Certificats

Généralites

Un certificat électronique est une carte d'identité numérique dont l'objet est d'identifier une entité physique ou non-physique. Le certificat numérique ou électronique est un lien entre l'entité physique et l'entité numérique (Virtuel). L'autorité de certification fait foi de tiers de confiance et atteste du lien entre l'identité physique et l'entité numérique. Le standard le plus utilisé pour la création des certificats numérique est le X.509.

Méthode de création de certificats signés

- Apache : https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&actp=CROSSLINK&id=AR198
- Tomcat : https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&actp=CROSSLINK&id=AR227
- Red Hat ApacheSSL Server : https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&actp=CROSSLINK&id=AR142

Documentation

- Certificat électronique : http://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique
- Infrastructure à clés publiques : http://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publiques
- Génération d'une clé : http://www.linux-kheops.com/doc/redhat73/rhl-cg-fr-7.3/s1-installation-generatingkey.html
- Création d'un certificat : http://www.linux-kheops.com/doc/redhat73/rhl-cg-fr-7.3/s1-installation-selfsigned.html
- Types de certificats : http://www.linux-kheops.com/doc/redhat73/rhl-cg-fr-7.3/s1-installation-certs.html
- Ressources : http://www.linux-kheops.com/doc/redhat73/rhl-cg-fr-7.3/apache-secure-server-additional-resources.html

Apache

Il faut avoir une installation propre d'Apache. Les fichiers dont nous allons parler par la suite sont déjà présent mais ne sont que des exemples. Pour gérer les certificats, il faut au préalable installer openssl. Il est présent sur le DVD Red Hat. Le cocher à l'installation ou l'installer après en montant le DVD. L'autre méthode est de se rendre sur l'excellent site dag-wieers qui regroupe les paquetages

des différentes versions Red Hat : http://dag.wieers.com/rpm/packages.php

Récupérer le rpm d'openssl en fonction de l'architecture du système et la version de la Red Hat.

```
wget http://dag.wieers.com/rpm/packages/openssl/openssl-….el4.rf.i386.rpm
```

L'installer avec la commande suivante :

```
rpm -ivh openssl……el4.rpm
```

Je n'ai pas eu de dépendances à installer avec une installation de base de RHEL4.6. Si il y en a les obtenir sur le même site et les installer avec la même commande avant d'installer le paquetage que l'on désire.

Configuration

Configuration général

Emplacement	Fonction
/etc/httpd/conf/*	Dossier qui contient les clés et certificats ainsi que les outils pour les générer.
/etc/httpd/conf/ssl.key/*	Dossier qui contient la clé publique.
/etc/httpd/conf/ssl.crt/*	Dossier qui contient le certificat.
/etc/httpd/conf/Makefile	Fichier qui sert notamment à la génération des certificats.

Configuration spécifique

Pour créer un certificat auto-signé, il faut tout d'abord générer une clé, ensuite générer le certificat et redémarrer le service Apache pour qu'il prenne les modifications en compte.

Remarque : Ici est détaillé la création d'un certificat auto-signé sans pass phrase. La pass phrase est demandée à chaque fois qu'on redémarre le serveur Web. Pour plus de sécurité, il faudrait l'utiliser. Cependant, la génération de certificat est utilisé pour les serveurs Web des pages d'administrations. Pour les services Web important nous faisons appel à des autorités certifiées. Pour les interfaces d'administrations, une pass phrase est donc un peu disproportionné. Nous n'en mettrons pas.

Les deux fichiers que nous voulons générer sont appelés par les deux mots clés suivant du fichier de configuration apache ou des virtuals hosts.

```
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
```

Se positionner dans le dossier `/etc/httpd/conf/` qui contient les clés.

```
cd /etc/httpd/conf
```

Tout se déroule en étant dans ce dossier. Ceci est important car un fichier Makefile est lus lorsque nous lançons la commande make.

Sauvegarder les fichiers suivants.

```
cp ssl.key/server.key /root
cp ssl.crt/server.crt /root
```

Les supprimer.

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

Générer la clé.

