

Procedura pozyskania i instalacji certyfikatów SSL dla serwera Apache

1. Generowanie pary kluczy oraz wniosku o certyfikat CSR.

Aby wygenerować parę kluczy oraz wniosek o certyfikat należy w trybie terminalowym wykonać następującą polecenie:

```
$openssl req -new -nodes -config CCS-SSL.conf > server.csr
```

CCS-SSL.conf jest to plik konfiguracyjny o następującej zawartości:

```
.....
HOME                = .
RANDFILE            = $ENV::HOME/.rnd

[ req ]
default_bits        = 1024
default_keyfile     = server.key
distinguished_name  = req_dn

[ req_dn ]
commonName          = Nazwa podmiotu (nazwa serwera)
commonName_default  = www.moja_firma.com

emailAddress        = Adres Email
emailAddress_default = postmaster@moja_firma.com
.....
```

pozostałe dane do certyfikatu zostaną pobrane z polityki certyfikatu serwerów WWW.

Powyższe polecenie utworzy nam w katalogu bieżącym dwa pliki: server.csr, oraz server.key. Pierwszy z nich jest wnioskiem o certyfikat (CSR) w formacie PKCS#10 będzie on potrzebny w procesie pozyskiwania certyfikatu. Natomiast drugi jest kluczem prywatnym twojego serwera WWW i należy go specjalnie chronić przez dostępem osób niepowołanych.

Pliki o których mowa mają postać zbliżoną do następującej:

server.csr:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBcDCB2gIBADAxMRMwEQYDVQQDEwphc2QuYXNkLnBsMR0wGAYJKoZIhvcNAQkB
Fgthc2RACXdkZS5wbDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA9TVAtPy1
U3/YeIKpbk+ysORYuDvYiKlWmg9YaCBjxGqzzrocAQeV702fNwvfMunDPNIIG6n7
mS5401aBdmQLh1AQFP8boR5jVpZFZJq7v34Jng2FnA7XxfKlfr7D/u/rE5amHgYn
arhVd5WFloGQl+IhdEHf02pv+zfekfU+Do8CAwEAAaAAMA0GCSqGSIb3DQEBAUA
A4GBACwOy7R43F4000E6WByOUK+shtuDrDKnHQszZlEKlrecdax0coRKxUDK5tTj
WTW3qrtTpN0/ipca3nXxjPlIvp4xuhnZMjJ5esOdAf4I56ZCG3dFmI1vG8DXsDhA
adds5yZyBPgovrqrXaqnl1HPDWXy7iM8LSRpHXkeMCZ0qkKz
-----END CERTIFICATE REQUEST-----
```

server.key:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQD1NUC0/LVTf9h4gqluT7Kw5HK409iIqVaaDlhoIGPEarPOuhwB
B5XvTZ83C98y6cM80iUbqfuZLNg7VoF2ZAuHUBAU/xuhHmNWlkVkmru/fgmeDYWc
DtFf8qV+vsP+7+sTlqYeBidquFV3lYWWgZCX4iF0Qd87am/7N96R9T40jwIDAQAB
AoGAPB9bh0TzHM8a/6lh67dE5BSPgFbEJ/YFUu7ySU2vyKg1ADonxaTbgXpx0Ghr
yKsCgPYxvQ+3rf5z4nC6e5HaNU9vOrv1cZeB7kDAUusAQD1H9KXIBvcp6cRzIk9I
TWwGYJrG+s9zjgg6SJXZA50Z1lUg9xSkdQrssiWPhg7FzskCQQD91IeY2RZ2+a42
65Cb1vwy2hiX+B1Pvw+fRrnukM+7u/JG7knCZNGyttSP6xyZKnaiFUjxRmsRRy3D
D7k4A50zAkEA903azn7dWqW9C1kl+RN0I3c+wqIxjrsmGacWNY+e2Fv7jUBZ25BL
gPRp9DJn1wK+WWfJaEc4AdQDwQc1rXlxNQJAAQDNBKGfPxsfgCIQMT15Q64u+LLH
TtrfeG6sH3A9Ee3dOECK1BTX60/jqSnxs/1B+MQCxM1vdP0GBkZSoHEJlwJAGYvv
WHL+gEiyuIjxBUPfMXK2BwEeQXJPwxeoUdcXf54w5CyLm8TSJ+YXs+QpGersouu3
wI/qlzWB1cUa5GqxKQJAcwz1lOiebtq60CYTc2gf6QEKa9lEusjYAqPvdUK1rL3r
QIMDZtYAEF46HFSLA0pX2DqT+qskiW0Yj8sMBkevXQ==
-----END RSA PRIVATE KEY-----
```

Posiadając już wniosek CSR należy upewnić się czy został on wygenerowany we właściwy sposób oraz czy zawiera zadowalające dane. Można dokonać tego korzystając z oprogramowania OpenSSL wydając następujące polecenie:

```
$openssl asn1parse < server.csr
```

lub

```
$openssl req -in server.csr -text -noout
```

Po dokładnym sprawdzeniu poprawności wniosku o certyfikat klucz prywatny należy zabezpieczyć przed utratą kopiując go na bezpieczny nośnik.

2. Instalacja certyfikatu.

Na podstawie wniosku o certyfikat przesłanego do Centrum Certyfikacji Signet zostaje utworzony certyfikat SSL serwera WWW, który klient może pobrać i zainstalować na swoim serwerze WWW.

Typowa instalacja certyfikatu na serwerze Apache posadowionym w środowisku UNIX może wyglądać następująco:

Należy zalogować się jako użytkownik root

```
$cd APACHE_DIR/ssl.key
$cp KEY_DIR/server.key .
$chmod 400 server.key
$chown root:root
$chattr +i server.key
```

```
$cd APACHE_DIR/ssl.crt
$cp CERT_DIR/server.crt .
$make
```

gdzie:

APACHE_DIR jest katalogiem w którym zainstalowany jest serwer apache;
CERT_DIR jest katalogiem do którego został pobrany plik certyfikatu;
KEY_DIR jest katalogiem w którym został utworzony klucz prywatny;

3. Konfiguracja serwera WWW.

Konfiguracja serwera Apache polega na przeedytowaniu pliku konfiguracyjnego serwera httpd.conf.

Poniżej przedstawiony jest fragment tegoż pliku niezbędny do uruchomienia serwera www w otoczeniu SSL:

```
<IfModule mod_ssl.c>
SSLPassPhraseDialog builtin
SSLSessionCache dbm:/apache/logs/ssl_scache
SSLSessionCacheTimeout 300
SSLMutex file:/apache/logs/ssl_mutex
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
SSLLog /apache/logs/ssl_engine_log
SSLLogLevel info
</IfModule>

<VirtualHost www.moja-firma.pl:443>
ServerName www.moja-firma.pl
ServerAdmin postmaster@moja-firma.pl
DocumentRoot /apache/htdocs
SSLEnable
SSLEngine on

SSLCertificateFile /apache/conf/ssl.crt/server.crt
SSLCertificateKeyFile /apache/conf/ssl.key/server.key

</VirtualHost>
</IfDefine>
```

Po zapisaniu zmian w edytowanym pliku należy zrestartować serwer WWW.

np.

```
/apache/bin/apachectl stop
/apache/bin/apachectl startssl
```

Serwer WWW jest już gotowy do serwowania dokumentów w osłonie SSL.