Apache et ssl

SSL est un sigle :

> **Secure Sockets Layer**, un protocole de sécurisation des échanges sur Internet, devenu Transport Layer Security (TLS) en 2001 ;
> Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS.

Ajouter le module ssl

```
a2enmod ssl
/etc/init.d/apache2 force-reload
On peut créer son certificat SSL auto signé en installant le paquet openssl.
```

créer son certificat SSL

Pré-requis

Le paquet `openssl` doit être installé par la commande :

```
sudo apt-get install openssl
```

openssl req -x509 -nodes -days 365 -newkey rsa:1024 -out **/etc/apache2/server.crt** -keyout **/etc/apache2/server.key**

Explications :

- **-x509 -nodes** donne le type de certificat voulu
- **-days 365** indique la durée de validité (en jours) de votre certificat
- **-newkey rsa:1024** demande une clé RSA de 1024 bits - d'après la doc apache, il est déconseillé de créer une clé plus grosse pour des histoires de compatibilité
- **-out /etc/apache2/server.crt** est le chemin de votre certificat
- **-keyout /etc/apache2/server.key** est le chemin de la clé privée

Répondez alors aux questions posées :

```
Country Name (2 letter code) [GB]:
```

Entrez **BE** si vous êtes situé en belgik et validez par la touche « Entrée »

```
State or Province Name (full name) [Some-State]:
```

X.509 est une norme de cryptographie

Dans le système X.509, une autorité de certification attribue un certificat liant une clé publique à un nom distinctif (Distinguished Name), à une adresse électronique ou un enregistrement DNS.

Les certificats racines sont des clés publiques non signées, ou auto-signées, dans lesquels repose la confiance. Des autorités de certification commerciales détiennent des certificats racines présents dans de nombreux logiciels, par exemple les navigateurs Web. Quand le navigateur ouvre une connexion sécurisée (SSL) vers un site ayant acheté une certification auprès d'une autorité connue, il considère le site comme sûr dans la mesure où le chemin de certification est validé. Le passage en mode sécurisé est alors transparent.

Entrez **BELGIQUE** et validez par la touche « Entrée »

```
Locality Name (eg, city) []:
```

Indiquez ici le nom de votre ville. (*exemple :* **LIEGE**) et validez par la touche « Entrée »

```
Organization Name (eg, company; recommended) []:
```

Indiquez le nom de votre organisation, de votre société. (*exemple :IPEPS***-hosting**) et validez par la touche « Entrée ». Si vous n'avez pas de société, vous pouvez mettre un nom fictif, le nom de notre site Web par exemple.

```
Organizational Unit Name (eg, section) []:
```

Indiquez ici le nom de la section de votre organisation, de votre société. Si vous n'en avez pas, mettez la même chose que pour la question précédente.

```
Common Name (eg, YOUR name) []:
```

Ici, il convient de faire particulièrement attention à ce que vous allez entrer. Vous devez indiquer le *nom de domaine* que vous désirez sécuriser. En ce qui nous concerne, il s'agit du domaine : IPEPS**.com**. Nous indiquons donc **IPEPS.COM** et nous validons par la touche « Entrée ».

```
Email Address []:
```

Ici, il s'agit d'indiquer l'adresse E-mail de l'administrateur. En ce qui nous concerne, il s'agit de : admin@IPEPS.com. Nous terminons bien entendu en validant par la touche « Entrée ».

```
Generating a 1024 bit RSA private key
.....................................++++++
.++++++
writing new private key to '/etc/apache2/server.key'
-----
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]:BE
State or Province Name (full name) [Some-State]:Liege
Locality Name (eg, city) []:Liege
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IPEPS
Organizational Unit Name (eg, section) []:WEBMASTER
Common Name (eg, YOUR name) []:ETUDIANT
Email Address []:
```

Enfin, on empêche les curieux de lire notre clé privée :

```
chmod 440 /etc/apache2/server.key
```

Ajout de la directive Listen 443

Par défaut, Apache2 est configuré pour écouter sur le port **80**. Il s'agit là de la configuration usuelle d'un Serveur Web. Cependant, le protocole SSL a besoin d'un port spécifique pour pouvoir fonctionner. Il s'agit du **port 443**.

Nous allons donc rajouter une directive de configuration nommée **Listen** qui permettra d'indiquer à Apache2 qu'il doit aussi écouter sur le port 443.

Editez **/etc/apache2/ports.conf** et rajoutez la ligne suivante :

```
Listen 443
```

Création du fichier de configuration

Ayant déjà configuré notre hôte virtuel, un fichier de configuration doit exister dans le répertoire **/etc/apache2/sites-available**.

