Compte-rendu n°1

(03 avril 2017 - 19 mai 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, block-chain, Advanced Electronic Signatures, SAML 2.0, Open ID Connect, OAuth, Git, GitLab.

2 Les tâches accomplies

Dans un premier temps, les tâches réalisées ont consisté à se familiariser avec le projet, c'est-à-dire le contexte du projet, les notions techniques relatives au projet ainsi que les outils déjà mis en place dans le cadre du projet. Concernant le contexte, différents documents de conception ont été mis à ma disposition afin que je puisse comprendre la finalité du projet. J'ai donc commencé par lire ces documents et j'ai ensuite pu échanger avec mon maître de stage sur les éventuelles incompréhensions ou questions survenues lors de la lecture. Ensuite, j'ai dû effectuer des recherches en autonomie sur divers concepts (cryptographie, certificats, signature électronique) en lien avec le projet. Parmi les concepts, on peut notamment citer : PKI (Public Key Infrastructure), -AdES, SAML 2.0, OAuth 2 ou encore OpenID Connect. Au niveau des outils, j'ai pu me familiariser avec TLManager[2] et SD-DSS[3]. TLManager est un outil spécifique au projet qui a pour but de fournir à ses utilisateurs des fonctionnalités de gestion de listes de Trust Services. Cet outil m'a permis de me familiariser avec les notions importantes du projet (notamment les notions de Trust Service Status Lists, Trust Service Providers, Trust Services). SD-DSS est une librairie Java sur laquelle est basée TLManager et qui fournit un ensemble de fonctionnalités permettant de générer et de valider divers formats de signatures électroniques ayant une valeur légale au sein de l'Union Européenne. J'ai pu prendre en main cette librairie qui va être utilisée lors de la phase d'implémentation.

Dans un second temps, j'ai été confronté à des tâches de recherche et développement impliquées par ce projet. Ces recherches tournent autour de concepts très récents qui sont la blockchain et le web décentralisé. Le but du projet est de mettre à disposition des utilisateurs toutes les informations concernant les Trust Service Status Lists de manière décentralisée, ce qui permet le « no single point of failure », et d'utiliser les concepts, notamment d'immutabilité, de résilience, de transparence et de non contrôle par un organisme tiers, de la blockchain pour substituer au système actuel. Parmi les technologies qui ont été envisagées on peut citer par exemple : Ethereum, Swarm, IPFS, StorJ, Openchain ou BigchainDB. Cette recherche a résulté en un document de comparaison qui a été fourni aux différents acteurs du projet.

Enfin, une dernière tâche a été de tester la capacité et la prise en main des différents outils relevés durant la phase de recherche. Le premier à avoir été examiné est Openchain. Pour cela, j'ai pu déployer une instance de l'outil dans une machine virtuelle ainsi que créer une image Docker afin d'interfacer l'outil avec une base de données MongoDB. Ensuite, j'ai pu

[2] Voir https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/TL+Manager+v5.1

[3] Voir https://github.com/esig/dss

analyser BigchainDB, Ethereum, Swarm et enfin IPFS. Pour Swarm et IPFS, j'ai pu mettre en place trois machines virtuelles afin de créer un réseau « peer-to-peer » décentralisé et privé permettant le stockage des données de manière distribuée. Ces différentes analyses ont fait l'objet de documents écrits notamment pour les installations et les points importants des différentes technologies.

3 Les travaux futurs

La phase de conception venant d'arriver à son terme, la phase suivante est donc l'implémentation. Afin de préparer l'implémentation des spécifications du projet, j'ai à charge de mettre en place une preuve de concept utilisant les technologies explorées durant la phase de recherche. Cette preuve de concept consiste à développer une API REST s'interfaçant avec un système de stockage d'informations décentralisé et une blockchain afin de conserver les adresses de stockage de manière transparente et sécurisée.

Concernant l'API REST, elle sera développée en Java et utilisera le framework Spring Boot. À l'heure actuelle, les deux technologies envisagées pour le stockage d'informations sont Swarm et IPFS. Enfin, Ethereum a été retenu pour la partie blockchain. La Figure 1 ci-dessous illustre le système qui sera mis en place.

