

## Rapport d'activité n°1 (12 mois)\*

### A. Identification

Programme – année	ARA – SSIA - 2005
Projet (acronyme)	Cops
Nom du coordonnateur du projet et affiliation (société/organisme - laboratoire ou entité de rattachement)	Philippe Balbiani Institut de recherche en informatique de Toulouse
Référence convention ou décision	Décision n° ANR-05-SSIA-0007-01
Projet : date de début – date de fin	Composition de politiques et de services 24 janvier 2006 - 23 janvier 2009
Période faisant l'objet du rapport d'activité (date début – date fin)	24 janvier 2006 - 30 novembre 2006
Rédacteur de ce rapport : nom	Philippe Balbiani
téléphone	05.61.55.60.91
adresse électronique	balbiani@irit.fr
Date du rapport	30 novembre 2006

**B. Rappel des tâches allouées par partenaire pour l'ensemble du projet** (partir du planning généralement fourni dans le projet. Ce document est à remplir par le coordonnateur du projet à partir des informations fournies par chacun des partenaires)

*Ce tableau (à compléter) décrit les principales tâches du projet qui ont été définies lors de son démarrage*

Tâches du projet	Partenaires concernés par la tâche (2)		2006		2007	2008	Commentaires
			Semestre 1 (1)	Semestre 2 (1)			
Langages pour l'expression de politiques de sécurité	P1, P2, P3	Prévue/Nouvel le	P		P	P	
		Réalisée/Abandonnée		R			
Combinaison de politiques de sécurité et de services électroniques	P1, P2, P3	Prévue/Nouvel le	P		P	P	
		Réalisée/Abandonnée		R			
Algorithmes pour la composition de services électroniques	P1, P2, P3	Prévue/Nouvel le	P		P	P	
		Réalisée/Abandonnée		R			

(1) P=Prévue, N=Nouvelle, R=Réalisée, A=Abandonnée (dans ce dernier cas, justifier obligatoirement avec un commentaire)

(2) Partenaires concernés : ceux-ci sont à expliciter dans un tableau (cf. ci-dessous)

Partenaire P1	Institut de recherche en informatique de Toulouse / Toulouse / Equipe Lilac	Philippe Balbiani
---------------	---	-------------------

\* Le canevas pour ce premier rapport dit « à 12 mois » sera également à utiliser pour les rapports semestriels suivants

Partenaire P2	Laboratoire lorrain de recherche en informatique et ses applications et Laboratoire d'informatique de l'université de Franche-Comté / Nancy et Besançon / Projet Cassis	Michael Rusinowitch
Partenaire P3	Laboratoire d'informatique fondamentale de Marseille / Marseille / Equipe Move	Denis Lugiez

## Eléments qualitatifs

### C. Description des travaux effectués pour la période concernée et conformité de l'avancement aux prévisions (15 à 50 lignes maximum suivant le nombre de partenaires)

**(1) Langages pour l'expression de politiques de sécurité :** Considérant, dans un premier temps, qu'un service électronique pouvait être assimilé à un processus, nous avons exploré le mode de contrôle d'accès qui répond le mieux aux besoins de la programmation orientée service. Trois concepts, le temps, le coût et la confiance, nous semblent nécessaires pour le définir. Olivier Perrin (Loria) et Christophe Ringeissen (Loria) pensent qu'un service a besoin d'exprimer sa politique de contrôle d'accès par l'intermédiaire de contraintes temporelles. Pour ce faire, ils étendent le modèle Colombo par des contraintes qualitatives et quantitatives. Olga Kouchnarenko (LIFC) et Jérôme Voinot (LIFC) pensent qu'un service définit aussi son mode de fonctionnement à travers la notion de coût qu'ils intègrent à la relation de transition du modèle CCS. Philippe Balbiani (Irit) et Fahima Cheikh (Irit) pensent que la notion de confiance est essentielle dans un environnement distribué comme celui des services où les échanges se fondent par l'envoi et la réception de certificats.

**(2) Combinaison de politiques de sécurité et de services électroniques :** Yannick Chevalier (Irit), Denis Lugiez (Lif) et Michael Rusinowitch (Loria) analysent les services électroniques au niveau des messages XML qu'ils échangent. Pour ce faire, ils modélisent ces messages par des termes constitués de constructeurs associatifs et de constructeurs associatifs/commutatifs pour désigner les fils d'un noeud. Ce travail a nécessité une extension significative des résultats connus sur la décidabilité de certains problèmes d'accessibilité. Yannick Chevalier, Denis Lugiez et Michael Rusinowitch travaillent également sur l'extension du modèle d'intrus avec des contraintes de sous-termes qui permettent l'expression de contraintes comme "le message doit contenir la signature de l'élément body".

