant d'effectuer une transaction de données sensibles, les agents d'un HiMAS émettent un jugement les uns les autres pour juger de leur fiabilité [7]. Lorsque celle-ci est jugée satisfaisante, la transaction peut alors commencer. Cette fonction peut être implantée par exemple

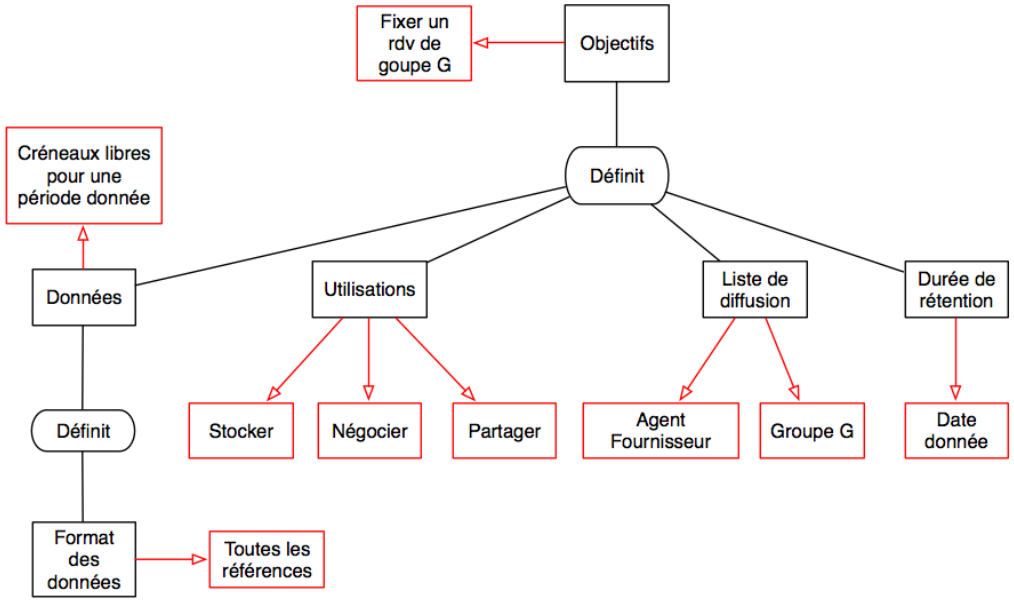

FIG. 4 – Instanciation du dictionnaire applicatif pour l'objectif "fixer un rendez-vous de groupe"

un processus de gestion de la confiance comme dans [8].

La préférence du fournisseur et la politique du consommateur sont spécifiées sous forme de fichiers XML devant se conformer à un schéma XSD prédéfini. Pour que le protocole soit mener à terme, une première contrainte impose donc que le fichier XSD valide le fichier XML.

Les valeurs présentes dans le XML doivent correspondre au vocabulaire décrit dans le dictionnaire applicatif. Il s'agit de la deuxième contrainte de notre protocole de communication d'informations sensibles.

Politique. Un consommateur construit sa politique en fonction des objectifs qu'il doit atteindre. La connaissance de ceux-ci permet donc à un agent de construire sa politique en utilisant le dictionnaire applicatif afin qu'il soit compris des autres agents et que son comportement soit respectueux de la sphère privée.

Dans notre dictionnaire applicatif, les objectifs du consommateur sont reliés sémantiquement à tous les autres principes utilisés dans une transaction de données sensibles. Le dictionnaire applicatif contient pour chaque objectif toutes les valeurs possibles pour les classes représentant ces principes. Ainsi un consommateur peut savoir s'il viole la sphère privée ou non en vérifiant que les éléments de sa politique soient contenus dans le dictionnaire applicatif et qu'ils respecte les relations sémantiques.

Afin de définir entièrement notre protocole, il faut que cette politique soit syntaxiquement correcte par rapport au XSD. Une politique doit donc contenir la spécification des objectifs, la date de suppression des données sensibles collectées, la liste de diffusion de ces informations et l'ensemble des références demandées pour chaque information, figure 5 et tableau 2.

