AGENCE NATIONALE DE LA RECHERCHE ANR	**Compte-rendu de fin de projet**	

Projet ANR-09-SEGI-002-01

CESSA : Compositional Evoluation of Secure Services using Aspects

Programme SEGI 2009

Ce document est à remplir par le coordinateur en collaboration avec les partenaires du projet. L'ensemble des partenaires doit avoir une copie de la version transmise à l'ANR.

Ce modèle doit être utilisé uniquement pour le compte-rendu de fin de projet.

A IDENTIFICATION

Acronyme du projet	CESSA
Titre du projet	Compositional Evolution of Secure Services with Aspects
Coordinateur du projet (société/organisme)	Armines/École des Mines de Nantes
Période du projet (date de début – date de fin)	18/1/2010 – 17/1/2013
Site web du projet, le cas échéant	http://www.cessa.gforge.inria.fr

Rédacteur de ce rapport	
Civilité, prénom, nom	M. Mario Südholt
Téléphone	02.51.85.82.47
Adresse électronique	sudholt@mines-nantes.fr
Date de rédaction	16/3/2013

Si différent du rédacteur, indiquer un contact pour le projet	
Civilité, prénom, nom	
Téléphone	
Adresse électronique	

Liste des partenaires présents à la fin du projet (société/organisme et responsable scientifique)	- Armines/EMN, M. Mario Südholt - EURECOM, M. Yves Roudier - IS2T, M. Fred Rivard - SAP, M. Anderson Santana De Oliveira

B RESUME CONSOLIDE PUBLIC

Ce résumé est destiné à être diffusé auprès d'un large public pour promouvoir les résultats du projet, il ne fera donc pas mention de résultats confidentiels et utilisera un vocabulaire adapté mais n'excluant pas les termes techniques. Il en sera fourni une version française et une version en anglais. Il est nécessaire de respecter les instructions ci-dessous.

B.1 INSTRUCTIONS POUR LES RESUMES CONSOLIDES PUBLICS

Les résumés publics en français et en anglais doivent être structurés de la façon suivante.

Titre d'accroche du projet *(environ 80 caractères espaces compris)*
Titre d'accroche, si possible percutant et concis, qui résume et explicite votre projet selon une logique grand public : il n'est pas nécessaire de présenter exhaustivement le projet mais il faut plutôt s'appuyer sur son aspect le plus marquant.

« Compositions Sécurisés pour les Services Web »

Les deux premiers paragraphes sont précédés d'un titre spécifique au projet rédigé par vos soins.

Titre 1 : situe l'objectif général du projet et sa problématique *(150 caractères max espaces compris)*
Paragraphe 1 : *(environ 1200 caractères espaces compris)*
Le paragraphe 1 précise les enjeux et objectifs du projet : indiquez le contexte, l'objectif général, les problèmes traités, les solutions recherchées, les perspectives et les retombées au niveau technique ou/et sociétal

Titre 2 : précise les méthodes ou technologies utilisées *(150 caractères max espaces compris)*
Paragraphe 2 : *(environ 1200 caractères espaces compris)*

Le paragraphe 2 indique comment les résultats attendus sont obtenus grâce à certaines méthodes ou/et technologies. Les technologies utilisées ou/et les méthodes permettant de surmonter les verrous sont explicitées (il faut éviter le jargon scientifique, les acronymes ou les abréviations).

Résultats majeurs du projet *(environ 600 caractères espaces compris)*
Faits marquants diffusables en direction du grand public, expliciter les applications ou/et les usages rendus possibles, quelles sont les pistes de recherche ou/et de développement originales, éventuellement non prévues au départ.
Préciser aussi toute autre retombée= partenariats internationaux, nouveaux débouchés, nouveaux contrats, start-up, synergies de recherche, pôles de compétitivités, etc.

Production scientifique et brevets depuis le début du projet *(environ 500 caractères espaces compris)*
Ne pas mettre une simple liste mais faire quelques commentaires. Vous pouvez aussi indiquer les actions de normalisation

Illustration
Une illustration avec un schéma, graphique ou photo et une brève légende. L'illustration doit être clairement lisible à une taille d'environ 6cm de large et 5cm de hauteur. Prévoir une résolution suffisante pour l'impression. Envoyer seulement des illustrations dont vous détenez les droits.

Informations factuelles
Rédiger une phrase précisant le type de projet (recherche industrielle, recherche fondamentale, développement expérimental, exploratoire, innovation, etc.), le coordonnateur, les partenaires, la date de démarrage effectif, la durée du projet, l'aide ANR et le coût global du projet, par exemple « Le projet XXX est un projet de recherche fondamentale coordonné par xxx. Il associe aussi xxx, ainsi que des laboratoires xxx et xxx). Le projet a commencé en juin 2006 et a duré 36 mois. Il a bénéficié d'une aide ANR de xxx € pour un coût global de l'ordre de xxx € »

B.2 RESUME CONSOLIDE PUBLIC EN FRANÇAIS

« Compositions Sécurisées pour les Services Web »

B.2.1 SECURISER LES SERVICES: UN BESOIN VITAL SUR INTERNET

La composition de services constitue aujourd'hui le principal moyen de structuration des applications sur Internet, le web et dans le Nuage (commerce électronique, services pour particuliers tels que Facebook, etc.). Son importance est censée s'accroître bien plus encore à l'avenir à cause de la variété des périphériques utilisés et les types d'interaction correspondants (réseaux nomades, mobiles ; environnements ubiquitaires, etc.). La sécurité d'applications construites à l'aide de compositions de services et leur évolution est un besoin crucial : elles requièrent souvent la divulgation de données privées des utilisateurs, nécessitant, par exemple, le stockage et le traitement d'une multitude de données bancaires.