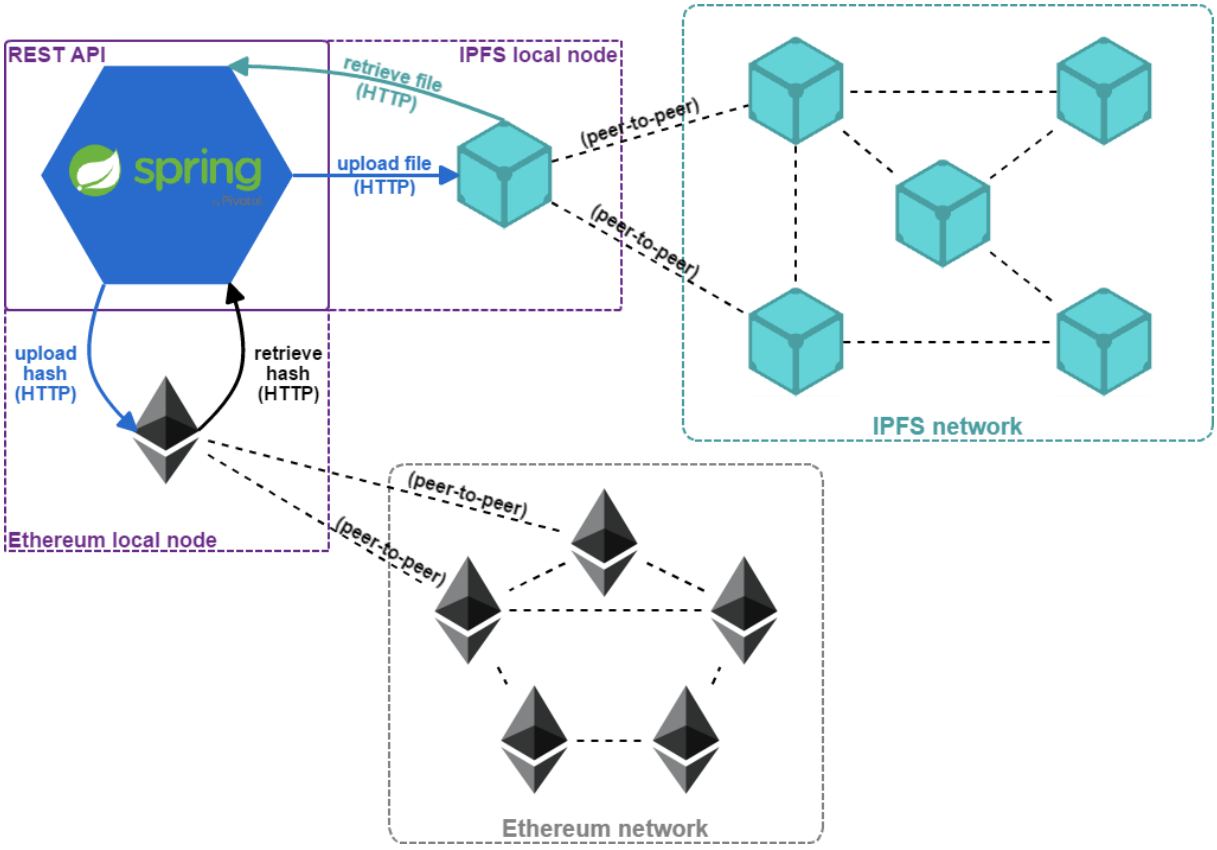

Figure 1 : Schéma de la preuve de concept

4 Les difficultés rencontrées

La première difficulté rencontrée a été de se familiariser rapidement avec les différentes notions de cryptographie, de certificats et de signatures électroniques énoncées précédemment. En effet, ce sont des notions dont je ne connaissais pas le fonctionnement, j'ai donc dû m'initier à chacune d'entre elles.

La seconde difficulté a été de mettre en place les différents outils à la suite de la phase de recherche. En effet, la plupart de ces outils sont très récents et donc peu stables et/ou peu documentés. J'ai donc dû m'adapter à cette situation en explorant entièrement les documentations ou en interagissant directement avec des développeurs impliqués dans ces projets.