# Préservation de l'Intimité dans les Protocoles de Conversations

Nawal Guermouche*, Salima Benbernou**
Emmanuel Coquery**, Mohand-Said Hacid**

*LORIA, INRIA Lorraine, Campus scientifique,
BP 239, 54506 Villiers-Lès-Nancy.
nawal.guermouche@loria.fr,
**LIRIS - UFR d'Informatique,
Université Claude Bernard Lyon 1,
43, boulevard du 11 Novembre 1918,
69622 Villeurbanne cedex.
{salima.benbernou,emmanuel.coquery,mshacid}@liris.cnrs.fr

**Résumé.** Le travail présenté dans cet article, rentre dans le cadre de la gestion des données privées en vue de la substitution, appelée remplaçabilité, dynamique des services Web. Trois contributions sont apportées, (1) modélisation des politiques privées spécifiant les règles d'utilisation des données privées, prenant en compte des aspects se rapportant aux services Web, (2) étendre les protocoles de conversations des services Web par le modèle proposé, afin d'apporter les primitives nécessaires pour l'analyse des protocoles en présence de ces règles, (3) définition d'un mécanisme d'analyse de la remplaçabilité d'un service par un autre en vue de ses politiques privées.

En se reposant sur des standards, les services Web sont devenus le candidat naturel à une architecture d'échange inter-applications, à la fois au sein d'une entreprise et également en B2B. Pour réaliser des services, les entreprises ont souvent besoin de collecter des données privées de leurs clients. La sensibilité de l'échange des données privées a fait naître le besoin de définir des règles guidant l'utilisation de ces données. Dans cette optique, plusieurs travaux ont été développés visant à fournir des mécanismes et des modèles expressifs [Agrawal et al. (2005), Kagal et al. (2004)]. Principalement nous citons la plate-forme *P3P* qui est une plateforme de standardisation et de spécification des politiques privées pour les sites Web [Agrawal et al. (2003)].

Dans cet article, nous introduisons le modèle des règles privées que nous avons proposé ainsi que son intégration aux protocoles de conversation [Benatallah et al. (2004)]. Ceci afin d'apporter les primitives nécessaires pour l'analyse de la remplaçabilité des services Web en vue de ces règles. Sachant qu'un service Web peut être un client ou un fournisseur, nous distinguons deux types de règles : (1) Les règles spécifiées par le service fournisseur appelées *politiques privées* [Agrawal et al. (2003)], et (2) Les règles spécifiées par le service client appelées *préférences privées* [Agrawal et al. (2003)].

- *Les politiques* : Nous définissons une politique comme étant un ensemble de *termes d'utilisation des données* noté *TUD*. Un *tud* $\in$ *TUD* défini la *donnée* ainsi que le *but*, appelé *Purpose*, pour lequel la donnée a été collectée. Pour réaliser un but, le fournisseur peut exiger d'avoir le choix de réaliser d'autres opérations qu'on appelle *Rights*. En outre, pour assurer la sécurité des données collectées, on associe aux *Purposes* et aux *Rights* des opérations appelées *Obligations* ayant pour but la sécurité des données collectées.
- *Les préférences* : Les préférences d'un service client, définies comme une politique, sont composées de deux parties : (1) *préférences locales* concernent les propres données privées du service, et (2) *préférence externes* concernent les données privées collectées par le service auprès de ses clients. Pour tenir compte des restrictions des clients dans les préférences du service fournisseur, nous proposons d'extraire automatiquement les préférences externes des politiques.

Afin d'intégrer les règles privées aux services Web, nous avons proposé d'étendre leurs protocoles de conversations i.e les séquences de méssages supportées par un service Web [Benatallah et al. (2004)]. Le résultat de cette extension a donné ce que nous avons appelé *protocoles de conversations privées*.

En se basant sur le niveau de restrictions des politiques, nous avons proposé trois classes de remplaçabilité des politiques privées : (1) *remplaçabilité privée totale*, (2) *équivalence privée*, (3) et *remplaçabilité privée partielle*. Ces trois classes nous ont permis d'étendre la notion de simulation des protocoles de conversations privées [Benatallah et al. (2004)].

## Références

Agrawal, R., T. W. Grandison, P. Bird, S. Logan, W. Rjaibi, et G. Kiernan (2005). Extending relational database systems to automatically enforce privacy policies. *International Conference on Data Engineering*.

Agrawal, R., J. Kiernan, R. Srikant, et Y. Xu (2003). Implementing p3p using database technology. *International Conference on Data Engineering (ICDE'03)*, 595.

Benatallah, B., F. Casati, et F. Toumani (2004). Analysis and management of web service protocols. *Int: Procs of ER'04, Shanghai, China.*.

Kagal, L., M. Paolucci, N. Srinivasan, G. Denker, T. Finin, et K. Sycara (2004). Authorization and privacy for semantic web services. *IEEE Intelligent Systems (Special Issue on Semantic Web Services)*.

## Summary

In this paper, we propose an approach for the replaceability of Web services regarding their privacy policies. In this context, we present a model of privacy rules, and we show how we integrate it in the definition of business protocols which gave *Private business protocols*. We also, propose a mechanism for analyzing replaceability between Web services according to their private business protocols.