Créer sa propre Autorité de Certification (AC) ou CA en anglais

Bien le bonjournasse ami lutingue, aujourd'hui on va faire un gros HOWTO (bouuuuh le vilain, un HOWTO, y'a papa Théo qui va encore sévir en voyant ça) pour créer sa propre autorité de certification, afin de se faire ses propres certificats tous beaux.

Cette CA, dont vous difuuserez sur toutes vos machines et à tous vos amis qui ont des comptes mail-ssl ou https chez vous, vous permettra de créer une hiérarchie de confiance afin de créer un certificat par service par machine. Je ne sais pas si je suis très clair, mais bon on va dire que oui.

Ce tip présuppose que les notions de biclef qui vont de pair avec le chiffrement asymétrique sont connues.

Toutes ces manipulations supposent que vous êtes r00t.

Génération de notre propre Autorité de Certification

On se crée un joli endroit dans /etc/ssl pour stocker la biclef.

```
export HOSTNAME=`hostname`
cd /etc/ssl
mkdir CA
cd CA
```

Génération de la clé

On génère la clef privée de notre CA.

```
openssl genrsa -des3 -out ${HOSTNAME}-ca.key 2048
```

On va vous demander un mot de passe. Il est évident que ce mot de passe doit être d'une solidité à tout épreuve, car si vous divulguez ou que vous vous faites voler votre clef privée de votre certificat racine, vous foutez toute la sécurité en l'air.

Seul r00t a le droit de la lire.

```
chmod 400 ${HOSTNAME}-ca.key
```

Génération du certificat

On génère un certificat auto-signé.

```
openssl req -new -x509 -days 3650 -key ${HOSTNAME}-ca.key -out ${HOSTNAME}-ca.crt
```

On peut rentrer comme paramètres ce qui suit.

```
Unite d'organisation OU = Secure Server Certification Authority
Organisation O = Pinpin Data Security, Inc.
Pays C = FR
Nom commun CN = <rien> ou ce qui est dans le champ "O"
```

Pour voir le certificat, on peut utiliser la commande suivante

```
openssl x509 -in ${HOSTNAME}-ca.crt -text -noout
```

Créer une clé et un certificat pour un serveur quelconque (Web, SMTP, POP etc)

Par exemple, si c'est pour un serveur web, vous pouvez procéder comme suit :

```
export SERVICE="www"
cd /etc/ssl
mkdir ${SERVICE}
cd ${SERVICE}
```

Génération de la clef privee

```
openssl genrsa -des3 -out ${HOSTNAME}-${SERVICE}.key 1024
chmod 400 ${HOSTNAME}-${SERVICE}.key
```

Génération du certificat à faire signer par l'AC

```
openssl req -new -key ${HOSTNAME}-${SERVICE}.key -out ${HOSTNAME}-${SERVICE}.csr
```

Il est ***EXCESSIVEMENT*** important que vous indiquiez bien le Fully Qualified Domain Name de votre machine. Bien entendu, on suppose que vous n'avez qu'une seule IP sur votre machine, et qu'on est encore qu'en IPv4...

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

Méthode alternative

On peut, à la place des deux étapes du dessus (pour ne pas avoir de passphrase), effectuer la passe suivante.

```
openssl req -new -nodes -out ${HOSTNAME}-${SERVICE}.pem -keyout ${HOSTNAME}-${SERVICE}.key
```

Signature de la demande par le CA

```
openssl x509 -req -in ${HOSTNAME}-${SERVICE}.csr -out ${HOSTNAME}-${SERVICE}.crt -sha1 -CA /etc/
```

ou, si vous avez suivi la méthode alternative du dessus

```
openssl x509 -req -in ${HOSTNAME}-${SERVICE}.pem -out ${HOSTNAME}-${SERVICE}.crt -sha1 -CA /etc/
/etc/ssl/CA/${HOSTNAME}-ca.key -CAcreateserial -days 3650 && rm ${HOSTNAME}-${SERVICE}.pem
```

ATTENTION: ce certificat et cette clé seront valides pour uniquement pour un serveur ayant le nom FQDN spécifié. Il faudra générer autant de couple clé/certificat que le serveur hébergera de Virtual Host (en supposant que vous ayiez plusieurs IP sur la babasse)

Bonus, la conf Apache

```
SSLCertificateFile /etc/ssl/www/${HOSTNAME}-www.crt
SSLCertificateKeyFile /etc/ssl/www/${HOSTNAME}-www.key
```

```
SSLCertificateChainFile /etc/ssl/CA/${HOSTNAME}-ca.crt
SSLCACertificateFile /etc/ssl/CA/${HOSTNAME}-ca.crt
```

ChangeLog
10 mai 2007: créée – *mat*

TODO: certificats p12 et certificats de révocation.