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

La clé est créée dans le dossier `/etc/httpd/conf/ssl.key/server.key`

Positionner les bons droits :

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

Pour générer le certificat, nous utilisons la commande make avec un paramètre. Cette commande s'appuie sur le fichier Makefile lié symboliquement dans le dossier `/etc/httpd/conf`. Modifier ce fichier pour que lors de l'appel de testcert qui sert à créer le certificat, nous ayons un certificat d'une durée de validité de 10 ans au lieu d'1 ans par défaut.

Lors de l'appel à `make testcert`, un appel est fait à la fonction CRT. C'est celle-ci que nous allons modifier au niveau du nombre de jours. Pour cela, modifier la valeur -days à 3650 jours (10 ans).

```
testcert: $(CRT)

$(CRT): $(KEY)
        umask 77 ; \
        /usr/bin/openssl req -new -key $(KEY) -x509 -days 3650 -out $(CRT)
```

Toujours positionné dans le dossier de départ (`/etc/httpd/conf/`), taper la commande de génération du certificat.

```
make testcert
```

Des informations nous sont demandées. Pour rester en phase, entrer des valeurs cohérentes en changeant le nom du serveur.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

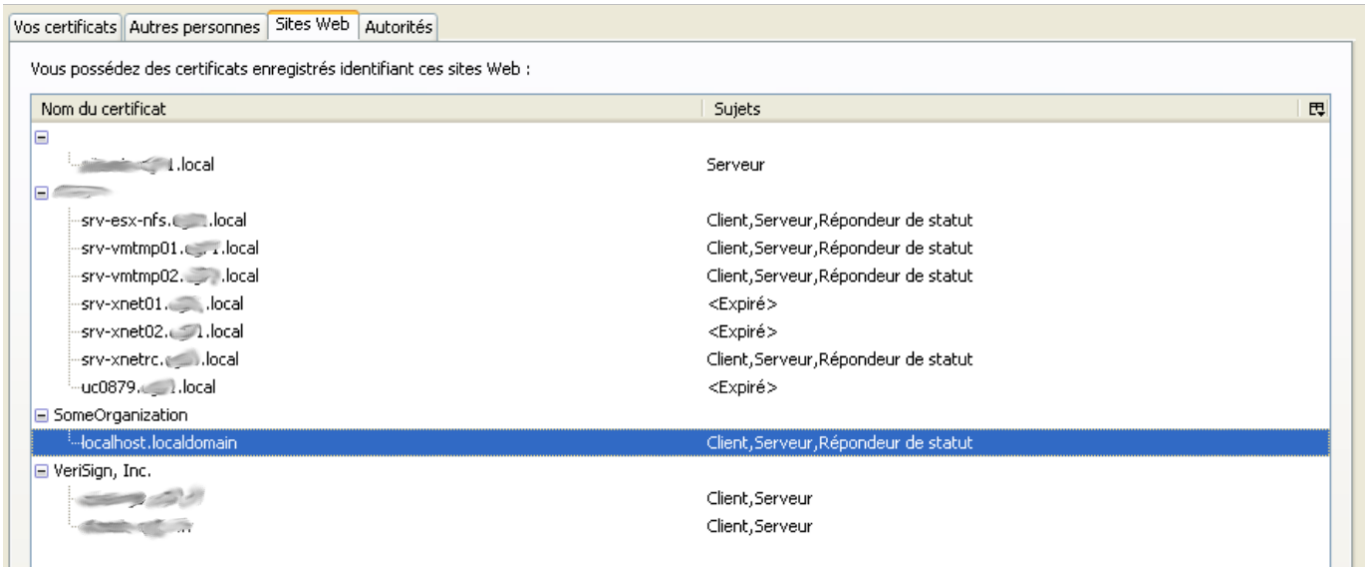
```
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:SAONE ET LOIRE
Locality Name (eg, city) []:MACON
Organization Name (eg, company) [Internet Widgits]:SOCIETE
Organizational Unit Name (eg, section) []:SERVICE RH
Common Name (your name or server's hostname) []:SERVEUR.DOMAINE.COM
Email Address []:RH@SOCIETE.COM
```

Le certificat est généré dans le dossier `/etc/httpd/conf/ssl.crt/server.crt`.

Redémarrer le serveur Web avec un `service httpd restart`.

L'interface d'administration ou le site web en question doit maintenant être auto-signée.

Avant la configuration du certificat.



Après le certificat auto-signé.