Valentin Calmels
Hugo Lagahe

Mohamed Maachaoui

Projet cryptanalyse

2021/2022

Sommaire :

Guide d'utilisation

Notre solution se compose de deux applications. La première et la principale, permet aux étudiants de déposer une demande de diplôme ainsi que de vérifier l'intégrité d'un diplôme. Elle permet également aux administrateurs de faire ces mêmes actions, mais aussi, s'ils se connectent, peuvent valider la demande et donc générer des diplômes. Cependant pour cela ils auront également besoin, en plus de leur connexion grâce à leurs identifiants, de générer un OTP pour confirmer leur identité.

Cela nous amène donc à notre deuxième application qui est destinée uniquement aux administrateurs. Elle leur permet de se connecter et de générer un OTP pour pouvoir confirmer leur identité sur l'application principale.

Tout d'abord, pour être sûr que notre solution fonctionne pour le mieux, il sera nécessaire d'installer les librairies utilisées. Pour cela veuillez ouvrir un terminal à la racine du projet, ou se trouve le fichier ***requirements.txt*** et exécuter la commande suivant : ***sudo pip install -r requirements.txt***

Application principale :

- pour lancer l'application, se déplacer dans le dossier **/src** du projet
- ouvrir un terminal et exécuter la commande suivante ***python3 main.py***
- une fois l'application lancé vous vous retrouvez dans un menu ou plusieur choix s'offrent à vous
  - s'identifier en tant qu'administrateur
    - l'administrateur peut alors saisir ses identifiants pour se connecter
    - un nouveau choix s'offre à lui
      - déposer une demande de diplôme
        - cette fonctionnalité est de nouveau accessible depuis le menu des administrateurs pour éviter qu'ils soient obligés de se déconnecter pour en saisir une
      - valider des demandes de diplômes
        - la liste de toutes les demandes en cours apparaît alors dans le terminal
        - l'administrateur choisit alors une demande en saisissant son ID
        - il peut ensuite la valider en saisissant son OTP (valable trente secondes) pour confirmer son identité
        - le diplôme est alors généré et envoyé par mail à l'utilisateur
      - se déconnecter
        - l'administrateur reviens alors sur le menu principal
    - si l'administrateur n'a pas encore d'identifiants, il lui suffit de saisir des informations quelconques et il lui sera alors proposer de s'enregistrer
  - déposer une demande de diplôme
    - cette fonctionnalité est accessible par tous les utilisateurs (étudiants et administrateurs)

        - il est alors demandé plusieurs informations à l'utilisateur pour la réalisation du diplôme : le nom de l'étudiant, son prénom, son mail et le diplôme qu'il prépare.
    - ➢ extraire les informations d'un diplôme
        - cette fonctionnalité est accessible par tous les utilisateurs (étudiants et administrateurs)
        - l'utilisateur est alors invité à s'assurer d'avoir bien déposer le diplôme dans le dossier **/sources**
        - ensuite il lui est demandé de saisir le nom (avec son extension) du fichier qu'il a déposé
        - un rapport est finalement généré qui présente les informations dissimulés par stéganographie dans l'image ainsi que les informations signés dans le qrcode
    - ➢ quitter l'application
        - l'application se ferme

Application secondaire pour générer l'OTP :

- pour lancer l'application, se déplacer dans le dossier **/src** du projet
- ouvrir un terminal et exécuter la commande suivante ***python3 generateOTP.py***
- il est ensuite demandé à l'administrateur de se connecter avec ses identifiants (il n'est pas possible de créer un compte administrateur depuis cette application, uniquement depuis la principale)
- un choix est ensuite proposer à l'utilisateur
    - ➢ générer un OTP
        - un code à 6 chiffres (OTP) est alors fourni à l'utilisateur. Il est valable pendant 30 secondes, si l'administrateur essaie d'en générer un autre pendant ce même laps de temps, c'est le même code qui lui sera fourni
    - ➢ se déconnecter
        - l'application se ferme

Public Key Infrastructure (PKI)

A) Introduction

Tout d'abord il faut savoir pourquoi la PKI à été créée. Un exemple est lorsque l'on veut se connecter à un site web, la connexion se fait par chiffrement symétrique et asymétrique mais un man in the middle reste possible. Il fallait un moyen de s'assurer que les clés fournies étaient bien celles de son correspondant.
Pour cela les certificats et les PKI ont été créés.

