

Procedura pozyskania i instalacji certyfikatu SSL dla **Stunnel 4.x**

Spis treści:

Wstęp	2
Przygotowanie.....	2
Generowanie wniosku o certyfikat	2
Proces pobierania certyfikatu z CC Signet.....	3
Instalacja certyfikatu	3
Podsumowanie i uwagi	3

Wstęp

Jest to dokument, który pokaże Ci, jak poprawnie skonfigurować Stunnel 4.x, do zestawiania szyfrowanych połączeń w protokole SSL/TLS. Kolejne rozdziały pomogą Ci przejść przez wszystkie etapy tworzenia wniosku o certyfikat oraz instalacji certyfikatu. W efekcie będziesz mógł z łatwością zabezpieczyć swój serwer korzystając z certyfikatów wystawionych przez **Centrum Certyfikacji Signet**.

Przygotowanie

Stunnel jest uniwersalnym oprogramowaniem szyfrującym połączenia TCP przy pomocy protokołu SSL. Pozwala udostępnić usługi tj. POP, IMAP, SMTP, LDAP, WWW i inne poprzez szyfrowane połączenia SSL. Robi to w sposób niezależny od wspomnianych usług.

Żeby wygenerować plik **stunnel.pem** potrzebny będzie nam pakiet OpenSSL.

Generowanie wniosku o certyfikat

Tworzymy katalog, w którym będziemy generowali wniosek CSR i przygotowujemy plik z certyfikatem, np.:

```
$ mkdir /tmp/certtmp
$ chmod 600 /tmp/certtmp
$ cd /tmp/certtmp
```

Tworzymy plik konfiguracyjny **stunnel.cnf** dla OpenSSL. Zawartość pliku jest następująca:

```
[ req ]
default_bits          = 1024
default_keyfile       = stunnel.key
distinguished_name    = req_distinguished_name

[ req_distinguished_name ]
commonName            = Nazwa podmiotu (nazwa serwera lub adres IP)
commonName_default    = localhost
emailAddress          = Adres Email
emailAddress_default  = postmaster@moja.domena.pl
```

Wykonujemy następujące polecenie generujące żądanie CSR:

```
$ openssl req -new -nodes -config stunnel.cnf > stunnel.csr
```

gdzie:

stunnel.csr jest plikiem zawierającym żądanie wystawienia certyfikatu. Jego zawartość powinna wyglądać mniej więcej tak:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADA+MRIwEAYDVQQDEw1sb2NhbGhvc3QxKDAmBgkqhkiG9w0BCQEW
GXBvc3RtYXN0ZXJAbW9qYS5kb211bmEucGwwZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMcfWcQ3T2dAE994qgzuniPNqcgqebb2YaE9ATkN6uIA9ZVspjxYqID7
/JJcPsygteO12Aw0yLjdzq5aQrSEE6Sw14ZP5X8mBai4G+0W8Nomt/VGHYqXPYAK
/q9N408GaMyaE10X6n7lHUBbxCW/TmbFv+QcvPRizJ0hEZQmM6MJAgMBAAGgADAN
BgkqhkiG9w0BAQQFAAObgQDA3kqRWxH70Bakmlu7hhuu3UKgAMCpT/XbjkONQbps
9peC92vT+xH40M1JRZGzin5RtVtWaumxyusrp0QrTxNPOPXNJtAu7712/lk1pG8T
qPyo1c3k6tpB99SLSvfl+YAgqjSMJvXKSn8D9dtqHv6ctDAVkJyWpGrSUC5BlxoJ
zg==
-----END CERTIFICATE REQUEST-----
```

W wyniku polecenia jest też tworzony plik **stunnel.key**, który zawiera klucz prywatny w postaci niezaszyfrowanej.

Możemy sprawdzić poprawność wniosku następującym poleceniem:

```
$ openssl req -text -noout < stunnel.csr
```

Proces pobierania certyfikatu z CC Signet

Następnym krokiem jest uzyskanie certyfikatu za pośrednictwem stron WWW Centrum Certyfikacji Signet (www.signet.pl). Otrzymany certyfikat zapisujemy w pliku **stunnel.crt**.

Instalacja certyfikatu

Po uzyskaniu certyfikatu z CC Signet możemy przystąpić do jego instalacji. W tym celu pobrany certyfikat i klucz prywatny zapisujemy w pliku **stunnel.crt**:

```
$ cp stunnel.key stunnel.pem
$ cat stunnel.crt >> stunnel.pem
```

umieszczamy certyfikat w dobrze chronionym obszarze filesystem'u i zabezpieczamy go przed odczytem przez osoby niepowołane np.:

```
$ cp stunnel.pem /usr/local/ssl/certs/stunnel.pem
$ chmod 400 /usr/local/ssl/certs/stunnel.pem
$ chmod +i stunnel.pem
$ rm -rf /tmp/certtmp
```

Położenie pliku **/usr/local/ssl/certs/stunnel.pem** jest domyślne.

Podsumowanie i uwagi

Powyższa procedura pozyskiwania certyfikatu i instalacji w Stunnel 3.x jest bardzo podobna do przedstawionej powyżej dla wersji 4.x.