```
à tester valider vérifier
```

Introduction

La plus grande partie des commandes ci-dessous demandent à avoir les droits de super administrateur. Comme vous risquez de détruire la configuration de votre serveur web (et donc d'une grande partie d'AbulÉdu) seuls les administrateurs chevronnés devraient s'y essayer.

Création d'un certificat auto-signé

C'est le plus simple (et surtout gratuit).

Création

- Créez un fichier Makefile dont le contenu est le suivant:

```
all: serveur key sign

serveur:
	openssl genrsa -out ca.key 2048
	openssl req -new -key ca.key -out ca.csr -config confca
	openssl x509 -req -in ca.csr -out ca.cert -days 10000 -signkey
ca.key

key:
	openssl genrsa -out ser.key
	openssl req -new -key ser.key -out ser.csr -config confkey

sign:
	openssl x509 -days 10000 -req -in ser.csr -out ser.crt -CA ca.cert -
CAkey ca.key -CAserial ca.srl -CAcreateserial

clean:
	rm -f ca* ser* *~
```

- Créez un fichier confca dont le contenu est le suivant:

```
[ req ]
default_bits           = 2048
distinguished_name     = req_distinguished_name
prompt                 = no

[ req_distinguished_name ]
C                      = FR
ST                     = Aquitaine
```

```
L                       = Villenave d'Ornon
O                       = RyXeo SARL
OU                      = RyXeo Certificates VO
CN                      = secure.ryxeo.com
emailAddress            = secure@ryxeo.com
```

Le fichier confca permet de créer votre autorité de certification. En bref vous allez agir comme si vous étiez cacert.org verisign ou autre autorité de certification.

Le certificat serveur que vous allez ensuite signer avec ce certificat “ca” sera donc ce qu'on appelle un certificat auto-signé et provoquera un petit message d'alerte sur le navigateur web de vos utilisateurs.

- Créez un fichier confkey dont le contenu est le suivant:

```
[ req ]
default_bits            = 2048
distinguished_name      = req_distinguished_name
prompt                  = no

[ req_distinguished_name ]
C                       = FR
ST                      = Bretagne
L                       = Rennes
O                       = Entreprise
OU                      = Votre Entreprise
CN                      = xxxxx.dyn.abuledu.net
emailAddress            = xxxxx@abuledu.org
```

Remplacez les champs par les informations concernant votre serveur web. Le nom xxxxx.dyn.abuledu.net est très important, c'est celui que vous utiliserez ensuite dans la configuration d'apache.

Génération du certificat

Placez-vous dans le répertoire où vous avez créé les fichiers précédents et lancez la commande “make” tout simplement.

```
root@servecole /etc/apache2/ssl ☠ ls
confca  confkey  Makefile
root@servecole /etc/apache2/ssl ☠ make
[plein d'infos]
root@servecole /etc/apache2/ssl ☠ ls
ca.cert  ca.csr  ca.key  ca.srl  confca  confkey  Makefile  ser.crt  ser.csr
ser.key
```

Vous pouvez-voir qu'après avoir lancé la commande make nous avons maintenant plein de fichiers en plus dans le répretoire. Les fichiers qui nous intéressent sont les suivants: ser.crt et ser.key.

Configuration d'apache

Maintenant que vous avez votre certificat SSL il faut l'utiliser dans apache, pour celà vous pouvez créer un fichier (par exemple abuledu_https) dans /etc/apache2/site-available dont le contenu sera le suivant:

```
Listen 443

<VirtualHost xxxxx.dyn.abuledu.net:443>
    DocumentRoot /var/www/intranet
    ServerName xxxxx.dyn.abuledu.net
    ErrorLog /var/log/apache2/error.log
    LogLevel warn
    CustomLog /var/log/apache2/access.log combined
    ServerSignature On

  <IfModule mod_ssl.c>
    SSLEngine on
    SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+SSLv2:+EXP:+eNULL
    SSLCertificateFile    /etc/apache2/ssl/ser.crt
    SSLCertificateKeyFile /etc/apache2/ssl/ser.key
    <Files ~ "\.(cgi|shtml)$">
      SSLOptions +StdEnvVars
    </Files>
    <Directory "/usr/lib/cgi-bin">
      SSLOptions +StdEnvVars
    </Directory>
    SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
  </IfModule>

</VirtualHost>
```

Ensuite, activez ce nouveau fichier de configuration à l'aide de la commande suivante

```
a2ensite abuledu_https
```

Et enfin, relancez apache avec

```
/etc/init.d/apache2 restart
```

Utilisation d'un certificat signé par un tiers de confiance

Détailler le principe. Je vous conseille d'aller voir http://www.cacert.org