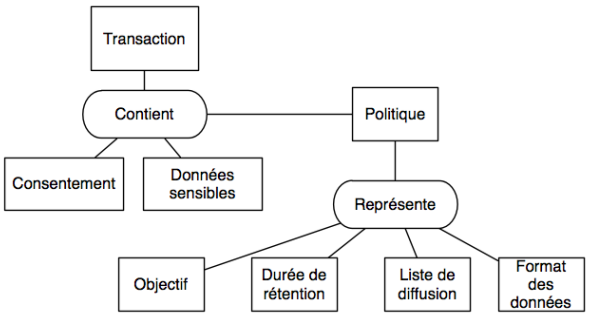

FIG. 5 – Description d'une transaction de données sensibles

Une fois que le consommateur a déterminé ses objectifs et les concepts dépendant de ce dernier, il construit une politique syntaxiquement correcte grâce au schéma prédéfini XSD et sémantiquement correcte grâce au dictionnaire applicatif.

Transaction de données sensibles. Une fois que le consommateur a défini et validé sa politique, la transaction de données sensibles peut se réaliser

$\forall y\, politique(y)$	$\rightarrow \exists z\ représente(y,z) \wedge objectif(z)$
$\forall y\, politique(y)$	$\rightarrow \exists z\ représente(y,z) \wedge format(z)$
$\forall y\, politique(y)$	$\rightarrow \exists z\ représente(y,z) \wedge listeDiffusion(z)$
$\forall y\, politique(y)$	$\rightarrow \exists z\ représente(y,z) \wedge duréeRétention(z)$

TAB. 2 – Formalisation des politiques.

à son initiative.

Nous avons défini une transaction de données sensibles comme un ensemble contenant une politique, une préférence, le consentement du fournisseur et les informations sensibles demandées par le consommateur.

Chacune des valeurs possibles pour les éléments d'une transaction de données sensibles est définie dans le dictionnaire applicatif afin que le consommateur construise une transaction valide pour le respect de la sphère privée d'un point de vue sémantique.

$\forall y\, transaction(y)$	$\rightarrow \exists z\ contient(y,z) \wedge consentement(z)$
$\forall y\, transaction(y)$	$\rightarrow \exists z\ contient(y,z) \wedge données Sensibles(z)$
$\forall y\, transaction(y)$	$\rightarrow \exists z\ contient(y,z) \wedge politique(z)$

TAB. 3 – Formalisation des transactions de données sensibles.

Pour construire une transaction de données sensibles correcte d'un point de vue syntaxique, nous adoptons le même procédé que pour une politique. Nous définissons une transaction de données sensibles d'un point de vue formel (tableau 3 et figure 5). Notons que ce formalisme ne fait pas référence à la préférence du fournisseur. En effet, une préférence et une politique s'appuyant des mêmes concepts, nous modélisons la préférence du fournisseur par les modifications qu'il induit à la politique du consommateur si elle ne lui convient pas.

Une fois le fichier de la transaction de données sensibles créé et validé, le consommateur peut alors l'envoyer au fournisseur afin que ce dernier prenne connaissance de sa requête.

Préférence. A partir des éléments de gestion de sa sphère privée, un fournisseur établit les règles d'utilisation, de diffusion, de rétention des informations sensibles qu'il détient. Une fois qu'il a reçu une transaction de données sensibles, ces règles lui permettent d'accepter ou non la politique du consommateur.

Avant de s'intéresser à la politique du consommateur, le fournisseur doit en premier lieu vérifier la validité de la transaction d'un point syntaxique (vérification des schémas) et d'un point de vue sémantique (vérification du dictionnaire applicatif). Ces deux validations permettent de déterminer si un consommateur a un comportement malicieux sur les limitations imposées par les principes d'un HiMAS et sur le protocole de communication d'informations sensibles.

Si la transaction de données sensibles est validée, le fournisseur peut alors mettre en correspondance sa préférence avec la politique du consommateur. Dans le cas où cette mise en correspondance échoue, le fournisseur peut proposer des adaptations de la politique du consommateur et la lui renvoyer.

Une fois le consommateur et le fournisseur en accord sur les termes de la politique, le fournisseur complète la transaction de données sensibles avec les valeurs des informations sensibles demandées. Si aucun accord n'est trouvé, la transaction n'aboutit pas et le fournisseur ne peut pas satisfaire la requête du consommateur.

3.5 Protocole de communication d'informations sensibles

La figure 6 présente le protocole de transactions d'informations sensibles que nous venons de présenter. D représente le dictionnaire applicatif, C le consommateur, Po sa politique et F le fournisseur, Pr sa préférence.

