TP4 Public Key Infrastructures

Ce TP est consacré à la mise en place d'une IGC (Infrastructure de Gestion des Clefs), ou PKI (Public Key Infrastructure), et à la création de certificats pour diverses utilisations.(sécurisation de sites web (authentification serveur et client), S/MIME, OpenVPN, IPsec, etc).

Conservez bien votre PKI, vous en aurez besoin pour les TP de système et de sécurité web !

Joignez à votre compte-rendu une archive contenant toute votre PKI (vous pouvez retirer les clefs privées).

Nous allons mettre en place une IGC à deux niveaux : je joue le rôle d'une autorité racine, qui certifiera des autorités intermédiaires. L'autorité intermédiaire délivrera des certificats :

- pour le courrier électronique S/MIME ;
- pour l'authentification client ou serveur TLS (SSL) ;
- pour un VPN IPsec (cf RFC 4945) ;
- pour un VPN OpenVPN en configuration client/serveur ;

Le rôle de l'autorité racine est de fournir des certificats pour les autorités intermédiaires. L'autorité que nous utiliserons est l'autorité M2_SSI.

La RFC 5280 contient le descriptif de tous les champs des certificats X.509. Voir aussi RFC 6487 de février 2012.

Exercice 1 (Diffusion de l'autorité) Pour être reconnue, l'autorité racine doit être intégrée dans les outils qui l'utiliseront.

Récupérez sur Universitice le certificat x509 de l'autorité. Son fingerprint sha256 est (option `-fingerprint` de la commande `x509` de `openssl` par exemple)
`01:1B:B1:FA:8A:8F:6E:1F:8F:A3:30:4A:C8:D1:71:07:`
`BA:75:E7:12:96:3D:3D:44:08:65:66:50:64:9D:24:2C`.

Expliquez à quoi sert le fingerprint, et pourquoi il est important de le vérifier ici (par exemple, quelle attaque pourrait-on envisager s'il n'était pas vérifié ?).

Selon l'environnement de travail que vous utilisez (windows, distribution linux, MAC-OS, etc.), vous pouvez double-cliquer sur votre certificat et l'importer. Comment faites-vous pour vous assurer de la validité de ce certificat ? Décrivez la procédure d'importation propre à votre poste, en vous assurant que ce certificat est bien reconnu comme valide. Si un mot de passe vous est demandé, expliquez à quoi il correspond.

Importez le certificat dans votre navigateur web. À quoi correspondent les différents onglets/magasins de certificats ? (Client, serveur, Autorités Intermédiaires, Autorités Racines)

Affichez le certificat sous votre navigateur, puis avec openssl en utilisant la commande

```
$ openssl x509 -in unCertif.crt -text -noout
```

Pour quel(s) usage(s) [1] ce certificat peut-il être utilisé ? (vous pouvez utiliser l'option `-purpose` de la commande `x509` de `openssl` et la section `CERTIFICATE EXTENSIONS` du manuel de `x509`).

1. Rappelez le contenu d'un certificat numérique. De toutes les données contenues dans le certificat, quelles sont celles qui sont des données en clair ? quelles sont celles qui sont des données produites après calculs cryptographiques ? Est-ce que le fingerprint `sha1` ou `sha256` est contenu dans le certificat ? Expliquez pourquoi.
2. A quoi correspondent les champs `issuer` et `subject` ? Qu'est-ce qu'un certificat racine ?
3. Lorsque votre navigateur se connecte sur un site web, le serveur lui envoie non seulement son certificat serveur, mais également plusieurs autres certificats. Lesquels et pourquoi ?

Exercice 2 (Création d'une autorité intermédiaire) Vous allez établir une autorité intermédiaire qui sera signée par notre autorité M2_SSI. Pour obtenir la signature de la clef publique de votre autorité intermédiaire par l'autorité M2_SSI, vous devez présenter à l'autorité une *requête* contenant votre clef publique et l'identité de votre autorité intermédiaire. Pour générer une requête de certificat au format PEM pour la clef privée `macle.pem`, vous utiliserez la commande

```
$ openssl req -new -key macle.pem -out requete.req
```

1. Générez une bi-clef RSA de 2048 bits pour l'autorité intermédiaire. Créez ensuite une requête de certificat pour votre autorite intermédiaire, vous choisirez le même DN (Distinguish Name) que l'autorité M2_SSI sauf pour
   — le Nom usuel (=CN) : `Autorite Intermediaire Nom`
   — l'email (le votre).
2. Visualisez là avec la commande

   ```
   $ openssl req -in requete.req -text -noout
   ```

   Expliquez les différents éléments contenus dans cette requête. La clef privée du sujet y figure-t-elle ? et sa clef publique ?
3. Transmettez-moi votre requête de certificat, sur universitice en incluant votre nom dans le nom de ficher de votre requête. Je vous donnerai alors un certificat pour votre autorité intermédiaire. En attendant, vous pouvez commencer l'exercice suivant.

Exercice 3 (Mise en place de l'autorité intermédiaire) *Détaillez les commandes que vous utilisez.*

Nous utiliserons la commande `ca` d'openssl. Vous devez créer une arborescence contenant :
— le certificat de l'autorité,
— la clef privée de l'autorité,
— un fichier `index.txt` vide,
— un fichier `serial` contenant la valeur `01`
— un répertoire `certs` vide.

Exercice 4 (Demande de signature pour un certificat utilisateur/serveur) Modifiez le fichier de configuration `openssl.cnf` en fonction du type de certificat que vous souhaitez produire. C'est-à-dire, ajouter des extensions (dans la section `# Extensions for a typical CA`) pour chaque utilisations types. Les paramètres important sont

1. Commentez les usages.

```
keyUsage =
extendedKeyUsage =
```

Générez avec votre autorité intermédiaire des certificats pour les utilisations citées au début du sujet. Précisez les configurations utilisées.

Exercice 5 (Enveloppe PKCS#12 d'un certificat) Une *enveloppe PKCS#12* (Personal Information Exchange Syntax Standard) est une norme de fichier contenant votre certificat, votre clef privée, le certificat de l'autorité ayant signé votre certificat, etc.

Réalisez une enveloppe pour votre certificat client SSL. Si vous avez configuré votre mail sous thunderbird, vous pouvez facilement envoyer des mails signés en S/MIME.

Exercice 6 (Listes de révocation CRL) Créez un nouveau certificat utilisateur. Révoquez-le. Expliquez précisément ce que fait l'option `revoke` de la commande `openssl ca`. Commentez. Générez une liste de révocation contenant ce certificat révoqué.