

FICHE ACTIONS

réf. CEA S51048, afférente à l'Accord Général de Collaboration
signé le 05/05/2021 entre ATOS et le CEA (Réf. CEA F39754)

Il est entendu que l'AFFILIEE signataire de la présente FICHE ACTIONS a dûment été avisée des termes de l'ACCORD susvisé dont elle s'engage à respecter les stipulations pour l'exécution du présent PROJET.

FICHE ACTIONS EXPLORATOIRE	OUI	X	NON	
----------------------------	-----	---	-----	--

A cocher systématiquement

Il est entendu qu'en cas d'envoi par le Partenaire d'un bon de commande (y incluant éventuellement des conditions générales d'achat), celui-ci sera considéré comme un document purement administratif ne revêtant aucune valeur contractuelle.

Les informations contenues de la présente FICHE ACTIONS doivent être considérées comme confidentielles.

PROJET FIRMSEC (indiquez l'acronyme du PROJET)		
Intitulé du PROJET	FIRMSEC Firmware de systèmes communicants : analyse préliminaire	
Version de travail du document	V0	
Unité concernée	<u>CEA</u> Direction : DRT Institut : LIST Département : DILS Laboratoire : LSL	<u>AFFILIEE d'ATOS International</u> ENTITE JURIDIQUE : Avantix SAS
Entité légale à facturer et adresse de facturation		Avantix SAS 655 Avenue Galilée - CS10323 13799 AIX EN PROVENCE Cedex 3
Contact gestion administrative et financière		
Chef de PROJET AFFILIEE		
Nom, prénom	CROUZET Jérémie	
BU	Avantix	
Téléphone	06 68 44 39 72	
Email	jeremie.crouzet@atos.net	
Chef de PROJET CEA		
Nom, prénom	BARDIN Sébastien	
Dir/Institut/Dpt/Labo.	DRT/LIST/DILS/LSL	
Téléphone	01 69 08 54 16	
Email	Sebastien.bardin@cea.fr	

Objectifs et enjeux	
Objectifs du PROJET	Le cadre général du projet est la sécurité des systèmes embarqués communicants, et plus particulièrement la sécurité des firmware typiquement trouvés dans l'implémentation des protocoles de communication. Avantix et le CEA envisagent des actions de long terme dans ce cadre. La présente fiche action a pour objet une première action en ce sens. Les objectifs de cette première action sont : 1) Au travers d'une étude de cas préliminaires, mieux comprendre les enjeux de l'analyse de firmware de systèmes communicants, l'adéquation de l'outil BINSEC à ce problème et les adaptations à prévoir, ceci afin de préparer au mieux les futures actions sur ce thème. 2) Définir précisément la direction de travaux futurs sur BINSEC dans la perspective du projet proposé à la DGA (plan technologique de défense).
Enjeux du PROJET, valeur ajoutée de la collaboration	Démarrer une collaboration de long terme entre AVANTIX et l'équipe LSL/SABR du CEA LIST sur l'analyse sécuritaire de firmware embarqués de systèmes communicants. L'équipe SABR du CEA LIST est spécialiste en analyse formelle de code binaire pour la sécurité, et développe notamment l'outil BINSEC, qui a été appliqué avec succès par exemple à des problèmes de détection de canaux cachés, d'attaques en faute ou de rétro-ingénierie. L'équipe AVANTIX est spécialisée en technologies de communication et notamment en analyse sécuritaire des normes des protocoles Wireless, dont les normes cellulaires du 3GPP.
Traitement de Données Personnelles	NON
FICHE(S) ACTIONS antérieure(s)	
Continuité d'une FICHE ACTIONS antérieure	NON
Nature et descriptif des CONNAISSANCES NOUVELLES issues de l'exécution d'une FICHE ACTIONS antérieure	<i>Sans objet (cette fiche action est la première sur ce projet)</i>
Présentation technique du PROJET	

Solutions technologiques	<i>Étude des performances de BINSEC sur des codes représentatifs fournis par Avantix, et retour d'expérience.</i>
Plateforme (si besoin)	N/A
Propriété Intellectuelle et Exploitation	
CONNAISSANCES ANTERIEURES CEA utilisées (BREVETS, SAVOIR-FAIRES, LOGICIELS)	<i>Ce point sera à renseigner avant le PROJET, à actualiser en cours de PROJET et confirmer à l'issue du PROJET.</i> <i>BINSEC (réf. CEA : LG21347) disponible sous format open source sous licence GNU LESSER GENERAL PUBLIC LICENSE (Version 2.1, February 1999)</i>
CONNAISSANCES ANTERIEURES AFFILIEE utilisées (BREVETS, SAVOIR-FAIRES, LOGICIELS ...)	<i>Expertise dans le domaine des protocoles et systèmes de communications</i>
Nature des CONNAISSANCES NOUVELLES attendues / issues de l'exécution de la FICHE ACTIONS : - CONNAISSANCES NOUVELLES PROPRES CEA - CONNAISSANCES NOUVELLES PROPRES AFFILIEE - CONNAISSANCES NOUVELLES CONJOINTES	<i>Ce point sera à renseigner avant le PROJET s'agissant des CONNAISSANCES NOUVELLES attendues, à actualiser en cours de PROJET et confirmer à l'issue du PROJET.</i> <i>CONNAISSANCES NOUVELLES PROPRES CEA : Amélioration de BINSEC (réf. CEA : LG21347)</i> <i>Pas de CONNAISSANCES NOUVELLES PROPRES AFFILIEE</i> <i>Pas de CONNAISSANCES NOUVELLES CONJOINTES</i>
PRODUITS et/ou SERVICES de l'AFFILIEE	<i>Produit : Non applicable pour ce Projet (Fiche Action Exploratoire)</i> <i>Services : Détection de vulnérabilité(s) dans les firmwares (microcode) de systèmes communicants .</i>
CONCURRENTS DIRECTS D'ATOS, pour l'application de l'article 8.2.4.iii)	<i>Non applicable pour ce projet en l'absence de CONNAISSANCES NOUVELLES PROPRES AFFILIEE ou de CONNAISSANCES NOUVELLES PROPRES CONJOINTES</i>
DOMAINE	Pour la présente FICHE ACTIONS, le DOMAINE est : protocoles et systèmes de communications

