openssl

- Objet : découvrir le ssl
- Niveau requis :
  débutant, avisé
- Commentaires : notes perso

Qu'est-ce que ssl ?

ssl : Secure Socket Layer

C'est un protocole réseau à mis chemin entre un protocole réseau orienté connexion (TCP/IP) et un protocole de la couche applicative (HTTP).

Il permet la sécurisation des communications entre un serveur et un client, au moyen :

1. d'une authentification mutuelle ;
2. d'une vérification de l'intégrité des communication par signature digitale
3. par un chiffrement par clés asymétriques afin que la communication soit privée

Le port par défaut est 443 :
Dans apache il faut ajouter une directive `Listen 443` dans le fichier de configuration d'apache /etc/sites-availables/default-ssl.

l'utilitaire OpenSSL

Lors de l'installation du module ssl (installer par défaut avec l'installation d'apache2 sur debian), il s'est installé aussi l'utilitaire OpenSSL.

C'est l'utilitaire qui permet de mettre en place les certificats.

- Le dossier de configuration de OpenSSL est /etc/ssl/ :

Il contient deux dossiers et un fichier : → **/etc/ssl/openssl.cnf** Fichier de configuration de opensl. On y met les directives. On peut y mettre son /home, l'autorité de certification ... → le dossier **/etc/ssl/cert/** : il contient nos certificats

- le dossier **/etc/ssl/private/** : il contient nos clés privées

Créer un certificat

- On génère une clé privée :

```
openssl genrsa 1024 > mon_fichier_pour_ma_clé
```

- On crée un fichier de certification :

```
openssl req -new -key nom_du_fichier
```

Après on envoie ce fichier de certification au CA qui le signe, c'est-à-dire qui donne un fichier de certificat signé.

- les ranger dans apache2:

> Le certificat envoyé au CA et celui qu'il nous a fourni signé dans `/etc/ssl/certs/certificat.com`

> La clé privée dans `/etc/ssl/private/sa_clé.key` [1)]

Créer un certificat auto-signé

Par exemple :

```
openssl req -x509 -nodes -days 365 -newkey rsa:1024\
-out /etc/ssl/certs/nom-du-site.com \
-keyout /etc/ssl/private/nom-du-site.com.key
```

> -x509 -nodes : type de certificat
> -days 365 : durée de vie du certificat (en jours)
> - newkey rsa:1024 : clé rsa de 1024 bits
> -out /chemin/fichier/du_certificat : crée le fichier du certificat
> -keyout /etc/apache2/server.key : chemin du fichier de sa clé privée

→ Cela crée un fichier /etc/ssl/certs/nom-du-site.com et un fichier /etc/ssl/private/nom-du-site.com.key dont on se sert pour configurer apache2.

Pour un certificat auto-signé, il faut répondre à la question “Common Name” le nom du domaine à protéger

- Donner les droits :

```
chmod 400 /ssl/private/nom-du-site.com.key
```

1)
avec sur cette clé les droits posix 400