La sécurisation de ces applications est particulièrement difficile aussi bien d'un point de vue fondamental que d'un point de vue pratique. Des failles de sécurité peuvent apparaître dans tous les composants d'une application et dans toutes les couches logicielles. Il est alors nécessaire de pouvoir définir des politiques et des propriétés de sécurité qui peuvent influer sur toute partie d'une application et des infrastructures les exécutant. En outre, concevoir des moyens de vérification et d'application de ces politiques qui permettent d'éliminer des failles potentiellement omniprésentes constitue aujourd'hui un verrou majeur pour l'utilisation généralisée d'applications sur Internet. Le développement de méthodes et de techniques modulaires pour la sécurisation est alors un besoin vital.

B.2.2 TECHNIQUES ET OUTILS NOUVEAUX POUR LA SECURISATION DES SERVICES

Les partenaires du projet CESSA ont développé des techniques pour la définition modulaire de politiques de sécurité, des mécanismes de vérification de propriétés de sécurité et des techniques d'implémentation de ces politiques dans un environnement hétérogène incluant des serveurs lourds et des périphériques mobiles (ou à ressources limitées).

Les partenaires ont proposé notamment des solutions pour l'application de politiques à un grand nombre de composants d'une application qui peuvent être sujet à des modifications dans le cadre d'évolution des compositions de services. Ce résultat a été obtenu en étendant

des techniques de la programmation par aspects ainsi que des moniteurs de référence aux compositions des services qui sont exécutés aussi bien sur des serveurs lourds que des périphériques légers.

Les mécanismes de sécurisation obtenus sont fondés sur des propriétés formelles, se présentent sous la forme d'extension de langages ou d'API existants pour une utilisation relativement facile et sont partiellement soutenus par un outillage logiciel intégré à la plateforme logicielle libre Eclipse.

B.2.3 RESULTATS MAJEURS

En ce qui concerne la définition modulaire des politiques de sécurité, les partenaires ont proposé un langage de définition de politiques orientées flux d'information et un nouveau système de type pour la définition de propriétés de sécurité des interactions entre service.

Quant à l'application des politiques, les partenaires ont apporté des mécanismes pour prévenir des vulnérabilités et pour déployer des politiques de sécurités dans une composition de web services, notamment par des nouvelles techniques de la programmation par aspects. Ces dernières permettent, en particulier, d'appliquer des politiques et propriétés de sécurité d'une manière incrémentale à des services qui ont été modifiés dans le contexte d'évolution. Des infrastructures pour l'exécution de service sur des périphériques légers et leur sécurisation ont également été développées.

La majorité des résultats du projet sera maintenue et développée dans le cadre d'intégration dans des produits commerciaux des partenaires ou bien dans le cadre d'autres projets collaboratifs, notamment le projet IP européen A4Cloud qui a démarré en octobre 2012.

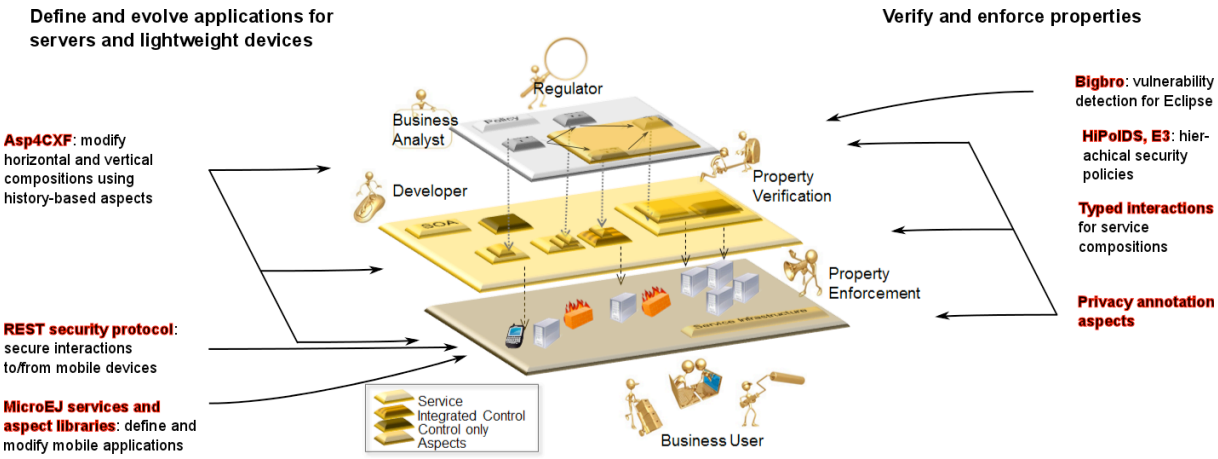
B.2.4 PRODUCTION SCIENTIFIQUE ET BREVETS

Les partenaires ont publié une douzaine d'articles scientifiques principalement dans les domaines des services web, de la sécurité des logiciels et des systèmes, et du génie logiciel. Ces publications couvrent tous les résultats et présentent souvent des synergies issues de l'utilisation conjointe de plusieurs de ces résultats.

Certains résultats du projet ont été intégrés par les partenaires industriels dans leurs produits commerciaux où une telle intégration est en cours d'évaluation. La protection de ces résultats via des brevets est prévue pour certains.

B.2.5 ILLUSTRATION

L'illustration suivante place les contributions du projet CESSA dans le contexte d'une application impliquant des serveurs lourds et des clients mobiles ou limités en ressources. Elle montre les moyens nouveaux pour la définition et l'évolution d'applications (à gauche) et ceux pour la vérification et l'application de propriétés (à droite). Elle illustre aussi à quelles compositions horizontales et verticales les contributions s'appliquent.