Ce protocole de communication est centré utilisateur et se place à l'opposé des protocoles de communication rencontrés dans la littérature qui sont essentiellement centrés service. Il reprend les principes de [24] et modélise une transaction de données sensibles à l'instar d'une interaction dans ISLANDER [11]. Pour que le respect de la sphère privée soit complet, ce protocole doit être intégré à un média de communication sécurisé (principe **7. Sécurité**).

4 Conclusion et perspectives

Notre protocole de communication d'informations sensibles permet d'appliquer sept principes d'un HiMAS : **1. Consentement**, **2.**

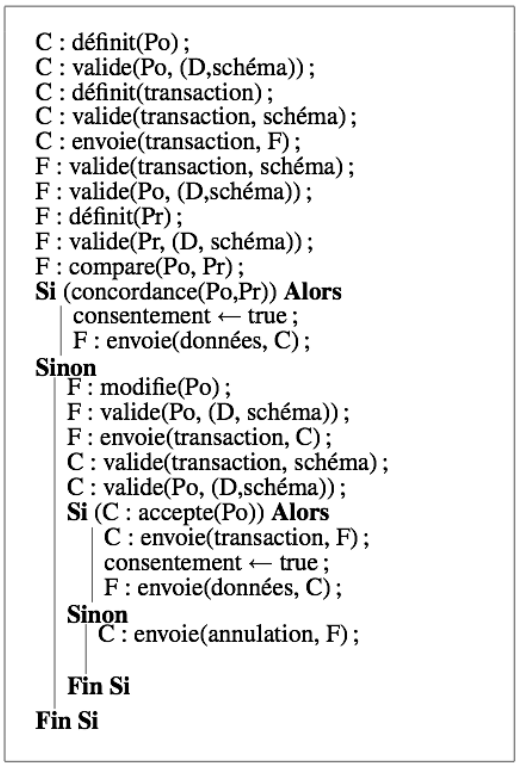

FIG. 6 – Protocole de communication d'informations sensibles

Connaissance des objectifs, **3. Collecte minimale**, **4. Utilisation minimale**, **5. Diffusion minimale**, **6. Rétention minimale** et **8. Transparence**.

Le respect de ces principes s'effectue en considérant notre protocole selon trois niveaux. Au niveau **méta**, les principes sont définis dans un dictionnaire les reliant. Le niveau **applicatif** représente l'instanciation de ce dictionnaire selon le contexte applicatif. Au niveau **agent**, les agents utilisent le dictionnaire applicatif pour construire une transaction de données sensibles.

En liant les principes, nous déterminons dans le dictionnaire applicatif l'ensemble maximal des manipulations de données sensibles qu'un consommateur peut exécuter sur celles qu'il recueille. Un fournisseur peut alors vérifier qu'un consommateur respecte les principes limitatifs en se référant à ce dictionnaire. Afin qu'aucun principe ne soit omis, nous formalisons également cette interaction spécifique. Cette formalisation contribue également à la détection d'un agent malicieux (qui ne la respecte pas).

Le fait d'inclure un dictionnaire applicatif dans notre protocole permet de ne pas être confronté au même problème que le P3P [21] : la mise en correspondance entre une politique et une préférence se fait en fonction du dictionnaire applicatif, ce qui permet aux agents de comprendre les intentions des consommateurs. Un autre avantage de l'introduction d'un dictionnaire applicatif réside en la possibilité de définir les limitations imposées par les principes d'un HiMAS.

Les principes liés au raisonnement des agents lors d'une transaction de données sensibles étant définis, nos perspectives de travail se portent maintenant sur le principe de conformité qui est relié à la problématique de l'interaction entre agents. Une première piste consiste à instaurer un contrôle social [5] en relation avec la fonction de jugement des agents. Nous envisageons de modéliser cette fonction par un processus de construction et de gestion de la confiance.

Remerciements : Ce travail a bénéficié d'un soutien du projet Web Intelligence, financé par le cluster ISLE de la région Rhône-Alpes. Nous remercions également France Télécom R&D pour son financement sur les recherches en relation avec la confiance mentionnées dans cet article.

Références

[1] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Hippocratic databases. In *Proceedings of the International Conference Very Large Data Bases (VLDB)*, pages 143–154. Morgan Kaufmann, 2002.

[2] Sara Baase. *A Gift of Fire : Social, Legal, and Ethical Issues in Computing*. Prentice-Hall, 2003.