B) Les certificats

Les principes du certificat sont :
• Confidentialité : La donnée que j'envoie n'est lisible que par mon destinataire
• Intégrité : La donnée que j'envoie n'est pas altérée, ou j'ai les moyens de le détecter
• Authenticité : Lors d'un échange, je peux m'assurer de l'authenticité de mon destinataire (il est identifiable et je peux lui faire confiance)

C) PKI

Cela nécessite une relation de confiance. En effet, quand le site internet fourni le certificat il doit faire confiance au site pour l'accepter et ensuite pouvoir s'y connecter.
Pour cela nous aurons besoin de la PKI ou « infrastructure à clés publique » qui permet de :

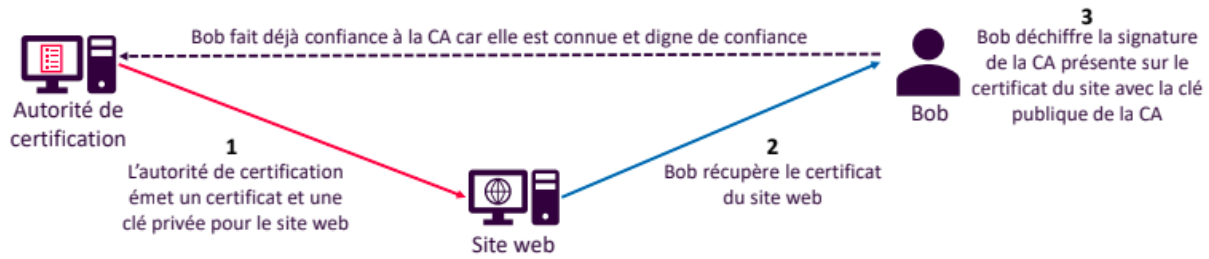
- Générer des certificats
- Assigner des rôles aux certificats
- Rassembler des autorités de confiances

Il en existe plusieurs type :

- Autorité de certification (CA Certification Authority)

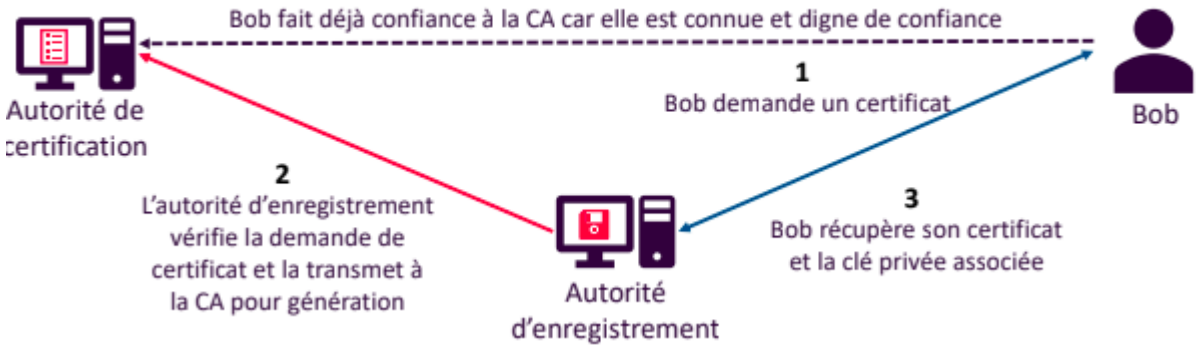
Elle peut émettre et vérifier des certificats et c'est un serveur de confiance, sécurisé et connu des clients.

Le fonctionnement de la PKI fonctionne sur le principe de la chaîne de certification. L'autorité de certification "racine" signe tous les certificats qu'elle émet. Un client final qui reçoit un certificat publique peut demander à l'autorité "racine" de vérifier l'authenticité du certificat publique.



- Autorité d'enregistrement (RA Registration Authority)

C’est le point d’entrée pour les processus de demande de certificats, elle permet également de vérifier qu’un certificat est toujours valide (principe de révocation). Elle permet à la CA de déléguer une partie de ses actions.



