Przewodnik administratora > Tworzenie certyfikatu podpisanego przez własnego CA

Opisany sposób będzie bez zmian ścieżek działał na Linux Debian.

Przechodzimy do katalogu zawierającym plik CA.pl i wykonujemy skrypt z parametrem -newca Tą opcją generujemy nowy urząd certyfikacji. Podajemy kolejno dane - jako Common Name może być BetaSoft CA.

```
#cd /usr/lib/ssl
#./CA.pl -newca
```

Generujemy żądanie (request) certyfikatu serwera - również odpowiadając na pytania - tym razem jako CommonName podajemy adres serwera jakim będą się posługiwać użytkownicy np. dev.bnet.pl, 192.168.1.10 itp.

```
openssl genrsa -out x.key 2048
openssl req -new -key x.key -out request.pem
```

Podpisujemy nasze żądanie, wcześniej aby spełnić wymogi nazewnicze defaultowej konfiguracji zmieniamy nazwy:

```
mv request.pem newreq.pem
mv x.key newkey.pem
./CA.pl -sign
```

Kopiujemy pliki certyfikatów do katalogu Apache

```
cp newcert.pem /etc/apache2/ssl/
cp newkey.pem /etc/apache2/ssl/
cp demoCA/cacert.pem /etc/apache2/ssl/
```

Modyfikujemy plik zawierający konfigurację SSL czyli /etc/apache2/sites-enabled/default-ssl

```
SSLCertificateFile /etc/apache2/ssl/newcert.pem
SSLCertificateKeyFile /etc/apache2/ssl/newkey.pem
SSLCertificateChainFile /etc/apache2/ssl/cacert.pem
```

Restartujemy Apache

```
/etc/init.d/apache2 reload
```

Eksportowanie certyfikatu oraz CA do formatu pfx: openssl pkcs12 -export -out certificate.pfx -inkey privateKey.pem -in certificate.pem -certfile cacert.pem

Gotowe! Nowy certyfikat serwera powinien mieć poprawną ścieżkę certyfikacji, dzięki czemu główny certyfikat można zainstalować w głównych zaufanych urzędach certyfikacji.