CAHIER DE CHARGE

Développement d'un module de signature électronique (PKI)

Oumar Djimé Ratou

7 avril 2019

Table des matières

1 Description et compréhension du projet

Le projet soumis à mon analyse consiste à mettre sur pied un module de signature électronique basant sur l'infrastructure à clés publique(ICP) ou la Public key infrastructure (PKI). Il va consister dans un premier temps :

— générer la paire de clés (publiques et privées),
— créer le certificat.

et ensuite :

— calculer une valeur de hachage du document(empreinte numérique),
— chiffrer l'empreinte générée avec la clé publique,
— créer la signature avec la clé privée,
— vérifier la signature avec la clé publique.

Ainsi le module permettra à d'autres développeurs d'intégrer facilement dans leur plateforme de même technologie afin que les utilisateurs finaux puissent l'utiliser aisément.

2 Étude de la faisabilité technique

2.1 Contexte et problématique

La création des signatures électronique basant sur les infrastructures à clé publiques que sa soit avec OpenSSL ou d'autres se font soit en console, soit d'utiliser des outils propriétaire (Word, Adobe Reader, DocuSign, Eversign, Yousign etc.), soit d'aller chez une Autorité de Certification (AC), qui sont complexes et coûteux pour les utilisateurs et surtout à ceux qui débutent en développement des applications et en sécurité informatique. Et encore malheureusement ils sont déjà intégrés dans leurs applications complètes, donc pas des moyens de les réutiliser dans d'autres logiciels comme des modules.

Les problèmes qui surviennent souvent dans les entreprises en particulier et chez les développeurs en général c'est la disposition des programmes modulaires pour intégrer facilement dans leurs plates-formes en fin de gagner en temps et en l'argent (surtout pour les entreprises). Ces nécessités nous amènent à nous poser les questions suivantes :

— Comment peut-on rendre cette difficulté de signer un document de manière transparente ?
— Comment faciliter le développement d'un outil informatique au sein de l'entreprise ?

2.2 Objectifs

2.2.1 Objectif global

Il sera question pour moi de développer un module des gestions des signatures basant les infrastructures à clé publique.

2.2.2 Objectif spécifique

De façon spécifique, il sera question pour moi de gérer les problèmes spécifiques liés aux :

— Création d'une signature d'un document numérique (texte, son, vidéo, PDF, etc.) en se basant sur les infrastructures à clé publique ou PKI,
— automatisation de la création des la signature à la main et autres,
— vérification de la signature de document numérique,
— prouver l'authenticité d'un signataire,
— faciliter à l'entreprise lors d'un besoin d'un module de signature électronique,

— rendre la vie facile au développeur qui ne maîtrise pas forcément la notion de cryptographie qui se cache derrière la signature numérique, d'intégrer ce module dans sa plate-forme.

Environnement

L'environnement dans lequel nous nous trouvons est favorable au projet puisqu'un tel système existe certes mais sous une licence payante non modulable. Sa mise en œuvre sera une innovation importante dans l'évolution numérique au sein de l'entreprise.

3 Description des besoins

3.1 Spécifications fonctionnelles

Notre module des signatures électronique aura comme spécification fonctionnelle :
— générer des paires de clés(publique et privée),
— signer un document numérique à l'aide de la clé privée,
— vérifier la signature d'un document numérique à l'aide de la clé publique,
— chiffrer/déchiffrer un document,
— générer un hash d'un document.

3.2 Spécifications non-fonctionnelles

Comme spécification non-fonctionnelle, nous aurons :
— authentification : le fait de s'assurer que l'expéditeur est bien celui qu'il prétend être,
— intégrité : le fait de s'assurer que l'information ne subisse aucune altération ou destruction volontaire ou accidentelle, et conserve le format initial,
— le module doit être ergonomique,
— fonctionne 24 heure sur 24, 7 jours sur 7.

4 Délai

J'estime que ce module pourra me prendre 1 à 2 mois.