UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Licence 3 INFO
INFO0503

TP n°11

Signatures et certificats

Le but de ce TP est de créer des certificats personnalisés et de mettre en place une autorité de certification. Nous pourrons ainsi reprendre les applications du TP précédents en utilisant cette fois-ci la gestion des certificats.

1 Création d'un certificat

Nous souhaitons écrire nos propres certificats au format JSON. Ils seront utilisés au moment de l'établissement d'une connexion entre deux applications pour vérifier leur identité.

Nous supposons qu'un certificat contient les informations suivantes :

- Nom de la machine (une chaîne de caractères correspondant à l'application)
- Adresse IP de la machine
- Clé publique
- Nom de l'autorité (une chaîne de caractères)
- Adresse IP de l'autorité de certification qui a généré le certificat
- Signature du certificat

La signature doit être réalisée sur les clés et les données et non sur la chaîne de caractères correspondant au format JSON du certificat. Avec deux JSON identiques (clés et valeurs), mais avec un formatage différent (espaces, tabulations ou retours à la ligne), nous obtenons deux signatures différentes.

Questions

Dans un premier temps, nous ne nous intéressons pas à la signature.

1. Créez la classe `Certificat` permettant de représenter un certificat.
2. Ajouter les méthodes pour permettre la gestion JSON (sérialisation + désérialisation).

Un certificat possède une signature qui est soit récupérée (lors de la réception d'un certificat), soit calculée à partir des données. Une méthode doit permettre également de vérifier la signature fournie.

3. Ajoutez la gestion de la signature.

2 Autorité de certification

Nous souhaitons développer une autorité de certification qui attend des connexions (TCP) sur un numéro de port donné. Elle doit pouvoir fournir son propre certificat ou créer des certificats à la demande de clients.

Au démarrage d'un client, nous devons vérifier si les clés existent (publique et privées) et qu'un certificat est présent. Si le certificat n'existe pas, un nouveau est généré en contactant l'autorité de certification. Le nom du fichier contenant le certificat, l'adresse de l'autorité de certification et le nom du fichier contenant le certificat de l'autorité sont spécifiés dans le fichier de configuration.

Questions

1. Quelles sont les requêtes auxquelles doit répondre l'autorité ? Quelles données sont échangées ?
2. En vous aidant du code des applications du TP précédent et de l'exercice précédent, développez votre autorité de certification.
3. Développez un client et un serveur qui exploitent les certificats de l'autorité pour s'echanger des données chiffrées (reprenez les applications du TP précédent).