B.2.6 INFORMATIONS FACTUELLES

- Projet de recherche industrielle
- Date de démarrage : 18/1/2010, durée : 36 mois
- Coût global : 2129 K€, aide ANR : 902 K€
- Partenaire
  - Armines/École des Mines de Nantes (coordinateur)
  - Eurecom
  - IS2T S.A.
  - SAP AG

B.3 RESUME CONSOLIDE PUBLIC EN ANGLAIS

Suivre impérativement les instructions ci-dessus.

"Secure compositions for web services"

B.3.1 SERVICE SECURITY : A CRUCIAL NEED ON THE INTERNET

Service composition today constitutes the principal means for application structuring on the Internet, the web and in the Cloud (electronic commerce, services for consumers such as Facebook, etc.). Its importance is likely to increase significantly in the future because of the wider variability of devices and the corresponding types of interactions (nomadic and mobile networks, ubiquitious environments, etc.). The security of applications built using service compositions and their évolution constitutes a crucial requirement: they frequently need to divulge private data of users, for example, storing and treating large sets of banking data.

Making these applications secure is particularly difficult from a fundamental point of view as well as a practical one. Security faults may appear in any of the application's components and in any layer of the software stack. Means are therefore needed to define security policies and properties that may modify all parts of an application and the corresponding execution

infrastructures. The development of verification and enforcement techniques for these policies is one of the major locks to the generalized use of applications on the Internet. At the same time, the development of modular security methods and techniques for Internet security constitutes a crucial need in order to be able to apply such policies in a localized and incremental manner.

B.3.2 New techniques and tools for secure services

The partner of the CESSA project have developed techniques for the modular development of security policies, mechanisms for the verification of security properties and implementation techniques for these policies in heterogeneous environments comprising heavyweight servers and mobile and other resource-constraint devices.

The partners have proposed, in particular, solutions for the enforcement of policies to a large number of components of an application whose service compositions may be subject to évolution. This result has been obtained by extending techniques of aspect-oriented programming and reference monitors to service compositions that are executed on back-end servers and lightweight devices alike. The security mechanisms are based on formal properties, are expressed as language extensions or extensions of existing APIs. An integration of these security extensions with the open-source development platform Eclipse has been provided, thus facilitating their use.

B.3.3 Main results

The partners have proposed a new language for the modular definition of information-flow based security policies. They have also supported the modular definition of security properties by a new type system for service interactions.

As to the enforcement of policies, the partners have provided mechanisms for the prevention of security vulnerabilities in web service compositions, in particular, by means of new techniques for the aspect-based manipulation of services. The latter provide support, in particular, for the incremental application of security policies and properties to services that have been modified as part of évolution requirements. Infrastructures and aspect support for the secure execution of services on lightweight, notably mobile, devices have also been developed.

Most of the results of the project will be maintained and developed by integrating them in commercial products of the industrial partners or in the context of follow-up collaborative projects. The models and implementation techniques for type-based security of service interactions, the aspect-based manipulation of security properties of services, as well as the secure deployment of web services will be developed in the context of the European IP project A4Cloud that has started in October 2012.

B.3.4 Scientific production and patents

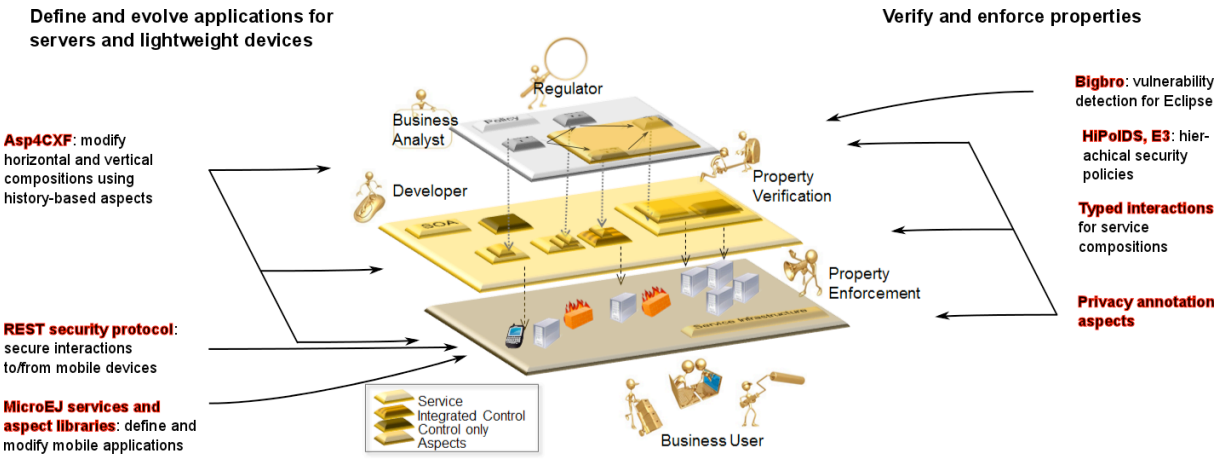
The partners have published a dozens of scientific articles, mainly in the domains of web services, software and systems security, and software engineering. These publications concern all results of the project and frequently present synergies obtained by the common exploitation of several results of different partners.

Several results of the project have been integrated by the industrial partners in their commercial products or are evaluating such an integration. The protection of these results by means of patents is planned for some of them.

B.3.5 Illustration

The following figure illustrates the contributions of the CESSA project in the context of an application of interacting heavyweight servers and mobile or resource-constraint devices. It shows the new means for the définition and évolution of applications (on the left-hand side) as well as property vérification and enforcement mechanisms (on the right-hand side). It also

indicates to which horizontal and vertical service compositions and interactions the contributions apply.



