

UNIZETO



POWSZECHNE  
CENTRUM CERTYFIKACJI



instrukcja użytkownika

# APACHE 2.0 + SSL – Linux

Użycie certyfikatów niekwalifikowanych  
w oprogramowaniu APACHE 2.0 + SSL – Linux

wersja 1.3

# Spis treści

<b>1. WSTĘP.....</b>	<b>3</b>
<b>2. TWORZENIE CERTYFIKATU.....</b>	<b>3</b>
2.1. GENEROWANIE WNIOSKU O CERTYFIKAT (CSR).....	3
2.2. TWORZENIE CERTYFIKATU NA PODSTAWIE UTWORZONEGO ŻĄDANIA (CSR).....	5
2.3. IMPORTOWANIE CERTYFIKATÓW .....	6
<b>3. INSTALOWANIE KLUCZY I CERTYFIKATÓW .....</b>	<b>8</b>
3.1. INSTALOWANIE CERTYFIKATÓW CERTUM.....	8
3.2. INSTALOWANIE KLUCZA PRYWATNEGO .....	8
3.3. INSTALOWANIE CERTYFIKATU SERWERA.....	9
<b>4. UWIERZYTELNIANIE WZGLĘDEM SERWERA NA PODSTAWIE CERTYFIKATU.....</b>	<b>9</b>
<b>5. OBSŁUGA WITRYN WIRTUALNYCH DLA ADRESÓW WIELOZNACZNYCH .....</b>	<b>10</b>
<b>6. KONFIGURACJA SSL/TLS DLA WIELU WIRTUALNYCH HOSTÓW .....</b>	<b>12</b>
6.1. KONFIGURACJA HOSTÓW WIRTUALNYCH BEZ UŻYCIA PROTOKOŁU SSL.....	12
6.2. KONFIGURACJA HOSTÓW WIRTUALNYCH Z UŻYCIEM PROTOKOŁU SSL .....	13

## 1. Wstęp

Apache jest najbardziej zaawansowanym serwerem WWW i można go pobrać w postaci kodu źródłowego. Serwer ten, dzięki modułowi modssl ma wsparcie silnej kryptografii.

Udział Apache w światowym rynku serwerów WWW zdecydowanie przeważa, a jego popularność, ze względu na dostępność dla różnych platform, wciąż rośnie.

Aby skonfigurować Apache w osłonie SSL będziemy potrzebowali następujących komponentów:

1. Apache - <http://httpd.apache.org>
2. OpenSSL - <http://www.openssl.org/>
3. mod\_ssl – <http://www.modssl.org/>

Jeśli Twoja dystrybucja Linuksa nie obejmuje powyższych składników, ściągnij je i zainstaluj.

**UWAGA:** W Apache 1.3 komponent mod\_ssl należy instalować jako osobny pakiet. Z kolei Apache 2.0 może być zintegrowany z mod\_ssl.

## 2. Tworzenie certyfikatu

### 2.1. Generowanie wniosku o certyfikat (CSR)

W celu wygenerowania kluczy dla Apache'a, wykorzystamy zewnętrzne narzędzie – Openssl, które można ściągnąć ze strony: <http://openssl.org>.

1. Po instalacji biblioteki Openssl, wydajemy polecenie:

```
openssl genrsa -des3 -out server.key 2048
```

Polecenie to spowoduje wygenerowanie klucza prywatnego o nazwie *server.key* dla naszego serwera. Klucz ten będzie miał długość 2048 bity i będzie zaszyfrowany algorytmem symetrycznym 3des. Podczas generowania klucza będziemy poproszeni o hasło, które zabezpieczy komponent.

```
OpenSSL> genrsa -des3 -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

Plik CSR wraz z kluczem prywatnym *server.key* należy zabezpieczyć na dyskiecie lub innym nośniku.

2. Po pomyślnym wygenerowaniu klucza prywatnego wydajemy polecenie:

```
openssl req -new -key server.key -out server.csr
```

Wynikiem tego polecenia jest żądanie certyfikatu CSR serwera, które zapisane będzie w pliku `server.csr`. Pamiętajmy o wskazaniu pliku z kluczem prywatnym `server.key`. Podczas generowania żądania CSR należy podać hasło zabezpieczające klucz prywatny oraz dane związane z naszą firmą i stroną www:

**Country (C)** - dwuliterowy symbol kraju (PL). Należy użyć kodu ISO, np. poprawnym kodem Polski jest PL (duże litery), a nie pl czy RP.

**State / Province (ST)** - nazwa województwa, np.: Zachodniopomorskie. Nie należy stosować skrótów .

**Locality (L)** - nazwa miasta lub wsi, np.: Szczecin, Kozia Wolka, Warszawa.

- **Organization Name (O)** - pełna nazwa swojej organizacji / firmy, np.: Moja Firma
- **Organizational Unit (OU)** - jeżeli zachodzi taka potrzeba, można wypełnić to pole, wstawiając nazwę działu np. Oddział w Moja Firma
- **Common Name (CN)** - bardzo ważne pole. Musi się tutaj znaleźć pełna nazwa DNS (fqdn) serwera np.: `www.test.com.pl` `pop3.test.net`.
- **Email (Email)** - podaj adres pocztowy administratora serwera np.: `cunizetowski@certum.pl`.

Pamiętajmy, że w pole **Common Name** musimy wpisać adres naszej witryny

- np. `mojserwer.com`, `mojadomena.pl`, `www.mojastrona.com.pl` – w przypadku adresu jednoznacznego:

```
OpenSSL> req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Zachodniopomorskie
Locality Name (eg, city) []:Szczecin
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Moja firma
Organizational Unit Name (eg, section) []:Oddział w Moja firma
Common Name (eg, YOUR name) []:mojserwer.pl
Email Address []:cunizetowski.pl_
```

- np. `*.mojserwer.com`, `*.mojadomena.pl`, `*.mojastrona.com.pl` – w przypadku adresu wieloznacznego:

```
OpenSSL> req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Zachodniopomorskie
Locality Name (eg, city) []:Szczecin
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Moja firma
Organizational Unit Name (eg, section) []:Oddział w Moja firma
Common Name (eg, YOUR name) []:*.mojserwer.pl
Email Address []:cunizetowski@certum.pl
```

**UWAGA:** Używanie znaków specjalnych % ^ \$ \_ lub polskich znaków diakrytycznych: Żółć przy podawaniu informacji dla żądania CSR spowoduje nieprawidłowe wygenerowanie certyfikatu !!!

## 2.2. Tworzenie certyfikatu na podstawie utworzonego żądania (CSR)

Wygenerowane w kroku poprzednim żądanie powinno mieć postać podobną do:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDMCCApkCAQAwgZoxGzAZBgNVBAMTEmRsdWJhY3oudW5pemV0by5wbDEhMB8G
A1UECXMpYRHpYyWwT2Nocm9ueSBjb21vcnNraWUxETAPBgNVBACjCFN6Y3plY2luMRswGQYDVQKExJVbml6ZXRv
IFNwLiB6IG8uby4xETAPBgNVBACjCFN6Y3plY2luMRswGQYDVQKExJaYWNob2Ru
aW9wb21vcnNraWUxETAPBgNVBAYTA1BMMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQC8JvRqRpb1toZyvMjfxCef5PIcyLMQv6Z2A10j2GMoeKBCCyZF1kHoDsWW
0ZF54FrTZhyKwYqfghiO5duLfJSBqb/PTzovZH9qXUtxl+zQIhcJnA4Z/jKyWHG1
X7LULC9u2bas/vWwQZwYvxeqNMW4RZ+LU9Qqm9b/YD2qtOZ2qwIDAQABoIIBUzAa
BgorBgEEAYI3DQIDMQwWCjUuMC4yMTk1LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYD
VR0PAQH/BAQDAgTWMBMGA1UdJQMMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQIC
MYHUMIHrAgEBHloATQBpAGMAcgbvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEA
bgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkA
ZABLAHIDgYkAXxNuAz6gcBaZUdef8WQ2PArOKMW8sprcKv7QD2encz6/Wct9DZ5C
kGynLgy0f+Lff7ViSDJqxYwaJ68ddqgXyAqIilF63kivPTiC6yxLaNX65v3cnKfx
4UrUrGXZtub7M7/NuxSipOW0Vv7yCHganypxDyRzp6IhulEnL4APEH4AAAAAAAAA
ADANBgbkqhkig9w0BAQUFAAOBgQAsTG3Hu00fFzNTekFo/fb3tKsmuS/1rCCB5sQK
iNpWGZ8Z8+TmqBB0Tuz4FPtkeSqLpWv1ORfmxMKPIu10dC3QwRP2E//oMPnaU807
IJIDwn2VZ7qQ/h0KcWoWSPmvt7J0KKshdGgAF7P6AYc7W4yA9B9nPeyEzQRW0t4D
YBApPQ==
-----END NEW CERTIFICATE REQUEST-----
```