**(3) Algorithmes pour la composition de services électroniques :** Nous avons exploré la difficulté intrinsèque du problème de la composition des services électroniques. Olga Kouchnarenko et Jérôme Voinot ont étudié le problème du remplacement et de la compatibilité entre services intégrant la notion de coût. Dans le cadre du modèle basé sur la notion de confiance, Philippe Balbiani et Fahima Cheikh ont montré que le problème de la composition des services est indécidable et ont défini des classes d'instances pour lesquelles ce problème devient décidable.

### D. Résultats obtenus pour la période concernée, dégager notamment les faits marquants (15 à 50 lignes maximum) *Décrire les résultats obtenus et préciser éventuellement les livrables déjà réalisés en interne au projet.*

**(1) Langages pour l'expression de politiques de sécurité :** Application des automates temporisés à la programmation orientée service (Perrin, Ringeissen). Définition d'un nouveau type d'automates finis, les automates conditionnels et étude de la complexité de la bisimulation et de l'équivalence des traces entre automates conditionnels (Balbiani, Cheikh). Intégration de la notion de confiance (Balbiani, Cheikh). Application de CCS à la programmation orientée service (Kouchnarenko, Voinot). Intégration de la notion de coût (Kouchnarenko, Voinot).

**(2) Combinaison de politiques de sécurité et de services électroniques :** Le travail sur les termes constitués de constructeurs associatifs et de constructeurs associatifs/commutatifs est en cours d'achèvement avec la définition d'une procédure de décision pour la sécurité des services électroniques qui utilisent le chiffrement avec des messages de profondeur XML bornée (Chevalier, Lugiez, Rusinowitch). Une réunion entre Yannick Chevalier, Denis Lugiez et Michael Rusinowitch est prévue en décembre à Marseille pour travailler sur ces questions.

**(3) Algorithmes pour la composition de services électroniques :** Nous travaillons encore à l'élaboration d'algorithmes pour la composition de services électroniques qui intègrent les concepts de temps, de coût et de confiance. Une réunion entre des membres du Loria et de l'Irit est prévue en février à Nancy pour travailler sur la difficulté intrinsèque du problème de la composition des services électroniques qui intègrent les notions de temps et de confiance. Une réunion entre des membres du LIFC et de l'Irit est prévue en février à Besançon pour travailler sur la difficulté intrinsèque du problème de la composition des services électroniques qui intègrent les notions de coût et de confiance.

**E. Difficultés rencontrées et solutions de remplacement envisagées (15 à 50 lignes maximum)** *ex : impasse technique, abandon d'un partenaire ou d'un sous traitant, maîtrise des délais, maîtrise des budgets. Faut-il revoir le contenu du projet ? Faut-il revoir le calendrier du projet ?*

**(1) Langages pour l'expression de politiques de sécurité :** Aucune.

**(2) Combinaison de politiques de sécurité et de services électroniques :** Aucune.

**(3) Algorithmes pour la composition de services électroniques :** Aucune.

**F. Livrables externes réalisés (15 à 50 lignes maximum)**

*Pour les articles et communications écrites, préciser s'il s'agit d'articles dans des revues à comité de lecture / d'ouvrages ou chapitres d'ouvrage / d'articles dans d'autres revues / de communications dans des colloques ou des congrès / de dépôt de brevet... Référencer selon les normes habituelles. Mentionner également s'ils peuvent ou non faire l'objet de communications externes par l'ANR et son unité support*

Indiquer, *Le cas échéant*, les thèses démarrées, en cours et/ou soutenues en relation directe avec le projet :

*Préciser le titre, date de soutenance (prévue ou réelle), soutien financier, devenir des étudiants pour les thèses soutenues*

Publications :

[1] P. Balbiani, F. Cheikh. A propos du problème de la composition des services électroniques. Fac 2006.

[2] P. Balbiani, Y. Chevalier, M. Kourjeh. Reasoning about actions and obligations. FCS-ARSPA 2006.

[3] E. Bernard, F. Bouquet, A. Charbonnier, B. Legeard, F. Peureux, M. Utting, E. Torreborre. Model-based testing from UML models. MBT 2006.

[4] F. Bouquet, F. Dadeau, J. Gros Lambert, J. Julliand. Safety property driven test generation from JML specifications. FATES/RV 2006.

[5] F. Bouquet, S. Debricon, B. Legeard, J.-D. Nicolet. Extending the unified process with model-based testing. MoDeVa 2006.

[6] F. Cheikh, G. De Giacomo, M. Mecella. Automatic Web services composition in trust-aware communities. SWS 2006.

[7] Y. Chevalier, M. Kourjeh. A symbolic intruder model for hash-collision attacks. ASIAN 2006.