B.3.6 INFORMATIONS FACTUELLES

- Industrial research project
- Start date : 18 Jan. 2010, Duration: 36 mois
- Global cost : 2129 K€, ANR subvention: 902 K€
- Partners
  - Armines/École des Mines de Nantes (coordinateur)
  - Eurecom
  - IS2T S.A.
  - SAP AG

C MEMOIRE SCIENTIFIQUE

Maximum 5 pages. *On donne ci-dessous des indications sur le contenu possible du mémoire. Ce mémoire peut être accompagné de rapports annexes plus détaillés.*

Le mémoire scientifique couvre la totalité de la durée du projet. Il doit présenter une synthèse auto-suffisante rappelant les objectifs, le travail réalisé et les résultats obtenus mis en perspective avec les attentes initiales et l'état de l'art. C'est un document d'un format semblable à celui des articles scientifiques ou des monographies. Il doit refléter le caractère collectif de l'effort fait par les partenaires au cours du projet. Le coordinateur prépare ce rapport sur la base des contributions de tous les partenaires. Une version préliminaire en est soumise à l'ANR pour la revue de fin de projet.

Un mémoire scientifique signalé comme confidentiel ne sera pas diffusé. Justifier brièvement la raison de la confidentialité demandée. Les mémoires non confidentiels seront susceptibles d'être diffusés par l'ANR, notamment via les archives ouvertes http://hal.archives-ouvertes.fr.

Mémoire scientifique confidentiel : non

C.1 RESUME DU MEMOIRE

Ce résumé peut être repris du résumé consolidé public.

SECURISER LES SERVICES: UN BESOIN VITAL SUR INTERNET

La composition de services constitue aujourd'hui le principal moyen de structuration des applications sur Internet, le web et dans le Nuage (commerce électronique, services pour particuliers tels que Facebook, etc.). Son importance est censée s'accroître bien plus encore dans l'avenir à cause de la variété des périphériques utilisés et des types d'interaction correspondants (réseaux nomades, mobiles ; environnements ubiquitaires, etc.). La sécurité de ces applications est un besoin crucial: elles requièrent souvent la divulgation de données

privées des utilisateurs et nécessitent le stockage et le traitement, par exemple, d'une multitude de données bancaires.

La sécurisation de ces applications est particulièrement difficile aussi bien d'un point de vue fondamental que d'un point de vue pratique. Des failles de sécurité peuvent apparaître dans tous les composants d'une application et dans toutes les couches logicielles. Il est alors nécessaire de pouvoir définir des politiques et des propriétés de sécurité qui peuvent influer sur toute partie d'une application et des infrastructures les exécutant. En outre, concevoir des moyens de vérification et d'application de ces politiques qui permettent d'éliminer des failles potentiellement omniprésentes constitue aujourd'hui un verrou majeur pour l'utilisation généralisée d'applications sur Internet. Le développement de méthodes et de techniques modulaires pour la sécurisation est alors un besoin vital.

RESULTATS MAJEURS

En ce qui concerne la définition modulaire des politiques de sécurité, les partenaires ont proposé un langage de définition de politiques orientées flux d'information et un nouveau système de type pour la définition de propriétés de sécurité des interactions entre services.

Quant à l'application des politiques, les partenaires ont apporté des mécanismes pour prévenir des vulnérabilités et pour déployer des politiques de sécurités dans une composition de web services, notamment par des nouvelles techniques de la programmation par aspects. Des infrastructures pour l'exécution de services sur des périphériques légers et leur sécurisation ont également été développées.

La majorité des résultats du projet sera maintenue et développée dans le cadre d'intégration dans des produits commerciaux des partenaires ou bien dans le cadre d'autres projets collaboratifs, notamment le projet IP européen A4Cloud qui a démarré en octobre 2012.

C.2 ENJEUX ET PROBLEMATIQUE, ETAT DE L'ART

Présenter les enjeux initiaux du projet, la problématique formulée par le projet, et l'état de l'art sur lequel il s'appuie. Présenter leurs éventuelles évolutions pendant la durée du projet (les apports propres au projet sont présentés en C.4).

Le projet CESSA a ciblé un enjeu crucial pour la généralisation des interactions et, par voie de conséquence, l'économie sur Internet : la sécurisation de la composition de services. Plus spécifiquement, ses partenaires ont étudié deux problématiques clés relatives au caractère transversal de la sécurité : i) comment définir d'une manière modulaire des politiques de sécurité qui sont définies sur des compositions complexes de services et ii) comment implémenter ces politiques dans des environnements hétérogènes caractérisés par des infrastructures différentes, sur des serveurs mais aussi des périphériques mobiles et ubiquitaires.

Ces problématiques se retrouvent au niveau de l'état de l'art. Les méthodes scientifiques, telles que la structuration du logiciel par aspects et la métaprogrammation, n'avaient été appliquées aux compositions de service que d'une manière très limitée et, surtout, en ne considérant pas des compositions exécutées sur des infrastructures hétérogènes. Les approches visant à la définition de politiques de sécurité étaient également limitées par rapport aux besoins des systèmes logiciels construits à l'aide de services.

C.3 APPROCHE SCIENTIFIQUE ET TECHNIQUE

Les partenaires ont globalement étudié le développement de nouveaux modèles et techniques fondés, d'une part, sur la programmation logique pour l'expression déclarative de politiques de sécurité et, de l'autre, sur la programmation par aspects pour la modularisation de fonctionnalités transverses de sécurité. Les problématiques concrètes ciblées ont été choisies sur la base de deux études de cas (une étude issue du commerce électronique, une

autre de la surveillance à distance de bâtiments), par des études empiriques et par une analyse détaillée de l'état de l'art scientifique et technique.

En outre, les modèles de domaines qui sous-tendent la définition des politiques de sécurité et le modèle d'aspects utilisé pour la modularisation de propriétés de sécurité ont été choisis avec un souci de compatibilité et d'interopérabilité. Le modèle de domaine de sécurité, par exemple, peut utiliser directement les notions d'interactions typées et d'aspects permettant de modifier les compositions, les intercepteurs de messages et les implémentations des services web.