Pour sécuriser cet Hôte Virtuel, nous allons donc devoir modifier ce fichier en y ajoutant un hôte virtuel accessible sur le **port 443**, ce dernier contenant des directives particulières qui sont les suivantes :

1. Directive **SSLEngine** :
   Cette directive permet d'activer le moteur SSL au sein d'un hôte virtuel, Elle peut prendre deux arguments –> **on/off**
2. Directive **SSLCertificateFile** :
   Cette directive définit le certificat authentifiant le Serveur auprès des clients. L'argument est le chemin d'accès au certificat. En ce qui nous concerne, le certificat se trouve dans le répertoire **/etc/apache2/**
3. Directive **SSLCertificateKeyFile** :
   Cette directive définit la clé privée du Serveur utilisée pour signerl'échange de clé entre le client et le serveur. Elle prend en argument le chemin d'accès à la clé (fichier). Dans notre cas, la clé se trouve dans le répertoire **/etc/apache2/**.
4. Par ailleurs, comme nous l'avons déjà fait pour notre hôte virtuel accessible sur le **port 80**, nous allons devoir rajouter une directive **NameVirtualHost** qui permettra que l'adresse nommée par le nom de notre hôte virtuel accessible sur le **port 443** soit résolue correctement. Nous rajouterons donc cette directive (*NameVirtualHost *:443*) au début de notre fichier de configuration.
5. Un répertoire particulier de public_html n'est accessible que par https L'acces par le port 80 est donc interdit

Mon fichier:

```
#NameVirtualHost *
<VirtualHost *:80>
      ServerAdmin webmaster@localhost
      DocumentRoot /var/www/
      <Directory />
            Options FollowSymLinks
            AllowOverride None
      </Directory>
      <Directory /var/www/>
```

```
            Options Indexes FollowSymLinks MultiViews
            AllowOverride None
            Order allow,deny
            allow from all
            # This directive allows us to have apache2's default start page
                # in /apache2-default/, but still have / go to the right place
                RedirectMatch ^/$ /apache2-default/
      </Directory>

      <Directory   "/home/*/public_html/securite">
      AllowOverride None
        Order deny,allow
        Deny from all
      </Directory>
</VirtualHost>

//éventuellement dans un autre fichier...(default-ssl )
Dans ce cas, on l'ajoute aux sites utilisables (liens)
```

```
a2ensite
Your choices are: default default-ssl
Which site(s) do you want to enable (wildcards ok)?
default-ssl
Enabling site default-ssl.
Run '/etc/init.d/apache2 reload' to activate new
configuration!
```

```
<VirtualHost *:443>

       DocumentRoot /home/etudiant/public_html/securite

 <Directory   "/home/*/public_html/securite">
AllowOverride all
        Order deny,allow
        Allow from all

</Directory>

        SSLEngine on
        SSLCertificateFile /etc/apache2/server.crt
        SSLCertificateKeyFile /etc/apache2/server.key
</VirtualHost>
```

Exemple d'utilisation :

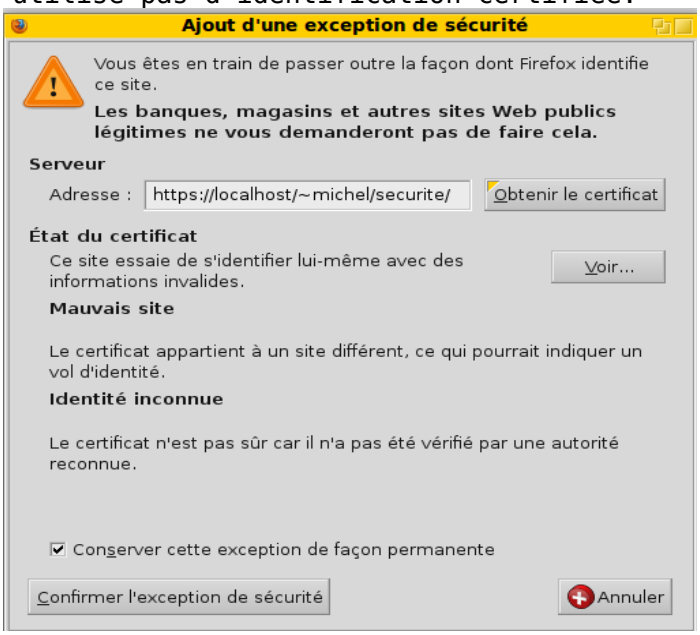
```
https://localhost/~etudiant/securite/
```

localhost utilise un certificat de sécurité invalide.

Le certificat n'est pas sûr car il est auto-signé.
Le certificat n'est valide que pour ETUDIANT.

(Code d'erreur : sec_error_untrusted_issuer)
Si vous comprenez ce qui se passe, vous pouvez indiquer à Firefox de commencer à faire confiance à l'identification de ce site. Même si vous avez confiance en ce site, cette erreur pourrait signifier que quelqu'un est en train de pirater votre connexion.

N'ajoutez pas d'exception à moins que **vous ne connaissiez une bonne raison** pour laquelle ce site n'utilise pas d'identification certifiée.



Détails :

On décoche éventuellement pour ne pas garder le certificat dans le future et On clique sur confirmer.