[8] Y. Chevalier, M. Rusinowitch. Hierarchical combination of intruder theories. RTA 2006.

Thèses démarrées :

[1] Fahima Cheikh. Modèles et algorithmes pour la composition de services. Doctorat préparé à l'université Paul Sabatier depuis septembre 2005. Soutenance prévue en juillet 2008. Aucun soutien financier.

[2] Marwa El Houry. Langages de haut niveau pour l'expression de politiques d'échanges de messages entre services. Doctorat préparé à l'université Paul Sabatier depuis juin 2006. Soutenance prévue en mai 2009. Bourse du bureau Moyen-Orient de l'Agence universitaire de la francophonie.

[3] Nawel Guermouche. Vérification de la politique de sécurité des services. Doctorat préparé à l'université Henri Poincaré depuis octobre 2006. Soutenance prévue en septembre 2009. Bourse Inria/Région.

[4] Mounira Kourjeh. Analyse de la sécurité des protocoles avec primitives cryptographiques imparfaites. Doctorat préparé à l'université Paul Sabatier depuis janvier 2006. Soutenance prévue en décembre 2008. Bourse de la Fondation Hariri.

[5] Vincent Prêtre. Génération automatique de tests à partir de modèle formel pour les applications de type web services. Doctorat préparé à l'université de Franche-Comté depuis octobre 2005. Soutenance prévue en septembre 2008. Financement sur contrat.

[6] Jérôme Voinot. Approximations et model-checking pour la sécurité de systèmes distribués. Doctorat préparé à l'université de Franche-Comté depuis octobre 2006. Soutenance prévue en septembre 2009. Bourse MNERT.

## **G. Autres commentaires**

---

## Eléments quantitatifs

### **H. Liste des réunions/séminaires/colloques organisés durant la période et des missions à l'étranger**

(préciser la date, le lieu, l'objet, le nombre des participants)

Réunions : Les activités du projet Cops sont décrites à l'adresse suivante [www.irit.fr/COPS/Accueil.htm](http://www.irit.fr/COPS/Accueil.htm).

La première réunion a eu lieu au laboratoire d'informatique fondamentale de Marseille du 16 au 17 mars 2006. Les participants étaient Philippe Balbiani (Irit), Fabrice Bouquet (LIFC), Fahima Cheikh (Irit), Yannick Chevalier (Irit), Pierre-Cyrille Heam (LIFC), Olga Kouchnarenko (LIFC), Mounira Kourjeh (Irit), Denis Lugiez (Lif), Olivier Perrin (Loria), Christophe Ringeissen (Loria), Michael Rusinowitch (Loria), Luigi Santocanale (Lif), Laurent Vigneron (Loria), Jérôme Voinot (LIFC), Silvano Dal Zilio (Lif)

La seconde réunion a eu lieu à l'institut de recherche en informatique de Toulouse du 5 au 6 octobre 2006. Les participants étaient Philippe Balbiani (Irit), Fahima Cheikh (Irit), Yannick Chevalier (Irit), Guillaume Feuillade (Irit), Nawel Guermouche (Loria), Olga Kouchnarenko (LIFC), Mounira Kourjeh (Irit), Olivier Perrin (Loria), Vincent Prêtre (LIFC), Christophe Ringeissen (Loria), Michael Rusinowitch (Loria), Laurent Vigneron (Loria), Silvano Dal Zilio (Lif)

Missions à l'étranger :

Y. Chevalier. Participation au workshop *Constraints and Verification* à Cambridge (England) en mai 2006.

### **I. Par rubrique et par partenaire, établir la consommation des dépenses financées par l'ANR, depuis le démarrage du projet.**

Partenaire	Fonct. (Keuros)	Equipement ( <i>préciser nature</i> )	Equip. (Keuros)
P1	5,0 Keuros	Aucun	0 Keuros
P2	2,2 Keuros	Aucun	0 Keuros
P3	0,9 Keuros	Aucun	0 Keuros

Total projet : 8,1 Keuros en fonctionnement et 0 Keuros en équipement.

### **J. Le cas échéant, préciser les travaux réalisés par les partenaires étrangers associés au projet sans aide de l'ANR**

Cédric Fournet et Andrew Gordon (Microsoft, Cambridge) sont associés au projet. Ils n'ont pas pu cette année participer à nos réunions.

### **K. Liste des personnels recrutés en CDD par des établissements publics dans le cadre du projet sur l'aide allouée par l'ANR**

Nom	Prénom	Qualifications	Date de recrutement	Durée du contrat (en mois)
...				

...

*Indiquer leur devenir postérieur à leur participation au projet : intégration comme chercheur, enseignant-chercheur, ingénieur, emploi dans le privé, chômeur, etc....*

Aucun personnel n'a été recruté en CDD dans le cadre du projet.