Finalement, les mécanismes de langages, API, infrastructures et outils développés ont été validés dans le cadre d'applications réalistes et, pour certains, par des intégrations dans des produits commerciaux des partenaires. Des résultats du projet ont été appliqués, en particulier, à la sécurisation des interactions entre serveurs utilisant des protocoles de sécurité du type WS-Security et des périphériques mobiles utilisant des API du type.

C.4 RESULTATS OBTENUS

Positionner les résultats par rapports aux livrables du projet et aux publications, brevets etc. Revisiter l'état de l'art et les enjeux à la fin du projet.

Les partenaires du projet CESSA ont produit trois types de résultats:
- des modèles et infrastructures logiciels pour la manipulation de services hybrides qui nécessitent des interactions entre services lourds (WS*/SOAP) et légers (REST) ;
- des modèles et infrastructures pour la définition de domaines de sécurité ;
- des outils pour la sécurisation des services web hybrides.

C.4.1 ASPECTS ET TYPES POUR INTERACTIONS ENTRE SERVICES HYBRIDES WS*/SOAP-REST

Nous avons défini un modèle pour la définition de composition de services couvrant aussi bien des services lourds (WS*/SOAP) et légers (REST). Le modèle est assorti d'un système de type qui permet de traiter un ensemble plus large de structures de données transmises entre services et garantit la correction du typage même en présence d'attaquants dans les systèmes. Finalement, nous avons défini un modèle d'aspects pour la manipulation de ces services, en pouvant modifier aussi bien l'implémentation des services que leurs interactions. Ce modèle d'aspect permet de quantifier sur l'historique d'exécution des compositions de services et fournit donc des moyens d'expression puissants et déclaratifs.

Une partie de ces travaux fait partie de la thèse « A new model for hybrid services and their interactions » de Diana Allam.

Publications : 1, 8, 12-15 ; livrables : D1.1, D1.2, D1.3, D3.2, D3.4.

C.4.2 DOMAINES DE POLITIQUE DE SECURITE ET MONITEURS DE REFERENCE

Nous avons réalisé le moteur d'un moniteur de référence pour mettre en application (*enforcement*) ou pour surveiller (*monitoring*) des politiques HiPoLDS. Ce prototype a été réalisé dans les langages Python et Pyke. Cette implantation permet de définir un ensemble de règles d'inférences logiques qui constituent la politique de sécurité définie pour le système. Ces règles sont ensuite activées par l'arrivée de trafic réseau analysé dans le prototype réalisé par un proxy écrit en Java avec le framework CXF. Nous avons également prototypé séparément un tel proxy à partir de l'analyseur de trafic WireShark. L'activation des règles dicte les mécanismes à mettre en œuvre pour mettre en application la politique définie.

Une partie de ces travaux à l'origine du langage HiPoLDS a été l'objet d'une contribution de la thèse « A Requirements Engineering Driven Approach to Security Architecture Design for Distributed Embedded Systems » de Muhammad Sabir Idrees. Ces travaux portent sur le

passage de propriétés de sécurité de haut-niveau vers des mécanismes concrets dans les architectures SOA, et notamment les problèmes de composition verticale.

Publications : 3, 5-7, 9, 11, 15 ; livrables : D2.1, D2.2, D2.3, D3.1, D3.2, D3.3

C.4.3 OUTILS POUR LA SECURISATION DES SERVICES WEB

Nous avons construit des prototypes pour démontrer les techniques proposées tout au long de la durée du projet : la détection et correction de vulnérabilités dans le code des applications distribués avec des techniques orientées par aspects, pour la sécurisation des web services REST (un standard de facto, très diffusée sur Internet) ; pour la protection des données relatives à la vie privée dans les web services en Nuage, et aussi sur l'application de politiques de sécurité de façon hiérarchique dans les web services. Ces travaux ont été menés partiellement dans le cadre de la thèse de Gabriel Serme.

Nous avons également développé des API du type REST et des infrastructures pour aspects et services pour des périphériques légers. Ces supports logiciels permettent - une première pour certains périphériques légers tels que certains microprocesseurs de ST Microelectronics - de sécuriser aussi bien les implémentations des services que leurs interactions, notamment avec un environnement du monde WS*/SOAP. Pour ce dernier, nous avons développé des outils pour la manipulation de services web bâtis sur l'infastructure CXF de la fondation Apache.

Publications : 2-7, 9-11, 15 ; livrables : D1.2, D2.1, D2.2, D2.3, D3.1, D3.2, D3.3, D3.3, D3.4

C.5 EXPLOITATION DES RESULTATS

Les résultats du projet sont actuellement sujets à deux différents types d'exploitation :

- ils ont partiellement été intégrés ou leur intégration est actuellement en phase d'évaluation dans des API pour périphériques légers (par le partenaire IS2T) et dans des systèmes d'informations d'entreprises (par le partenaire SAP). En outre, le partenaire SAP exploitera des concepts développés dans le projet CESSA pour l'intégration de nouveaux protocoles de sécurité aux services web déjà existants, via des moniteurs de référence qui traiteront les messages échangés entre services web ;
- ils sont utilisés et développés dans d'autres projets, coopératifs ou non. Les outils pour l'identification et l'élimination de vulnérabilités dans des services web ainsi que les modèles de services et aspects pour services du types WS*/SOAP et REST sont exploités dans le cadre du projet européen IP "A4Cloud" sur la responsabilisation des calculs et des traitements de données sur Internet (partenaires Armines/EMN, Eurecom, et SAP). Le partenaire Eurecom compte développer le langage HiPoLDS pour l'appliquer à l'expression déclarative et modulaire de différents types de propriétés de sécurité et à la spécification des mécanismes liés à leur satisfaction. Nous espérons pouvoir développer ce langage en particulier pour la définition, la mise en application et la surveillance de l'implantation de politiques de sécurité des flux d'information.