Choix d’implémentation

Nous avons choisis d’avoir une BDD avec deux tables : admins et demandesDiplome. La première pour stocker les infos de la partie administration (qui ont accès à la création, validation et vérification des diplômes) et la seconde pour stocker les demandes de diplômes.
Pour le hash nous avons choisi sha256 car plus sûr que md5.
Nous avons également choisi PKCS1_PSS pour la signature car c’est considéré comme sécurisé.
Schéma signature :

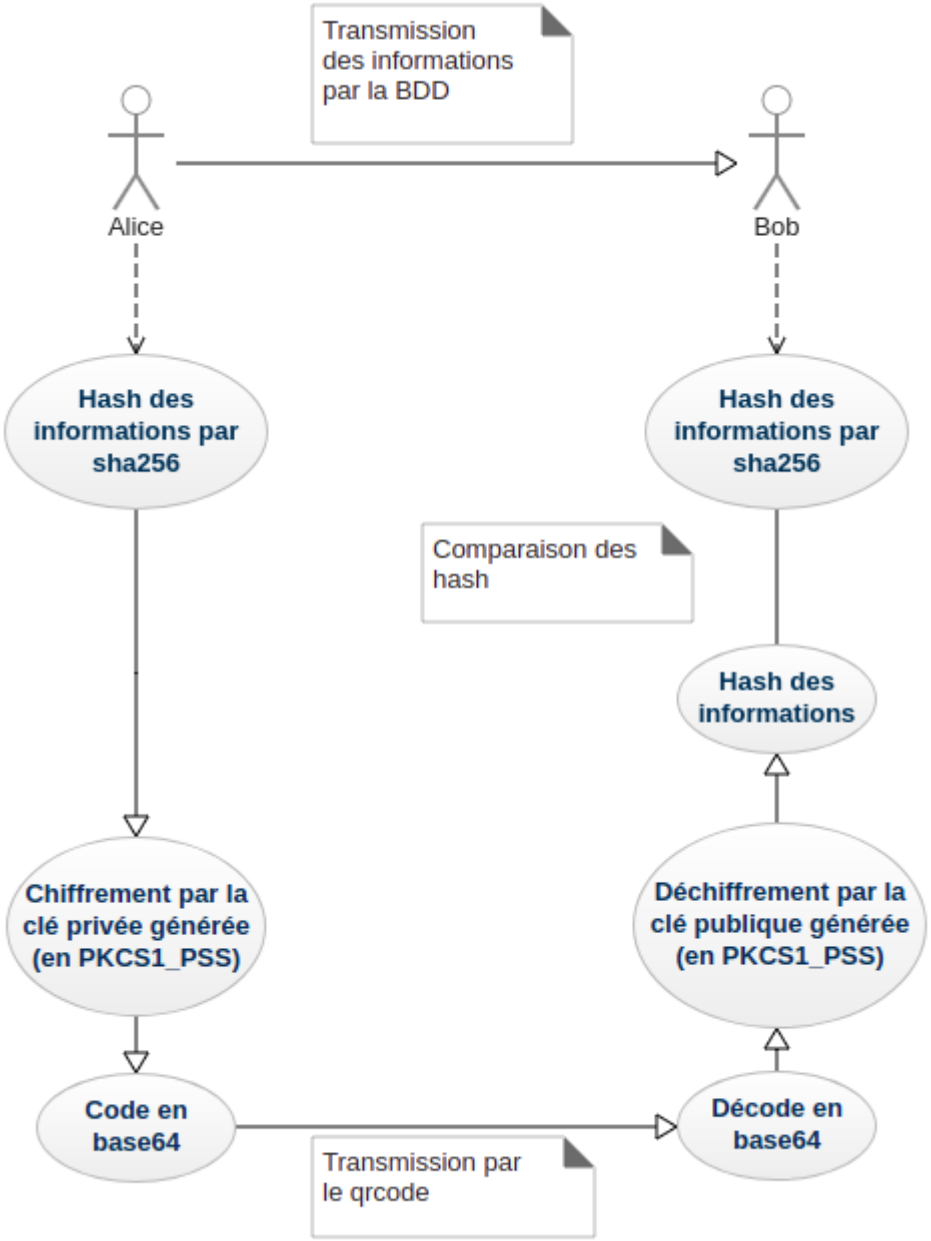
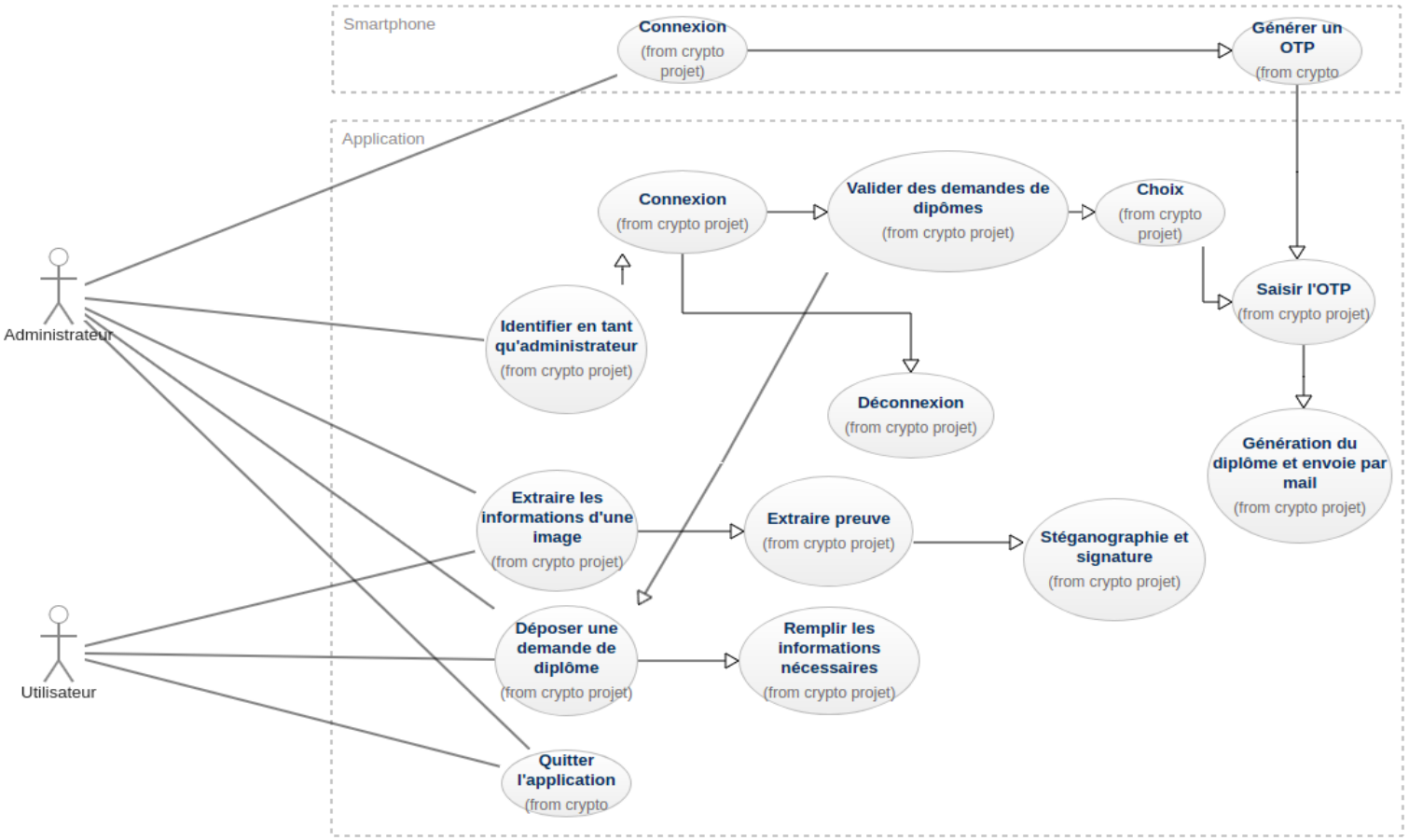


Schéma général :


Smartphone
Connexion
(from crypto projet)
Générer un OTP
(from crypto
Application
Connexion
(from crypto projet)
Valider des demandes de dipômes
(from crypto projet)
Choix
(from crypto projet)
Saisir l'OTP
(from crypto projet)
Administrateur
Identifier en tant qu'administrateur
(from crypto projet)
Déconnexion
(from crypto projet)
Génération du diplôme et envoie par mail
(from crypto projet)
Extraire les informations d'une image
(from crypto projet)
Extraire preuve
(from crypto projet)
Stéganographie et signature
(from crypto projet)
Utilisateur
Déposer une demande de diplôme
(from crypto projet)
Remplir les informations nécessaires
(from crypto projet)
Quitter l'application
(from crypto