Droits d'exploitation concedés à l'AFFILIEE sur les CONNAISSANCES NOUVELLES du CEA dans le couple PRODUITS (ou SERVICES)/ DOMAINE	<i>CONNAISSANCES NOUVELLES PROPRES CEA : Amélioration de BINSEC (réf. CEA : LG21347)</i> Avantix bénéficie d'une licence non exclusive d'utilisation de la version modifiée de BINSEC, tous domaines selon les conditions de la licence GNU LESSER GENERAL PUBLIC LICENSE (Version 2.1, February 1999).
Droits d'exploitation concedés au CEA sur les CONNAISSANCES NOUVELLES de l'AFFILIEE dehors du couple PRODUITS (ou SERVICES) / DOMAINE A FAIRE VALIDER PAR CHACUN DES CORRESPONDANTS LICENCE	<i>Sans objet</i>
Délai d'option	<i>Sans objet</i>
Planning prévisionnel du PROJET	
Tâche 1	Contenu : analyse préliminaire et retour d'expérience Le but est d'aider à mieux cerner les besoins d'Avantix en termes de fonctionnalité d'analyse, et l'adéquation entre l'outil BINSEC et les cas d'études envisagés (en termes de capacités d'analyse et de support de code et architectures). • L'équipe CEA mènera une analyse préliminaire sur les codes choisis afin d'évaluer la couverture en termes de support (jeux d'instructions, syscalls) des codes choisis, et les efforts éventuels à fournir pour l'améliorer. • L'équipe mènera également une analyse plus fonctionnelle, en discutant avec les équipes Avantix pour aider à mieux cerner les propriétés d'intérêt à vérifier, puis évaluer les capacités de BINSEC dans ce cadre d'analyse (support des propriétés, capacités à effectivement étendre la couverture du programme sous analyse).
Début	T₀ : 01 septembre 2025
Durée	8 mois Sous réserve de la fourniture des Données d'entrées.

Données d'entrée	Entrées d'Avantix - Codes jugés représentatifs : à la fois des codes <i>closed source</i> pour les architectures visées (ARM, RISC5) et des codes open-source, idéalement accompagnés de cas de test typiques pour ces codes. - Présentation générale des codes choisis, du domaine, et des propriétés typiques à vérifier / vulnérabilités à mettre en évidence.
Eléments livrés	- Document de retour d'expérience de l'utilisation de BINSEC sur les cas visés - Artefact pour rejouer les expériences - Présentation de BINSEC et tutoriel (2h)
Jalons Résultats majeurs Points de décision (go/nogo, inflexions, réunions d'avancement...)	M0 : kickoff adminsitratif en juin M1 : réunion (atelier technique) de lancement (une journée, une fois les use cases obtenus) M2 : Réception des uses cases (début septembre) M3 : réunion à mi-parcours M1+3 (une journée, mi-novembre) M4 : réunion finale T0+8 (une journée) (fin janvier, début février)
Budget du PROJET	
Budget et échéancier prévisionnel	Total : 51 000 € Facturation à la signature de la Fiche Actions : 25 500 € Facturation à la livraison de l'artefact : 25 500 € <i>Pour les besoins d'ATOS, le financement par les AFFILIEES pourra être qualifié de sous-traitance de R&D, conformément à l'Article 2 de l'ACCORD.</i>
ELEMENTS LIVRES du PROJET	
	- Un document de retour d'expérience de l'utilisation de BINSEC sur les cas visés - Artefact pour rejouer les expériences : ce logiciel consiste en un paquet englobant : - Un applicatif pour exécuter les use cases du projet, propriété d'Avantix. - Une version de BINSEC mis à jour pour pouvoir exécuter les tests. Cette version reste la propriété du CEA. - Une présentation de BINSEC et tutoriel (2h)

Fait à Saclay en deux (2) exemplaires

Signature AFFILIEE (<i>préciser</i>)	Signature CEA
<u>Date :</u> Madame/Monsieur <i>Fonctions</i>	<u>Date :</u> /Monsieur Patrick SAYD <i>Chef du DILS</i>