C.6 DISCUSSION

Discussion sur le degré de réalisation des objectifs initiaux, les verrous restant à franchir, les ruptures, les élargissements possibles, les perspectives ouvertes par le projet, l'impact scientifique, industriel ou sociétal des résultats.

Le projet CESSA a réalisé tous ses objectifs initiaux :

- la définition modulaire de modèles pour la sécurisation de compositions de services hybrides WS*/SOAP et REST ;
- le développement de techniques et d'outils pour l'implémentation de telles compositions sécurisées et la vérification de leurs propriétés ;
- l'application de ces résultats à des compositions hybrides dans les domaines des systèmes d'information d'entreprises et de la surveillance des bâtiments et

- leur exploitation dans les domaines des ERP et des systèmes embarqués.

Le projet CESSA a permis d'obtenir des avancées significatives relatives à ces enjeux et problématiques, notamment concernant l'identification de vulnérabilités de services web, la définition déclarative des politiques de sécurité, leur intégration modulaire dans des compositions de services complexes à l'aide de mécanismes d'aspects et leur déploiement et exécution dans des infrastructures réelles pour services sur serveurs et périphériques légers. Néanmoins, l'enjeu et les problématiques du projet sont aujourd'hui d'une actualité aussi saillante qu'au début du projet. Actuellement, l'exécution de composition de services dans des environnements de plus en plus hétérogènes doit être pris en compte (avec bientôt la généralisation des périphériques dans les lieux publics, les maisons et même les vêtements). De même, des applications plus dynamiques et des compositions de services plus variées doivent être traitées, comme par exemple, la composition entre applets sur périphériques légers, appelés « mash-ups » web, et les services de calculs sur serveurs lourds.

C.7 CONCLUSIONS

Le projet CESSA a fourni des résultats correspondant à tous ces objectifs initiaux :
- la définition modulaire de politique et propriétés de sécurité pour des compositions de services web,
- le développement de techniques correspondantes d'implémentation, de déploiement et de vérification,
- l'application à des compositions réels entre serveurs lourds et périphériques légers et mobiles et
- l'intégration des certains des résultats techniques dans des produits commerciaux.

Les résultats du projet ont été validés par une douzaine de publications scientifiques et des intégrations dans des produits commerciaux pour des périphériques légers. Finalement, ces résultats ouvrent des pistes intéressantes pour des travaux futurs aussi bien scientifiques que dans des contextes applicatifs et industriels. Plusieurs de ces pistes seront explorées dans le cadre du projet européen débutant A4Cloud.

D LISTE DES LIVRABLES

Quand le projet en comporte, reproduire ici le tableau des livrables fourni au début du projet. Mentionner l'ensemble des livrables, y compris les éventuels livrables abandonnés, et ceux non prévus dans la liste initiale.

Date de livraison	**N°**	**Titre**	**Nature** (rapport, logiciel, prototype, données, …)	**Partenaires** (souligner le responsable)	**Commentaires**
02/07/2010	D1.1	Survey and requirements analysis	Rapport	Armines/EMN	Néant
10/01/2011	D1.2	Model and formal architecture specification	Rapport	Armines/EMN	Néant
26/09/2011	D1.3	Language definition and aspect support - Extension of the Service Model for Security and Aspect	Rapport	Armines/EMN	Néant
23/07/2010	D2.1	State of the art and requirement analysis of security functionalities for SOAs	Rapport	Eurecom	Néant
27/05/2011	D2.2	Language definition for security specifications	Rapport	Eurecom	Néant
30/07/2012	D2.3	Security Analysis for Web Services	Rapport	Eurecom	Néant

Date de livraison	N°	Titre	Nature (rapport, logiciel, prototype, données, …)	Partenaires (souligner le responsable)	Commentaires
25/11/2010	D3.1	Security Analysis for Web Services	Rapport	SAP	Néant
22/04/2012	D3.2	Use-Case Analysis and Aspect Requirements	Rapport	SAP	Néant
11/01/2013	D3.3	Demonstrator for ERP	Rapport	SAP	Néant
07/03/2013	D3.4	Demonstrator for Embedded System	Rapport	IS2T	Néant

E IMPACT DU PROJET

Ce rapport rassemble des éléments nécessaires au bilan du projet et plus globalement permettant d'apprécier l'impact du programme à différents niveaux.

E.1 INDICATEURS D'IMPACT

Nombre de publications et de communications (à détailler en E.2)

Comptabiliser séparément les actions monopartenaires, impliquant un seul partenaire, et les actions multipartenaires résultant d'un travail en commun.
***Attention** : éviter une inflation artificielle des publications, mentionner uniquement celles qui résultent directement du projet (postérieures à son démarrage, et qui citent le soutien de l'ANR et la référence du projet).*

		Publications multipartenaires	Publications monopartenaires
International	**Revues à comité de lecture**	1	1
	Ouvrages ou chapitres d'ouvrage		
	Communications (conférence)	6	7
France	**Revues à comité de lecture**		
	Ouvrages ou chapitres d'ouvrage		
	Communications (conférence)		
Actions de diffusion	**Articles vulgarisation**	1	
	Conférences vulgarisation	1	
	Autres		Blogs : 8

Autres valorisations scientifiques (à détailler en E.3)

Ce tableau dénombre et liste les brevets nationaux et internationaux, licences, et autres éléments de propriété intellectuelle consécutifs au projet, du savoir faire, des retombées diverses en précisant les partenariats éventuels. Voir en particulier celles annoncées dans l'annexe technique).

