Demande n°4230 - ARED

Acronyme :CHIFFID

Identification

Identification

N°	4230
Année	2026
Statut	Soumis à l'établissement
Date de création	23/01/2026
Date de modification	23/01/2026
Date de soumission	23/01/2026
Acronyme	CHIFFID
Intitulé du projet / thèse	CHIFFrement de disques avec Intégrité des Données
Dispositif	ARED

Priorité régionale

Priorité régionale

Priorité régionale	Lien avec une politique publique de la Région (Cybersécurité, Agroécologie, Mer, Mobilités, Ports, Langues de Bretagne)

Stratégie régionale de recherche et d’innovation (S3)

Stratégie régionale de recherche et d’innovation (S3)

Domaine d'innovation stratégique (DIS) principal	Économie numérique sécurisée et responsable
Levier thématique associé au DIS principal	Cybersécurité
Axe transversal : transitions climatique et écologique	Non concerné
Axe transversal : cohésion et inclusion sociale	Non concerné

Organisme de tutelle

Organisme de tutelle

Établissement	INSA
Commune	RENNES
Civilité	Madame
Nom	Gouin
Prénom	Aurore

Unité de recherche

Unité de recherche

Nom de l'unité	IRISA
Civilité	Monsieur
Nom	Barais
Prénom	Olivier
Courriel	du@irisa.fr

Données complémentaires de l'unité de recherche

Libellé	Valeur
Statut et numéro de l'unité de recherche (UMR, USR, EA)	
Le cas échéant, nom de l'équipe de recherche	
Le cas échéant, nom du responsable de l'équipe de recherche	
Activités de recherche et points forts de l'équipe	Equipe SPICY (Security and Privacy) de l'IRISA, reconnue pour ses travaux sur les protocoles crypto. Membres complémentaires avec des compétences en crypto, implémentation, attaques et méthodes formelles.
Si implication dans un/plusieurs programmes européens ou internationaux, préciser	

Co-directeur de thèse

Description

Description du projet

Libellé	Valeur
Résumé synthétique du projet (2000 caractères max)	Le chiffrement de disque empêche un attaquant de récupérer le contenu d'un ordinateur en le démarrant sur une clef USB ou en branchant son disque sur un autre équipement. Le chiffrement de disques facilite aussi la fin de vie ou le changement de propriétaire d'un équipement puisqu'il n'est plus nécessaire d'effacer de manière sécurisée les données, opération coûteuse en temps. Alors que l'usage du chiffrement de disque devient une règle de bon sens, les outils actuels sont insatisfaisants. Qu'il s'agisse de logiciels intégrés aux systèmes d'exploitation comme BitLocker (Windows), FileVault (macOS) ou Luks (Linux) ou de logiciels indépendants comme VeraCrypt, aucun de ces outils n'assure l'intégrité des données. Il s'agit d'un problème peu étudié, qui est lié à l'utilisation du mode de chiffrement non authentifié XTS. L'usage combiné d'un algorithme de chiffrement avec un test d'intégrité (Encrypt-then-Mac) ou d'un mode de chiffrement authentifié n'est pas réalisable dans l'état actuel des connaissances, car la perte de performances est rédhibitoire. Ce projet de thèse vise à évaluer la menace, imaginer des scénarios d'attaque et apporter des solutions. Pour cela, un nouveau mode de chiffrement pourra être proposé ou, à défaut, les modes de chiffrement actuels pourront être adaptés pour atteindre un compromis raisonnable entre le gain en terme d'intégrité et la perte en terme de performances.
Porteur du projet : date d'obtention de l'HDR ou dérogation	Gildas Avoine (PR en France depuis 2013)
Collaborations scientifiques (nature/pays) et partenariat socio-économique envisagé (3000 car. max.)	Collaboration envisageable (contact pas encore pris) avec ANSSI sur les modes de chiffrements authentifiés pour chiffrement de disques durs.

Si DIS identifié, préciser l'adéquation du projet avec le DIS (2000 car. maximum)	
Si priorité régionale cochée, préciser en quoi le projet s'y rattache effectivement (2000 car.max.)	
Si priorité régionale "Politique publique Région", préciser (voir liste au point 4, Règlement 2025)	Projet soumis à CREACH LAB
Cotutelle financière internationale (oui/non)	Non
Nom(s) du(des) cofinanceur(s) envisagé(s) ou confirmé(s)	CREACH LAB
Si cofinancement industriel, justifier le choix du dispositif ARED au lieu du dispositif CIFRE	
État du cofinancement (indiquer "acquis" ou "demandé")	demandé
Si demandé, date prévisionnelle de réponse du cofinanceur	
Si cofinancement refusé, autre(s) source(s) de cofinancement identifiée(s)	
Si reversement prévu, préciser (partenaire, montant)	

Candidat

Collaboration internationale

Collaboration internationale

Pays	
Etablissement partenaire à l'étranger	

Pièces jointes

Date de mi	Type de pièce	Commentaire	Document	Valide	Commentaire
23/01/2026	ARED - Dépôt - CV du porteur	Obligatoire - Le CV doit préciser si le porteur est titulaire de l'HDR et, le cas échéant, depuis quand, et mentionner la liste des doctorant·e·s déjà encadré·e·s et des publications associées.	cv_gildas_avoine_2pages.pdf	Non traité	
	ARED - Dépôt - Avis directeur·rice d'unité	Obligatoire - Voir le modèle à suivre dans l'onglet "Documents à télécharger"		Non traité	
	ARED - Dépôt - Justificatif cofinancement	Facultatif - Dépôt de demande, justificatif d'obtention, courrier du cofinanceur pressenti...		Non traité	
	ARED - Dépôt - Lettre partenaire étranger	Facultatif - Lettre d'engagement de l'établissement partenaire étranger en cas de cotutelle internationale		Non traité	
	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	

	ARED - Instruction - Lettre de saisine	Lettre de l'établissement à transmettre à la Région (utiliser le modèle disponible dans la rubrique "Documents à télécharger")		Non traité	
	ARED - Versement - Convention de partenariat	Le cas échéant (si autorisation de reversement)		Non traité	
	ARED - Versement 2 - CV doctorant.e	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Copie du contrat doctoral (ou CDD ou attestation))	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Attestation bon déroulement travaux année 1	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Bilan financier année 1	Pour versement tranche 2 ARED		Non traité	
	ARED - Versement 3 - Attestation bon déroulement travaux année 2	Pour versement 50% tranche 3 ARED		Non traité	
	ARED - Versement 3 - Bilan financier année 2	Pour versement 50% tranche 3 ARED		Non traité	
	ARED - Versement 4 - Bilan financier année 3	Pour versement solde année 3 ARED		Non traité	
	ARED - Versement 4 - Certificat administratif précisant statut thèse	Pour versement du solde de la tranche 3		Non traité	