Création d'un certificat autosigné

1 Introduction

Objectifs. Pour les travaux pratiques suivants, nous avons besoin de créer un certificat autosigné afin d'utiliser SSL/TLS pour sécuriser les futurs échanges entre les clients et le serveurs.

2 Sur votre serveur SRV

1. Commençons par fixer les paramètres de notre certificat :

Les paramètres

```
## C'est le domaine DNS que nous utilisons
DOMAIN="idl.xfr"
## C'est le nom du serveur que nous utilisons
SERVER="srv.$DOMAIN"

## Cela doit fonctionner
ping -c 2 $SERVER
```

2. Ajoutons à la configuration `openssl` notre domaine et notre serveur :

```
cat <<FIN >>/etc/ssl/openssl.cnf

[ $DOMAIN ]
subjectAltName = DNS:$SERVER,IP:192.168.0.10

FIN
```

3. Construisons notre clé privée avec `openssl genrsa` :

```
## Génération de la clé privée (donnez un mot de passe simple)

cd /etc/pki/tls/certs
openssl genrsa -aes128 2048 > server.key
```

4. Décryptons notre clé privée avec `openssl rsa` :

```
## donnez le mot de passe choisi
openssl rsa -in server.key -out server.key
```

5. Construisons la requête avec `openssl req` :

```
## pour construire
openssl req -utf8 -new -key server.key \
  -out server.csr \
  -subj "/C=FR/ST=PACA/L=MARSEILLE/O=AMU/OU=IDL/CN=$SERVER"

## pour vérifier
openssl req -text -verify -in ./server.csr
```

6. Finalement, construisons le certificat avec `openssl x509` :

```
# pour générer
openssl x509 -in server.csr -out server.crt \
    -req -signkey server.key \
    -extfile /etc/ssl/openssl.cnf -extensions $DOMAIN -days 3650

# pour vérifier
openssl x509 -text -in ./server.crt

# pour protéger
chmod 600 server.key

# pour lister
ls -l server.*
```

7. Des informations plus détaillées sont disponibles sur ce tutoriel.