[3] Victoria Bellotti and Abigail Sellen. Design for privacy in ubiquitous computing environments. In *Proceedings of the European Conference on Computer Supported Cooperative Work (ECSCW)*, pages 75–. Kluwer Academic Publishers, 1993.

[4] M. E. Bratman. Intention, plans, and practical reason. O'Reilly, Harvard University Press : Cambridge,MA, 1987.

[5] Cristiano Castelfranchi. Engineering social order. In *Proceeding of the First International Workshop Engineering Societies in the Agent World (ESAW)*, volume 1972 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2000.

[6] Lorrie Faith Cranor. *Web Privacy with P3P*. O'Reilly, 2002.

[7] Ludivine Crépin, Laurent Vercouter, François Jaquenet, Yves Demazeau, and Olivier Boissier. Hippocratic multi-agent systems. In *Proceedings of the 10th International Conference of Entreprise Information Systems (ICEIS), Barcelona*, pages 301–308, 2008.

[8] Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, and Pierangela Samarati. P2P-based collaborative spam detection and filtering. In *Proceedings of 4th International Conference on Peer-to-Peer Computing*, 2004.

[9] Yves Demazeau, Dimitri Melaye, and Marie-Hélène Verrons. A decentralized calendar system featuring sharing, trusting and negotiating. In *Proceedings of the International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (IEA/AIE)*, volume 4031 of *Lecture Notes in Computer Science*, pages 731–740. Springer, 2006.

[10] Pierre Demeulenaere. Les difficultés de la caractérisation de la notion de la vie privée d'un point de vue sociologique. In *La protection de la vie privée dans la société d'information*, volume 11, 2002. Groupe d'études Société d'information et vie privée.

[11] Marc Esteva, David de la Cruz, and Carles Sierra. Islander : an electronic institutions editor. In *Proceedings of the First International Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS)*, pages 1045–1052. ACM, 2002.

[12] Hilary H. Hosmer. Metepolicies I. *ACM SIGSAC Data Management Workshop*, 10(2-3) :18–43, 1991.

[13] Hilary H. Hosmer. Metepolicies II. In *Proceeding of the 15th National Computer Security Conference*, pages 369–378. Elsevier Advanced Technology Publications, 1992.

[14] Winfried E. Kühnhauser. A paradigm for user-defined security policies. In *Symposium on Reliable Distributed Systems*, pages 135–144, 1995.

[15] Lawrence Lessig. *Code and Other Laws of Cyberspace*. Basic Books, New York, 2000.

[16] Emil Lupu, Morris Sloman, Naranker Dulay, and Nicodemos Damianou. Ponder : Realising enterprise viewpoint concepts. In *Proceeding of the 4th International Enterprise Distributed Object Computing Conference (EDOC)*, pages 66–75. IEEE Computer Society, 2000.

[17] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In *Proceedings of the 2003 Conference on Human Factors in Computing Systems (CHI)*, pages 129–136. ACM, 2003.

[18] Jacques Pitrat. *Métaconnaissance, Futur de l'Intelligence Artificielle*. Hermés, 1990.

[19] Jaime Simão Sichman and Yves Demazeau. Exploiting social reasoning to deal with agency level inconsistency. In *Proceedings of the First International Conference on Multiagent Systems (ICMAS)*, pages 352–359. The MIT Press, 1995.

[20] John F. Sowa. *Conceptual Structures : Information Processing in Mind and Machine*. Addison-Wesley, 1984.

[21] Robert Thibadeau. A critique of P3P : Privacy on web, dollar.ecom.cmu.edu/p3pcritique/. 2000.

[22] Judith J. Thomson. The right of privacy, 1975. Philosophy and Public Affairs 4 : 295-314.

[23] Kevin P. Twidle and Emil Lupu. Ponder2 - policy-based self managed cells. In *Proceeding of the First International Conference on Autonomous Infrastructure, Management and Security (AIMS)*, volume 4543 of *Lecture Notes in Computer Science*, page 230. Springer, 2007.

[24] W3C. Plateform for privacy preferences, http ://www.w3.org/p3p/. 2002.

[25] W3C. Owl web ontology language, http ://www.w3.org/tr/owl-features/. 2004.

[26] Samuel D. Warren and Louis D. Brandeis. *The right to privacy*. Wadsworth Publ. Co., Belmont, CA, USA, 1985.

[27] Alan F. Westin. Special report : legal safeguards to insure privacy in a computer society. *Commun. ACM*, 10(9) :533–537, 1967.