	Nombre, années et commentaires (valorisations avérées ou probables)
Brevets internationaux obtenus	
Brevet internationaux en cours d'obtention	
Brevets nationaux obtenus	
Brevet nationaux en cours d'obtention	

Licences d'exploitation (obtention / cession)	
Créations d'entreprises ou essaimage	
Nouveaux projets collaboratifs	A4CLOUD – Accountability for the Cloud - Integrated project, EU FP7
Colloques scientifiques	
Autres (préciser)	

E.2 LISTE DES PUBLICATIONS ET COMMUNICATIONS

Répertorier les publications résultant des travaux effectués dans le cadre du projet. On suivra les catégories du premier tableau de la section ***Erreur ! Source du renvoi introuvable.*** *en suivant les normes éditoriales habituelles. En ce qui concerne les conférences, on spécifiera les conférences invitées.*

E.2.1 COMMUNICATIONS SCIENTIFIQUES PUBLIEES

1. R.-A. Cherrueau, O. Chebaro, M. Südholt: **"Flexible Aspect-Based Service Adaptation for Accountability Properties in the Cloud"**, 4th Int. Workshop on Variability and Software Composition, Mar. 2013.
2. G. Serme, M. Guarnieri, P. El Khoury, and A. Santana De Oliveira. **Towards assisted remediation of security vulnerabilities**. Proceedings of the Sixth International Conference on Emerging Security Information, Systems and Technologies. SECURWARE 2012. (**Best paper award**)
3. Theodoor Scholte, William K. Robertson, Davide Balzarotti, Engin Kirda: **Preventing Input Validation Vulnerabilities in Web Applications through Automated Type Analysis**. COMPSAC 2012: 233-243
4. P. Yu, J. Sendor, G. Serme, and A. Santana de Oliveira. **Automating privacy enforcement in cloud platforms**. Proceedings of the 7th International Workshop on Data Privacy Management. DPM 2012, in conjunction with the 17th annual European research event in Computer Security symposium (ESORICS 2012), Springer.
5. M. Dell'Amico, G. Serme, M. S. Idrees, A. Santana de Oliveira, and Y. Roudier. Hipolds: **A security policy language for distributed systems**. Proceedings of the 6th Workshop in Information Security Theory and Practice. WISTP 2012.
6. M. Dell'Amico, G. Serme, M. S. Idrees, A. Santana de Olivera, and Y. Roudier. **Hipolds: A security policy language for distributed systems**. Information Security Technical Report , ISSN 1363-4127. (**Extended journal version**)
7. G. Serme, A. Santana de Oliveira, J. Massiera, Y. Roudier. **"Enabling Message Security for RESTful Services"**, International Conferences on Web Services, June 2012.
8. D. Allam, R. Douence, J.-C. Royer, H. Grall and M. Südholt. **"A Message-Passing Model for Service-Oriented Computing"**, 8th International Conference on Web Information Systems, Apr. 2012
9. M. Sabir Idrees, G. Serme, Y. Roudier, A. Santana De Oliveira, H. Grall, M. Südholt. **"Evolving Security Requirements in Multi-Layered Service-Oriented-Architectures"**, 4th Int. WS on Autonomous and Spontaneous Security, Leuven, Belgium, Sep. 2011
10. G. Serme, G. Harel, **"Adaptive service security for mobile systems"**, Smart-Mobility'11, Sep. 11
11. G. Serme, M.S. Idrees, **"Adaptive Security on Service-based SCM Control System"**, accepted for publication at WSNSCM'11, June 2011.
12. I. Mejía, M. Südholt: **"Structured and flexible gray-box composition using invasive distributed patterns"**, in: "International Journal on Computer Science and Information Systems (IJCSIS)", Apr. 2011.

13. I. Mejía, M. Südholt: **"Structured and Flexible Gray-box Composition: Application to Task Rescheduling for Grid Benchmarking"**, in: IADIS International Conference Applied Computing 2010 (AC), Oct. 2010.
14. M. Lacouture, H. Grall, T. Ledoux: **"CREOLE: a Universal Language for Creating, Requesting, Updating and Deleting Resources"**, in: 9th Int. WS on the Foundations of Coordination Languages and Software Architectures (FOCLASA'10), Sep. 2010. PDF, abstract, ref.

E.2.2 COMMUNICATIONS EN COURS D'EVALUATION

15. R. Cherrueau, R. Douence, J.-C. Royer, M. Sudholt, A. Santana De Oliveira, Y. Roudier, M. Dell'Amico : **"Reference monitors for security and interoperability in OAuth 2.0"**, ICWS 2013, en cours d'évaluation

E.2.3 COMMUNICATIONS DE VULGARISATION

16. G. Serme, G. Harel, **"Adaptive service security for mobile systems"**, Smart-Mobility Industrial Event, Sep. 2011
17. J.-C. Pazzaglia, M. Südholt, Invited talks on Cloud Security, Journée « Cloud & SI » du pôle de compétitivité « Images & Réseaux », 27 Sep. 12

E.3 LISTE DES ELEMENTS DE VALORISATION

La liste des éléments de valorisation inventorie les retombées (autres que les publications) décomptées dans le deuxième tableau de la section ***Erreur ! Source du renvoi introuvable.****. On détaillera notamment :*

- *brevets nationaux et internationaux, licences, et autres éléments de propriété intellectuelle consécutifs au projet.*
- *logiciels et tout autre prototype*
- *actions de normalisation*
- *lancement de produit ou service, nouveau projet, contrat,…*
- *le développement d'un nouveau partenariat,*
- *la création d'une plate-forme à la disposition d'une communauté*
- *création d'entreprise, essaimage, levées de fonds*
- *autres (ouverture internationale,..)*

Elle en précise les partenariats éventuels. Dans le cas où des livrables ont été spécifiés dans l'annexe technique, on présentera ici un bilan de leur fourniture.

E.3.1 LOGICIELS ET AUTRE PROTOTYPE

Nous classons les logiciels selon les résultats principaux du projet.

