# Compte-rendu n°2

(19 mai 2017 - 10 août 2017)

---

## Implémentation d'un service de trust list globale basé sur les concepts de blockchain

Yoann Raucoules

Année 2016-2017

Stage de fin d'études réalisé dans l'entreprise ARHS Spikeseed

en vue de l'obtention du diplôme d'ingénieur de TELECOM Nancy

Maître de stage : Vincent Bouckaert
Encadrant universitaire : Olivier Festor

# Table des matières

# 1 Sujet de stage

**Implémentation d'un service de trust list global basé sur la block-chain**

Dans le cadre d'un large projet européen de recherche Arηs Spikeseed travaille au sein d'un consortium de spécialistes dans le domaine de la confiance électronique. Ses responsabilités dans le cadre de ce projet couvrent notamment la révision de l'implémentation actuelle des Trusted Lists Européennes[1] de façon à la rendre plus générique et supporter des Trusted Lists étrangères (hors UE) ainsi que des fournisseurs de Trust Services étrangers. Dans la mesure où une grande partie des concepts liés aux block-chains sont applicables dans ce contexte, cette technologie sera utilisée dans le cadre de cette implémentation.

Le stagiaire aura pour mission :

- de se familiariser avec des concepts de cryptographie appliquée : certificats électroniques, signatures électroniques avancées, block-chain ;
- sur base de l'analyse haut niveau réalisée lors d'une phase précédente du projet, d'effectuer l'analyse technique plus détaillée débouchant sur des choix d'implémentation ;
- d'éprouver ces choix (réalisation de Proof of Concept), de les présenter aux autres membres du consortium lors de conférences vidéo afin de les faire valider ;
- sur base de cette analyse technique détaillée, d'implémenter des composants utilisés dans le service de Trust List globale ;
- de documenter tous les aspects techniques et fonctionnels de la solution implémentée ;

Le stagiaire aura à sa disposition :

Un environnement de développement fourni par Arηs Spikeseed (ordinateur portable) ;

Un tuteur qui aura pour rôle de le suivre, de le conseiller mais également d'effectuer les revues des livrables produits par le stagiaire (documentation, livrables applicatifs), ce tuteur sera Vincent Bouckaert, responsable de l'équipe Digital Trust au sein d'Arηs Spikeseed ;

Toutes les ressources d'infrastructure nécessaires au bon déroulement du stage (machine virtuelle, matériel informatique, outils de développement, documentation).

---

[1] Cfr. ETSI 119 612, v2.2.1 (http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020201p.pdf)

Le stage est réalisé dans les locaux d'Arŋs Spikeseed, la langue officielle du projet pour les communications avec les autres membres du consortium (mails, documents, conférence téléphonique) est l'anglais ; la langue utilisée en interne est principalement le français.

Le stage est rémunéré.

**Mots-clés** : Java, blockchain, Advanced Electronic Signatures, SAML 2.0, Open ID Connect, OAuth, Git, GitLab.

# 2 Les tâches accomplies

Comme indiqué dans le compte-rendu précédent, la phase entreprise mi-mai a été de concevoir une preuve de concept permettant de valider le choix des technologies qui seront mises en œuvre dans le cadre du service de Global Trust List. Cette preuve de concept a consisté au développement d'une API REST s'interfaçant avec un système de stockage d'informations décentralisé, dans lequel les données sont adressables à partir d'un hash représentatif de ces données, et avec une blockchain permettant de conserver les adresses de stockage de manière transparente, immutable et sécurisée. L'implémentation résultante ayant été très concluante, nous avons choisi de conserver les deux technologies utilisées qui sont IPFS, pour le système de stockage d'informations décentralisé, et Ethereum, pour la blockchain.

La phase suivante a consisté à imaginer l'implémentation du service de trust list global (gTSL). Pour cela, j'ai eu pour mission de :

- Définir l'API REST qui permettra aux utilisateurs externes d'accéder aux informations de la gTSL ;
- Concevoir la gestion des utilisateurs qui est basée sur un système de votes entre les acteurs de la gTSL ;
- Concevoir le module permettant gérer la persistance des données de manière décentralisée ;
- Concevoir un gestionnaire de versions afin de conserver l'historique des mises à jour de la gTSL ;
- Concevoir un moteur de recherche efficace permettant aux utilisateurs d'effectuer des recherches sur base de filtres dans la gTSL ;
- Concevoir un module permettant de conserver les adresses des données dans la blockchain ;
- Définir le workflow d'ajout, d'édition et de suppression d'une liste dans la gTSL.

Ensuite, mon rôle a été de mettre en place l'installation du projet, de documenter le processus d'installation et d'écrire le mode d'emploi pour l'équipe de développement. Pour réaliser cela, j'ai pu utiliser Docker afin de créer un conteneur exécutant un nœud IPFS et un second conteneur permettant de se connecter à la blockchain Ethereum. J'ai aussi réalisé des scripts Shell afin d'automatiser au maximum le processus de build et de run.

Enfin, nous avons débuté l'implémentation de la gTSL qui est actuellement toujours en cours de développement. La date de livraison du projet est prévue pour le 30 novembre 2017.

# 3 Les travaux futurs

Dans un premier temps, les tâches à effectuer sont la rédaction du mémoire qui doit être rendu au plus tard le 4 septembre et la préparation de la soutenance qui aura lieu le 22 septembre.

Ensuite, l'implémentation de la gTSL sera poursuivie. Cette phase consiste à implémenter les modules définis lors de la conception à savoir :

- Un module de gestion des utilisateurs, basé sur votes d'un consensus, à l'aide d'un smart-contract déployé dans la blockchain Ethereum ;
- Un module de gestion des données, utilisant IPFS ;
- Un module de conservation des adresses à l'aide d'un smart-contract déployé dans la blockchain Ethereum ;
- Un module de gestion de versions permettant de conserver l'historique des mises à jour de la gTSL ;
- Un module de recherche sur les données de la gTSL ;
- Un module d'import/export de fichier XML des données ;
- Un module de signature des listes de confiance.

Enfin, la dernière tâche sera de documenter tous les aspects du système mis en place.

# 4 Les difficultés rencontrées

La seule difficulté rencontrée a été de concevoir un moteur de recherche optimisé en utilisant IPFS. En effet, aucun outil répondant à notre besoin de recherche d'informations dans IPFS sur base de filtres n'existe actuellement. Nous avons envisagé deux solutions pour mettre en place une recherche sur la gTSL. La première solution est de créer un « reverse-index » sur les données qui peuvent être filtrées, cela permettra une recherche rapide mais nous force à concevoir un gestionnaire d'index, de trouver une solution pour conserver les index et de modifier la structure actuelle des données afin d'optimiser les recherches. La seconde solution envisagée est de représenter les données de la gTSL comme un arbre et de procéder à un filtrage en supprimant les branches inintéressantes au fur et à mesure de l'exploration de l'arbre. L'implémentation du moteur de recherche n'ayant pas encore débuté, il est possible que d'autres solutions soient envisagées et préférées.