**L. Le cas échéant, indiquer les différents types d'aides complémentaires obtenues grâce à ce projet.**

*(Il peut s'agir de ressources financières, ressources humaines, allocations de recherche,...)*

Le partenaire P2 bénéficie d'un financement par le plan Etat - région Lorraine dans le cadre de l'action QSL COWS ("Contraintes pour la composition de services web") du thème "Qualité et sûreté des logiciels et systèmes informatiques". Cette action est coordonnée par Olivier Perrin (Loria) et Laurent Vigneron (Loria). Elle a démarré en 2006 et durera 2 années.

**M. Le cas échéant, modalités d'utilisation du complément de financement « pôles de compétitivité » (15 lignes maximum)**

*Rappel : ceci ne s'applique pas aux entreprises, mais seulement aux laboratoires publics et autres structures non soumises à l'encadrement communautaire des aides d'Etat à la R&D. Le complément de financement est destiné à couvrir des frais supplémentaires liés à la participation aux activités du pôle : ingénierie de projets partenariaux publics-privés, recherche de partenaires ; valorisation de la recherche ; relations inter-pôles et internationales...*

Nous ne bénéficions d'aucun complément de ce type.

## **N. CADRE RESERVE AU COORDONNATEUR DU PROJET (15 à 50 lignes maximum)**

*Commentaire général sur l'état d'avancement du projet, les interactions entre les différents partenaires, les efforts particuliers en matière d'interdisciplinarité, l'ouverture internationale, etc.*

Après les réunions de Marseille (mars 2006) et de Toulouse (octobre 2006), des collaborations évidentes apparaissent entre les membres des différents partenaires. En particulier,

1. Dans le cadre de la tâche **Algorithmes pour la composition de services électroniques**, Philippe Balbiani (Irit), Fahima Cheikh (Irit), Nawel Guermouche (Loria), Olivier Perrin (Loria) et Christophe Ringeissen (Loria) ont décidé de travailler ensemble sur la difficulté intrinsèque du problème de la composition des services électroniques qui intègrent les notions de temps et de confiance. Une réunion entre ces personnes est prévue à Nancy en février.
2. Dans le cadre de la tâche **Algorithmes pour la composition de services électroniques**, Philippe Balbiani (Irit), Olga Kouchnarenko (LIFC) et Jérôme Voinot (LIFC) ont décidé de travailler ensemble sur la difficulté intrinsèque du problème de la composition des services électroniques qui intègrent les notions de coût et de confiance. Une réunion entre ces personnes est prévue à Besançon en février.
3. Yannick Chevalier (Irit), Denis Lugiez (Lif) et Michael Rusinowitch (Loria) travaillent ensemble à la réalisation de la tâche **Combinaison de politiques de sécurité et de services électroniques**. Ils préparent ensemble deux rapports de recherche.

Si une collaboration informelle entre Yannick Chevalier, Denis Ligiez et Michael Rusinowitch préexistait au projet Cops (Yannick Chevalier a préparé sa thèse sous la direction de Michael Rusinowitch et Denis Lugiez a été rapporteur pour cette thèse), la collaboration entre Philippe Balbiani et Fahima Cheikh, d'une part, et Nawel Guermouche, Olivier Perrin, Christophe Ringeissen, Olga Kouchnarenko et Jérôme Voinot, d'autre part, a vu le jour par l'entremise du projet Cops.

Par ailleurs, à travers la notion de test, nous avons étudié un aspect du problème de la composition des services électroniques dont il n'avait pas été question lors de la rédaction de la description scientifique du projet. Tester les services électroniques, c'est détecter leurs défauts. Il faut pour cela générer tous les cas d'utilisation possible de tel ou tel service électronique. Cet aspect est abordé principalement par le partenaire P2 en collaboration avec le partenaire P1. La réunion prévue à Besançon en février aura aussi pour objectif de clarifier les questions qu'il soulève : comment générer les tests, faut-il tester les services en fonction des services avec lesquels ils risquent d'interagir, quels sont les problèmes liés à la relation de confiance que les services ont les uns pour les autres.

## **CADRE RESERVE A l'USAR**

Nom du coordinateur scientifique de l'USAR :

Date :

---

## Glossaire

**Livrable** : tout composant matérialisant le résultat de la prestation de réalisation. Toute production émise par le titulaire au cours du projet : document, courrier revêtant un caractère officiel , module de code logiciel, dossiers de tests, application intégrée, objet, dispositif...

**Livrable interne** : réalisé au sein du programme et non communiqué à l'extérieur du programme.

**Livrable externe** : élément diffusé ou livré hors de la communauté du projet de recherche..

**Faits marquants** : élément non nécessairement quantifiable mais significatif pour le projet.