TP 2: La certification en Openssl

Des aides:

- Vous aurez: le document pdf sur Openssl (de la dernière fois) et un powerpoint sur la certification en Openssl de Roberta Daidone

1. Générez une paire de clés RSA de 2048 bits dans un fichier Keys.pem. Vérifiez la longueur de p,q, et du module N = pq dans la clé publique. Chiffrez votre fichier Keys.pem avec 3Des.
2. Exportez la clé publique dans un fichier PKey.pem.
3. Vous allez jouer le rôle d'une autorité de certification (AC) et, au même temps, celui d'une personne qui veut certifier sa clé publique. Du côté AC : créez un répertoire qui s'appelle exampleCA. Dans ce répertoire-ci, créez deux répertoires : un qui s'appelle certs, l'autre qui s'appelle private. Pour ceci vous pouvez utiliser la commande

   ```
   mkdir certs private
   ```

   Puis changez les permissions pour le répertoire private : *chmod 700 private* . Vous devez créer également un comptoir pour le numéro de certifs issus par l'AC. On fait cela avec la commande :

   ```
   echo '01' > serial
   ```

   Vous pouvez visualiser l'effet en utilisant la commande *ls* (le fichier serial a été créé) et puis la commande *cat*.

4. Créez deux fichiers : index.txt et openssl.cnf en utilisant la commande touch :

   ```
   touch index.txt
   touch openssl.cnf
   ```

   Le dernier de ces deux fichiers et un fichier de configuration pour les certificats. Ce type de fichier donne toujours le contenu et les usages d'un certificat.
5. Exécutez les commandes sur le transparente 5 de la présentation de Daidoni.
6. On va maintenant configurer le fichier openssl.cnf. Lisez attentivement les transparents 6 à 10 de la présentation de Daidoni. Essayez d'expliquer, en vos propres mots, la signifiance de chacun des détails à remplir.
   Maintenant on doit rédiger le fichier openssl.cnf dans le même style. Ce fichier doit contenir tout le contenu sur les transparents 7 à 10 (dans les boites).
   Utilisez par contre la fonction sha1 au lieu de md5 pour default_md (pourquoi ?) et puis, pour le commonName utilisez ExampleCA, enlevez stateOrProvinceName, pour countryName utilisez FR (attention : le nom du pays a toujours seulement 2 charactères au max), et puis pour l'organizationName : CA for IntroToSecurity.
   Pour rédiger ce fichier vous pouvez utiliser votre éditeur favorit.

7. Maintenant on va créer une requête de certification pour certifier notre clé de certification. Utilisez la commande :
   ```
   openssl req -x509 -newkey rsa:2048 -out cacert.pem -outform PEM
   ```
   Vous devez également donner un mot de passe pour chiffrer la clé privée.
8. Cela doit avoir généré deux fichiers : le fichier privkey.pem dans le répertoire exampleCA/private et le fichier cacert.pem dans exampleCA/. Pourquoi est-ce que le fichier privkey a été généré également ? (Indication : il faut revoir le fichier de configuration…). Vérifiez l'existence de ces deux fichiers.
9. Visualisez le certificat en utilisant la commande :
   ```
   Openssl x509 –in cacert.pem –text –noout
   ```
10. Attention: les clés générées pour l'AC ne sont pas les clés dans le fichier keys. En fait on a utilisé la commande : `–newkey rsa :2048` pour générer une nouvelle paire de clés pour l'AC.
11. Maintenant on joue le rôle d'une personne qui veut certifier sa clé publique (la clé dans PKey.pem). On doit créer une requête de certification (qu'on appelle Certreq) en utilisant la commande :
    ```
    openssl req –new –key Keys.pem –out Certreq
    ```
    Vous devez remplir quelques details sur votre identité. Vous pouvez voir ce qui veulent dire les initiales : C, ST, etc. dans le document joint (pas les transparents, l'autre). Pour Country, utilisez la France (toujours FR), pour l'ST, c'est la Bretagne. Pour la location, utilisez Rennes, après pour l'Organisation : ISTIC (par exemple). Pour le CN, veuillez utiliser votre nom et prénom, et donnez une adresse email.
    Après la création du fichier, veuillez visualiser le fichier que vous avez créé en utilisant la commande :
    ```
    openssl req -in Certreq -text -noout
    ```
12. Normalement, l'usager va envoyer le fichier Certreq à l'autorité de certification. Pour l'instant, comme vous jouez le rôle de l'AC, vous devez signer cette requête en utilisant la clé de l'AC. Quelle clé est-ce que vous devez utiliser – la clé publique où la clé privée de l'AC? Où se trouve-t-elle ?
13. Signez la requête en utilisant la commande :
    ```
    openssl x509 -days <durée de validité en jours> -CAserial
    serial -CA cacert.pem -CAkey <chemin au fichier necessaire pour
    la clé dans la question 12>-in ../req -req -out ../cert
    ```
14. Visualisez votre certificat en utilisant la commande :
    ```
    openssl req -in Certreq -text –noout
    ```
    Lisez maintenant le contenu du fichier serial. Pourquoi a-t-il changé ?
15. Maintenant vous avez une paire de clés – privée et publique (Keys.pem) et un certificat pour eux : cert. On va les utiliser pour signer et chiffrer un courriel. Suivez les instructions dans la section 3.4.1 du pdf joint.