E.3.1.1 Aspects et types pour interactions entre services hybrides WS/SOAP-REST*

- Asp4CXF : Système d'aspects pour services du Framework CXF de la fondation Apache
  - http://a4cloud.gforge.inria.fr/doku.php?id=start:aspect4cxf
  - Outil en développement dans le cadre du projet EU IP « A4Cloud »
- Le « REST security protocol » avec des intercepteurs sur le framework CXF
- API et librairie pour la programmation par aspects sur périphériques légers
  - Intégré aux produits commerciaux du partenaire IS2T
- Librairie de support aux types d'interactions pour services Web

E.3.1.2 Domaines de politique de sécurité et moniteurs de référence

- HiPolDS - l'architecture pour la mise en œuvre des politiques de sécurité hiérarchiques sur les systèmes distribués [6]
- E3 : création d'un logiciel prototype de moniteur de référence pour HiPoLDS
- Annotations et aspects pour la « privacy » dans le cloud
    - Outil en évaluation chez SAP pour intégration produit

E.3.1.3 Outils pour la sécurisation des services web

- Bigbro : détections et correction de vulnérabilités dans Eclipse pour des web services avec des aspects
    - Outil en évaluation chez SAP pour intégration produit
- API et librairie pour service web sur périphériques légers
    - Intégré aux produits commerciaux du partenaire IS2T

E.3.2 PROJETS COLLABORATIFS

Projet européen IP « Accountability for the Cloud » (A4Cloud)

E.4 BILAN ET SUIVI DES PERSONNELS RECRUTES EN CDD (HORS STAGIAIRES)

Ce tableau dresse le bilan du projet en termes de recrutement de personnels non permanents sur CDD ou assimilé. Renseigner une ligne par personne embauchée sur le projet quand l'embauche a été financée partiellement ou en totalité par l'aide de l'ANR et quand la contribution au projet a été d'une durée au moins égale à 3 mois, tous contrats confondus, l'aide de l'ANR pouvant ne représenter qu'une partie de la rémunération de la personne sur la durée de sa participation au projet.
Les stagiaires bénéficiant d'une convention de stage avec un établissement d'enseignement ne doivent pas être mentionnés.

Les données recueillies pourront faire l'objet d'une demande de mise à jour par l'ANR jusqu'à 5 ans après la fin du projet.

Identification				Avant le recrutement sur le projet			Recrutement sur le projet				Après le projet				
Nom et prénom	Sexe H/F	Adresse email (1)	Date des dernières nouvelles	Dernier diplôme obtenu au moment du recrutement	Lieu d'études (France, UE, hors UE)	Expérience prof. Antérieure, y compris post-docs (ans)	Partenaire ayant embauché la personne	Poste dans le projet (2)	Durée missions (mois) (3)	Date de fin de mission sur le projet	Devenir professionnel (4)	Type d'employeur (5)	Type d'emploi (6)	Lien au projet ANR (7)	Valorisation expérience (8)
ALLAM Diana	F	Diana.Allam@mines-nantes.fr	29/03/2013	Ingénieur	France	0	Armines/EMN	Doctorande	30 mois	17/01/2013	Doctorande jusqu'en sept. 2013	-	-	-	-
IDREES Muhammad Sabir	H	sabir.idrees@gmail.com	22/02/2013	Master of Science	Suède (UE)	1 an	EURECOM	Doctorant	30 mois	Sept. 2012	Post-doc France (en cours d'embauche)	Enseignement et recherche publique	chercheur	non	oui
LACOUTURE Mayleen	F	Mayleen.Lacouture@mines-nantes.fr	29/03/2013	Master of Science	Colombie	0	Armines/EMN	Ingénieur de développement	6 mois	31/07/2013	CDI	SME	Ingénieur	non	oui
SERME Gabriel	H	gabriel@serme.net	15/03/2013	Master	France	0	SAP	Chercheur/ Thésard	36	31/11/2012	CDI	Grande entreprise	ingénieur	Non	oui

Aide pour le remplissage

(1) Adresse email : indiquer une adresse email la plus pérenne possible
(2) Poste dans le projet : post-doc, doctorant, ingénieur ou niveau ingénieur, technicien, vacataire, autre (préciser)
(3) Durée missions : indiquer en mois la durée totale des missions (y compris celles non financées par l'ANR) effectuées sur le projet
(4) Devenir professionnel : CDI, CDD, chef d'entreprise, encore sur le projet, post-doc France, post-doc étranger, étudiant, recherche d'emploi, sans nouvelles
(5) Type d'employeur : enseignement et recherche publique, EPIC de recherche, grande entreprise, PME/TPE, création d'entreprise, autre public, autre privé, libéral, autre (préciser)
(6) Type d'emploi : ingénieur, chercheur, enseignant-chercheur, cadre, technicien, autre (préciser)
(7) Lien au projet ANR : préciser si l'employeur est ou non un partenaire du projet
(8) Valorisation expérience : préciser si le poste occupé valorise l'expérience acquise pendant le projet.

Les informations personnelles recueillies feront l'objet d'un traitement de données informatisées pour les seuls besoins de l'étude anonymisée sur le devenir professionnel des personnes recrutées sur les projets ANR. Elles ne feront l'objet d'aucune cession et seront conservées par l'ANR pendant une durée maximale de 5 ans après la fin du projet concerné. Conformément à la loi n° 78-17 du 6

janvier 1978 modifiée, relative à l'Informatique, aux Fichiers et aux Libertés, les personnes concernées disposent d'un droit d'accès, de rectification et de suppression des données personnelles les concernant. Les personnes concernées seront informées directement de ce droit lorsque leurs coordonnées sont renseignées. Elles peuvent exercer ce droit en s'adressant l'ANR (http://www.agence-nationale-recherche.fr/Contact).