Mise en œuvre d'un démonstrateur pour la « self-sovereign identity »

Référence	CYBERINSTITUTE-INT-20010
Description	L'objectif du stage est de mettre en œuvre un démonstrateur de type « reference design » sur la « self-sovereign identity ». Actuellement, de nombreuses applications décentralisées (dApp) émergent. Orchestrées autour de smart contracts, leur particularité est qu'elles émettent des transactions depuis un compte dont l'identifiant est anonymisé. Cet identifiant peut servir à identifier l'utilisateur ou le possesseur du compte. On voit apparaitre une tension sur la notion de privacy : comment identifier un utilisateur qui utilise un identifiant anonymisé ? Le but du démonstrateur qui sera mis en œuvre pendant le stage est d'étudier cette problématique. Le stage se déroulera par étapes : 1) Tout d'abord, il s'agira de prendre connaissance de l'existant dans le domaine, notamment des recommandations du groupe (standard) W3C, des réalisations existantes (uport, sovrin, shocard…) et d'être critique sur les avantages et limites de chacune. 2) Puis de se familiariser avec les outils, les briques technologiques existantes au labo, le développement de smart contracts, leur déploiement et leur exécution sur une blockchain. 3) Il s'agira ensuite de faire un choix d'implémentation de l'identité décentralisée autour de smart contracts pouvant être accédés par trois types d'acteurs : l'utilisateur, le fournisseur et le contrôleur. Suivront le développement des smart contracts en langage « Solidity » et des dApps en Python. 4) On pourra ensuite s'intéresser à la génération des identifiants anonymisés, et envisager quels éléments cryptographiques doivent être transmis, présentés afin de permettre le contrôle. A cette étape, plusieurs critères de performance pourront être considérés : la légèreté (éléments courts et peu nombreux), la privacy (confidentialité, respect des données personnelles), la sécurité et la protection des secrets dans les dispositifs utilisateur. 5) un temps sera réservé à la rédaction du rapport de stage et d'un article scientifique. <u>Contexte</u> Le Grenoble Alpes Cybersecurity Institute regroupe environ 150 chercheurs - experts en informatique, cryptographie, micro-électronique mais également en droit international, politique et économie - issus de 16 laboratoires de l'Univ. Grenoble Alpes et travaillant dans les domaines de la cybersécurité et de la protection de la vie privée. Ses principaux axes de recherche sont les éléments sécurisés à bas coût, les infrastructures critiques sécurisées et leur gestion en terme de cycle de vie, l'analyse de vulnérabilité et les défis globaux en termes d'analyse des risques et de validation des grands systèmes, incluant la résilience pratique dans l'industrie et la société. En prenant en compte l'impact sociétal de la cybersécurité, cette approche – dite holistique – permet d'intégrer la recherche fondamentale dans un contexte plus large, donc plus pertinent (https://cybersecurity.univ-grenoble-alpes.fr).
Prérequis	Cybersécurité : Opérations sur courbes elliptiques, fonctions de hachage Informatique : Linux, Python, Javascript Motivation : Agilité et curiosité

Encadrant(s)	Christine Hennebert (PhD)
Candidature	Envoyer CV, lettre de motivation avec recommandation(s) de 1 ou 2 référents (dont responsable de la formation), relevés de notes de M1 (obligatoire) à cyberalps-contact@univ-grenoble-alpes.fr Pour plus d'information sur le stage, contacter : christine.hennebert@cea.fr
Localisation	CEA Grenoble, Laboratoire de Sécurité des Objets et des Systèmes Physiques
Date de début	Février 2020
Durée	6 mois
Gratification	Selon réglementation en vigueur (env. 560€/mois). Possibilité de prise en charge partielle des frais de transport.