Mając wygenerowane żądanie wypełniamy formularz zgłoszeniowy i wklejamy CSR na stronie CERTUM ([www.certum.pl](http://www.certum.pl)) -> *Oferta* -> *Certyfikaty niekwalifikowane* -> *Zabezpieczanie serwerów* -> *Serwery WWW* -> wybieramy, który certyfikat chcemy kupić i na dole strony wybieramy *Kup certyfikat*).

### Pobierz certyfikat Private WEB Server (niekwalifikowany)

#### - Żądanie certyfikatu

W poniższe pole wstaw żądanie certyfikatu zgodne z PKCS#10.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzCCATgCAQAwgY4xCzAJBgNVBAYTA1BMMRswGQYDVQKExJaYWNob2Ruaw9wb21vcnNraWUxETAPBgNVBACjCFN6Y3plY2luMRswGQYDVQKExJVbml6ZXRvIFNwLiB6IG8uby4xETAPBgNVBAYTA1BMMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8JvRqRpb1toZyvMjfxCef5PIcyLMQv6Z2A10j2GMoeKBCCyZF1kHoDsWW0ZF54FrTZhyKwYqfghiO5duLfJSBqb/PTzovZH9qXUtxl+zQIhcJnA4Z/jKyWHG1X7LULC9u2bas/vWwQZwYvxeqNMW4RZ+LU9Qqm9b/YD2qtOZ2qwIDAQABoIIBUzAaBgorBgEEAYI3DQIDMQwWCjUuMC4yMTk1LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYDVR0PAQH/BAQDAgTWMBMGA1UdJQMMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHUMIHrAgEBHloATQBpAGMAcgbvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABLAHIDgYkAXxNuAz6gcBaZUdef8WQ2PArOKMW8sprcKv7QD2encz6/Wct9DZ5CkGynLgy0f+Lff7ViSDJqxYwaJ68ddqgXyAqIilF63kivPTiC6yxLaNX65v3cnKfx4UrUrGXZtub7M7/NuxSipOW0Vv7yCHganypxDyRzp6IhulEnL4APEH4AAAAAAAAADANBgbkqhkig9w0BAQUFAAOBgQAsTG3Hu00fFzNTekFo/fb3tKsmuS/1rCCB5sQKiNpWGZ8Z8+TmqBB0Tuz4FPtkeSqLpWv1ORfmxMKPIu10dC3QwRP2E//oMPnaU807IJIDwn2VZ7qQ/h0KcWoWSPmvt7J0KKshdGgAF7P6AYc7W4yA9B9nPeyEzQRW0t4DYBApPQ==
-----END CERTIFICATE REQUEST-----
```

#### - Adres email

Podaj adres e-mail, na który zostaną wysłane dalsze instrukcje postępowania.

E-mail:

#### - Oświadczenie

ZANIM ZŁOŻYSZ WNIOSEK O WYDANIE CERTYFIKATU, POTWIERDZISZ GO, BĄDŹ UŻYJESZ DO REALIZACJI PIERWSZEGO PODPISU POWINIENIEŚ PRZECZYTAĆ TEKST NINIEJSZEGO OŚWIADCZENIA. JEŚLI NIE ZGADZASZ SIĘ Z WARUNKAMI NINIEJSZEGO OŚWIADCZENIA, NIE SKŁADAJ WNIOSKU O WYDANIE CERTYFIKATU, NIE POTWIERDZAJ I NIE UŻYWAJ GO.

Niniejsze oświadczenie obowiązuje od momentu przesłania przez Ciebie wniosku o wydanie certyfikatu do CERTUM - Powszechne Centrum Certyfikacji. Przedkładając wniosek o wydanie

Potwierdzam oświadczenie

Dalej

**UWAGA:** W celu wklejania certyfikatu na stronie należy skopiować fragment tekstu od linii "--BEGIN CERTIFICATE --" do "--END CERTIFICATE--" (razem z tymi liniami!!!), używając do tego celu edytora tekstowego.

Upewniamy się, że w polu *E-mail* jest wpisany poprawny adres (na ten adres zostaną wysłane dalsze instrukcje), oraz, że zaznaczyliśmy pole *Potwierdzam Oświadczenie* i klikamy *Dalej*.

Pojawi się strona, na której możemy się upewnić, że nasze żądanie CSR zostało wygenerowane na prawidłowe dane.

**Uwaga:** Należy się upewnić, że w polu podmiot jest wpisana poprawna nazwa naszej strony (jesli kupujemy certyfikat na domenę [www.mojastrona.com](http://www.mojastrona.com) upewnijmy się, że ta nazwa widnieje w tym polu)!!!

Upewniwszy się co do poprawności wprowadzonych danych klikamy *Dalej*:

### Pobierz certyfikat Private WEB Server (niekwalifikowany)

#### — Weryfikacja danych —

 Poniżej znajdują się dane, które zawarte są w żądaniu certyfikatu. Jeśli zachodzi potrzeba modyfikacji danych, należy anulować dalsze wypełnianie formularza i przygotować nowe żądanie PKCS#10

Kraj: PL  
Województwo: Zachodniopomorskie  
Miasto: Szczecin  
Firma: Certum  
Podmiot: **10.100.10.122**  
E-mail: mproszkiewicz@certum.pl

Jeżeli powyższe dane są poprawne, naciśnij "Dalej", aby kontynuować proces wydawania certyfikatu.

**Dalej**

Pojawi się okno z informacją o wymaganych dokumentach niezbędnych do zakończenia procesu uzyskania certyfikatu.

### 2.3. Importowanie certyfikatów

Po wykonaniu powyższej procedury z poprzedniego punktu otrzymamy stosownego e-maila z adresem strony oraz numerem ID umożliwiającym aktywację certyfikatu (umieszczenie certyfikatu w naszym repozytorium dostępnym na stronach www):

ID instalacyjne certyfikatu: b7b1610e652ec1bddbd7e247508dca82a8a5e6a9

Proszę wkleić ID na stronie:  
<https://www.certum.pl/install/>

--  
Zespół Unizeto CA  
[info@certum.pl](mailto:info@certum.pl)

Wchodzimy na stronę, wklejamy ID i aktywujemy certyfikat klikając *Dalej*:

### Instalacja certyfikatu

Wpisz numer certyfikatu który dostałeś w mailu od CERTUM:

b7b1610e652ec1bddbd7e247508dca82a8a5e6a9

**Uwaga!**

W przypadku certyfikatów e-mail instalacja podpisu powinna odbywać się na tym samym komputerze i przy pomocy tej samej przeglądarki, której używałeś podając adres e-mail.

Pojawi się okno ze szczegółami naszego certyfikatu:


### Instalacja certyfikatu

<b>Private WEB Server</b>	ważny do: 13.06.2007
Podmiot: 10.100.10.122	
Email: mproszkiewicz@certum.pl	
Numer: 0x37CCC	
<input type="button" value="Instaluj"/>	

Kopiujemy numer naszego certyfikatu, wchodzimy na stronę <https://www.certum.pl/services/search.html> i w polu *Nr seryjny*: wpisujemy numer naszego certyfikatu:

### Wyszukaj certyfikat (niekwalifikowany)

— **Wyszukaj certyfikat** —

 Wpisz adres e-mail lub nazwę podmiotu (imię i nazwisko lub adres serwera www) lub numer seryjny aby odnaleźć certyfikat.

E-mail:   
Nazwa podmiotu:   
Nr seryjny:

Pojawi się strona, z której będziemy mogli ściągnąć nasz certyfikat w formie binarnej lub tekstowej. Klikamy w *Zapisz tekstowo*:

### Wyszukaj certyfikat (niekwalifikowany)

<b>Private WEB Server</b>	Ważny do: 13-06-2007	
Podmiot: 10.100.10.122		
Numer: 0x37CCC		
Status: <b>Ważny</b>		
<input type="button" value="Zainstaluj własny"/>	<input type="button" value="Zapisz binarnie"/>	<input type="button" value="Zapisz tekstowo"/>

## 3. Instalowanie kluczy i certyfikatów

### 3.1. Instalowanie certyfikatów CERTUM

Poza naszym certyfikatem trzeba jeszcze dodatkowo zainstalować na serwerze certyfikaty CERTUM (certyfikaty CERTUM w jednej paczce znajdują się pod adresem <http://www.certum.pl/keys/ca-bundle.crt>). W paczce znajdują się wszystkie certyfikaty CERTUM: wszystkie certyfikaty pośrednie (w kolejności od Level I do Level IV), oraz root CA na końcu.

W celu zainstalowania certyfikatów root CA i certyfikatów pośrednich kopiujemy (z poziomu Midnight Commandera bądź linii poleceń) plik z naszą paczką *ca-bundle.crt* do katalogu, gdzie będziemy ją przechowywać, np. do:

```
/usr/share/ssl/certs/ca-bundle.crt
```

Wpis do pliku *ssl.conf* będzie wyglądał następująco:

```
SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
```

Po tych czynnościach restartujemy serwer poleceniem:

```
#httpd restart
```

Instalacja certyfikatu *root CA* i *certyfikatów pośrednich* została zakończona pomyślnie.

Dla naszej wygody w pliku *ca-bundle.crt* możemy umieścić na początku pliku certyfikat naszego serwera (kopiujemy zawartość z pliku *Nr\_certyfikatu.pem* i wklejamy na początku pliku *ca-bundle.crt*).

### 3.2. Instalowanie klucza prywatnego

Aby zainstalować klucz prywatny na serwerze, należy skopiować (z poziomu Midnight Commandera bądź linii poleceń) plik z kluczem prywatnym *server.key* do katalogu, w którym będziemy go przechowywać, np.:

```
/etc/httpd/conf/ssl.key/server.key
```

Wpis do pliku *ssl.conf* będzie wyglądał następująco:

```
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
```

Zdejmujemy hasło z klucza prywatnego, (aby przy każdym restarcie Apache nie pytał nas o hasło):

```
openssl rsa -in server.key -out server.key  
OpenSSL> rsa -in server.key -out server.key  
Enter pass phrase for server.key:  
writing RSA key  
OpenSSL>
```

Zabezpieczamy klucz przed odczytem:

```
#chmod 400 /etc/httpd/conf/ssl.key/server.key
```

Po tych czynnościach restartujemy serwer poleceniem:

```
#httpd restart
```

Instalacja klucza prywatnego została zakończona pomyślnie.

### 3.3. Instalowanie certyfikatu serwera

Po wklejeniu ID na naszych stronach, zostanie nam zwrócony certyfikat naszego serwera www. Należy go skopiować myszką do dowolnego edytora tekstowego i zapisać plik jako np. server.crt.

**UWAGA:** W celu wklejania certyfikatu ze strony należy skopiować fragment tekstu od linii "--BEGIN CERTIFICATE --" do "--END CERTIFICATE--", używając do tego celu edytora tekstowego np. Notepad i myszki.

**Nie używaj do tej operacji Worda, czy innego procesora tekstowego !**

W przypadku gdybyśmy stracili plik z certyfikatem serwera, należy pamiętać, iż znajduje się on na pierwszym miejscu w pliku *ca-bundle.crt* (skąd można go po prostu przekopiować). Alternatywą dla takiego rozwiązania jest wyszukiwanie interesującego nas certyfikatu w repozytorium na naszych stronach.

W celu zainstalowania certyfikatu serwera kopiujemy (z poziomu Midnight Commandera bądź linii poleceń) plik z certyfikatem do katalogu, gdzie będziemy go przechowywać, np. do:

```
/etc/httpd/conf/ssl.crt/server.crt
```

Wpis do pliku *ssl.conf* będzie wyglądał następująco:

```
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
```

Po tych czynnościach restartujemy serwer poleceniem:

```
#httpd restart
```

Instalacja certyfikatu serwera została zakończona pomyślnie.

Po skonfigurowaniu serwera DNS do obsługi naszej domeny (lub poddomeny) www, serwer będzie obsługiwał certyfikaty zarówno dla adresów jednoznacznych jak i wieloznacznych (jeśli dodamy hosty wirtualne – opis w pkt. 5).

Jeżeli nie posiadasz własnego serwera DNS skontaktuj się ze swoim providerem i przedstaw sytuację.

**UWAGA:** Klucze i certyfikaty mogą być również przechowywane w jednym pliku. W tym celu należy do pliku *ca-bundle.crt* dołączyć klucz prywatny i odpowiednio zmienić zapisy w pliku konfiguracyjnym *ssl.conf*:

```
SSLCertificateFile /sciezka_do_pliku/ca-bundle.crt
```

```
SSLCACertificateFile /sciezka_do_pliku/ca-bundle.crt
```

```
SSLCertificateKeyFile /sciezka_do_pliku/ca-bundle.crt
```

## 4. Uwierzytelnianie względem serwera na podstawie certyfikatu

Aby wymuszać na kliencie posiadanie certyfikatu w pliku *SSL.conf* dopisujemy (odkomentowujemy) dwie linie:

```
SSLVerifyClient require (wymuszanie certyfikatu klienta)
```

```
SSLVerifyDepth 10 (określa maksymalną głębokość ścieżki certyfikacji)
```

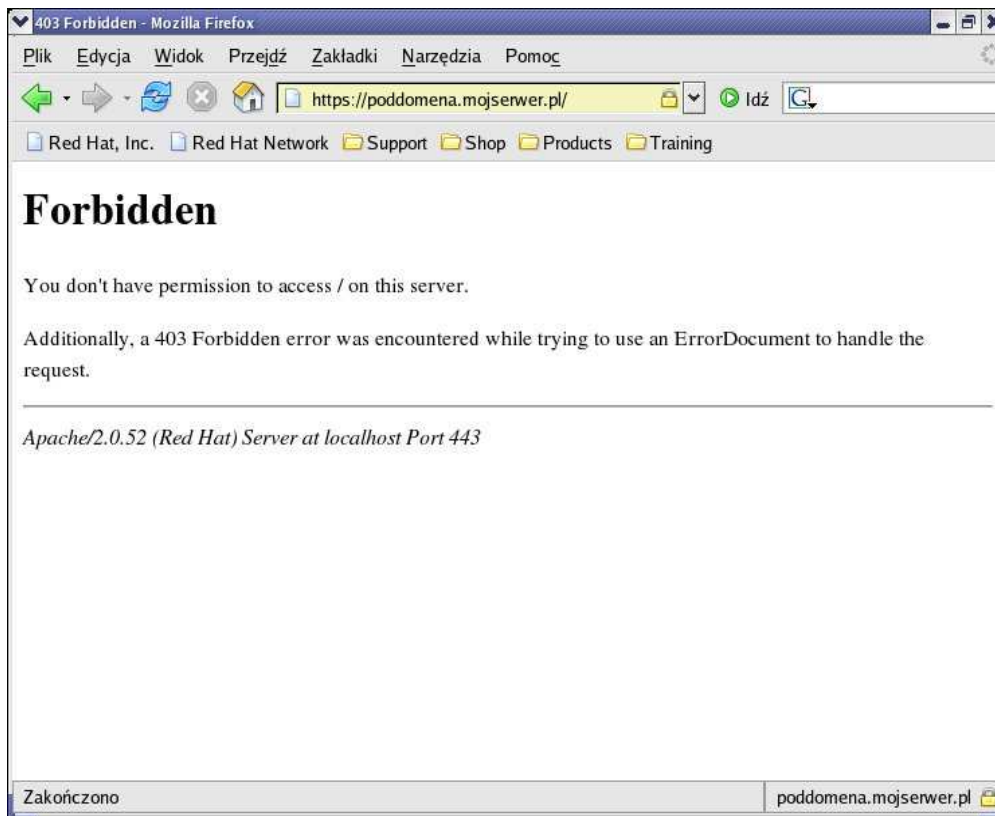
W celu ograniczenia dostępu do strony dla konkretnych użytkowników, np. dysponujących certyfikatem Certum Level III, o numerze seryjnym 02F110 dodajemy do pliku *ssl.conf* w sekcji *Location* wpis:

```
<Location />
```

```
SSLRequire ( %{SSL_CLIENT_I_DN_CN} eq "Certum Level III" and
```

```
%{SSL_CLIENT_M_SERIAL} eq "02F128" )  
</Location>
```

W przypadku gdy klient nie ma uprawnień do witryny, zostanie następującą stroną:



Zapisujemy plik *SSL.conf* i restartujemy serwer:

```
#httpd restart
```

Więcej informacji na ten temat znajdziemy na: <http://httpd.apache.org/>

## 5. Obsługa witryn wirtualnych dla adresów wieloznacznych

Aby na jednym serwerze uruchomić wiele poddomen wirtualnych, obsługiwanych przez nasze certyfikaty Wildcard'owe, należy nanieść kilka modyfikacji do pliku *ssl.conf*. W tym celu otwieramy plik w edytorze dodajemy wpis:

```
NameVirtualHost adres_ip_naszego_serwera:443
```

- Sekcja VirtualHost dla pierwszego host wirtualnego:

```
<VirtualHost adres_ip_naszego_serwera:443>
```

w tym katalogu umieścimy nasze pliki *www*:

```
DocumentRoot /var/www/html1
```

nazwa DNS wirtualnego hosta o certyfikacie *\*.mojserwer.pl*:

```
ServerName poddomena1.mojserwer.pl
```

obsługa sesji szyfrowanych:

```
SSLEnable
```

reszta pozostaje bez zmian:

```
...  
</VirtualHost>
```

- 2. Sekcja VirtualHost dla drugiego hosta wirtualnego:

```
<VirtualHost adres_ip_naszego_serwera:443>  
DocumentRoot /var/www/html2  
ServerName poddomena2.mojserwer.pl  
SSLEnable  
...  
</VirtualHost>
```

Zapisujemy zmiany i restartujemy serwer:

```
#httpd restart
```

Po skonfigurowaniu serwera DNS do obsługi tych domen (jeżeli nie posiadasz własnego serwera DNS skontaktuj się ze swoim providerem i przedstaw sytuację), serwer będzie przygotowany do obsługi certyfikatów dla adresów wieloznacznych.

Aby sprawdzić działanie wirtualnych serwerów uruchamiamy serwer:

```
#httpd start
```

i wpisujemy w przeglądarce:

- <https://poddomena1.mojserwer.pl>
- <https://poddomena2.mojserwer.pl>

Pojawienie się charakterystycznej kłódki u dołu ekranu:



oznacza sesję szyfrowaną.

W razie problemów warto diagnozować problem przy użyciu narzędzi typu *nmap*, *ps*, *netstat* czy *openssl s\_client*.

## 6. Konfiguracja SSL/TLS dla wielu wirtualnych hostów

### 6.1. Konfiguracja Hostów Wirtualnych bez użycia protokołu SSL

Serwer Apache umożliwia skonfigurowanie i przechowywanie wielu witryn WWW w obrębie jednego fizycznego serwera. Na podstawie nagłówków HTTP lub adresów w pakiecie IP serwer może odnaleźć witrynę, do której adresowane było żądanie. Istnieją dwa typy wirtualnych serwerów:

- oparta na nazwach
- oparte na adresach IP

Pierwszy typ umożliwia uruchomienie wielu witryn WWW na jednym fizycznym serwerze. Serwer musi posiadać tylko jeden publiczny adres IP. W tym przypadku docelowa witryna jest określana na podstawie żądań HTTP.

Drugi typ wirtualnych serwerów opiera na się adresach IP. Serwerowi (fizycznej maszynie) zostaje przypisanych kilka różnych, publicznych adresów IP. Z punktu widzenia użytkowników Internetu ten serwer jest widoczny jako dwa logiczne hosty. Każdy host obsługuje jedną witrynę. Określanie, którą witrynę należy przestać klientowi nie jest konieczne – to klient decyduje, z którym adresem chce się połączyć. Użytkownik wpisuje adres witryny w przeglądarce, a następnie serwer DNS rozwiązuje nazwę hosta i zwraca adres IP, na którym przechowywana jest żądana witryna.

Aby skonfigurować Hosty Wirtualne konieczna będzie edycja plików konfiguracyjnych serwera Apache. Na potrzeby tego poradnika założono, że główny plik konfiguracyjny (`httpd.conf`) znajduje się w katalogu `C:\Program Files\Apache Software Foundation\Apache2.2\conf`. Plik konfiguracyjny Hostów Wirtualnych to `C:\Program Files\Apache Software Foundation\Apache2.2\conf\extra\httpd-vhosts.conf`.

**Uwaga:** W zależności od platformy sprzętowej, systemu operacyjnego i wersji serwera nazwy katalogów i plików konfiguracyjnych mogą się różnić. Należy zapoznać się z dokumentacją systemu operacyjnego i serwera Apache aby określić prawidłową ścieżkę i nazwę pliku.

W głównym pliku konfiguracyjnym należy odnaleźć linijkę:

```
#Include conf/extra/httpd-vhosts.conf
```

i usunąć znak komentarza („#”). Następnie należy edytować plik `httpd-vhosts.conf`. Znajdują się w nim definicje Hostów Wirtualnych. Definicje Hostów opartych na adresach IP wyglądają podobnie do przedstawionych poniżej:

```
<VirtualHost 11.100.10.109:80>
    ServerAdmin admin@certum.pl
    DocumentRoot "C:/Program Files/Apache Software
Foundation/Apache2.2/htdocs/strona1.local"
    ServerName strona1.local
    ServerAlias strona1.local
    ErrorLog "logs/strona1.local.log"
    CustomLog "logs/strona1.local-access.log" common
</VirtualHost>
```

```
<VirtualHost 11.100.10.110:80>
  ServerAdmin jmila@certum.pl
  DocumentRoot "C:/Program Files/Apache Software
Foundation/Apache2.2/htdocs/strona2.local"
  ServerName strona2.local
  ServerAlias strona2.local
  ErrorLog "logs/strona2.local.log"
  CustomLog "logs/strona1-access.log" common
</VirtualHost>
```

Dyrektywa `<VirtualHost 11.100.10.109:80>` wskazuje, że serwer ma nasłuchiwać połączeń na interfejsie z adresem IP 11.100.10.109 i porcie 80. Dalej następują kolejne dyrektywy określające szczegóły konfiguracji serwera takie jak nazwa serwera, katalog z witryną i pliki z dziennikami zdarzeń.

Powyższa konfiguracja opisuje konfigurację serwerów wirtualnych opartych na adresach IP. Każdy wirtualny serwer posiada własny adres IP. Jeśli każdemu Hostowi Wirtualnemu przypisze się dokładnie taki sam adres IP, to będą to Hosty bazujące na nazwach.

## 6.2. Konfiguracja Hostów Wirtualnych z użyciem protokołu SSL

**Uwaga:** Aby skonfigurować protokół SS/TLS dla wielu różnych witryn muszą być dla nich skonfigurowane Hosty Wirtualne oparte na adresach IP.

Na potrzeby tego poradnika założono, że administrator jest w posiadaniu odpowiedniej ilości ważnych certyfikatów i pasujących do nich kluczy prywatnych. Wszystkie certyfikaty i klucze prywatne zostały zapisane w katalogu: `C:\Program Files\Apache Software Foundation\Apache2.2\SSL`. Klucze prywatne nie powinny być chronione hasłem. Jeśli klucze prywatne będą chronione hasłem uruchomienie protokołu SSL/TLS nie będzie możliwe bez podania tego hasła. Aby usunąć hasło należy wydać polecenie:

```
openssl rsa -in protected.key -out clear.key
```

Pierwszym krokiem w celu skonfigurowania Hostów Wirtualnych jest edycja głównego pliku konfiguracyjnego. Należy odnaleźć linijkę:

```
#LoadModule ssl_module modules/mod_ssl.so
```

i usunąć znak komentarza na początku linii. Następnie należy odnaleźć linijkę:

```
#Include conf/extra/httpd-ssl.conf
```

Tu także należy usunąć znak komentarza. Po wprowadzeniu tych zmian należy zapisać główny plik konfiguracyjny i przystąpić do edycji pliku `httpd-ssl.conf`.

Pierwszym elementem do konfiguracji jest włącznie obsługi protokołu SSL na porcie 443. Linijkę:

```
Listen 443
```

należy poprawić na:

```
Listen 443 https
```

Najważniejszym elementem będzie zdefiniowanie Wirtualnych Hostów. Należy użyć tych samych definicji Hostów Wirtualnych, jakich użyto do konfiguracji bez protokołu SSL/TLS i dokonać w nich stosownych zmian:

```
<VirtualHost 10.100.10.109:443>

DocumentRoot "C:/Program Files/Apache Software
Foundation/Apache2.2/htdocs/strona1.local"
ServerName strona1.local
ServerAdmin admin@certum.pl
ErrorLog "C:/Program Files/Apache Software
Foundation/Apache2.2/logs/error.log"
TransferLog "C:/Program Files/Apache Software
Foundation/Apache2.2/logs/access.log"

SSLEngine on

SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

SSLCertificateFile "C:/Program Files/Apache Software
Foundation/Apache2.2/SSL/strona1.local/strona1.local.pem"

SSLCertificateKeyFile "C:/Program Files/Apache Software
Foundation/Apache2.2/SSL/strona1.local/strona1.local.key"

SSLCACertificateFile "C:/Program Files/Apache Software
Foundation/Apache2.2/SSL/ca-bundle.cer"

</VirtualHost>
```

Kluczowe są tu następujące dyrektywy:

SSLEngine on – włącza protokół SSL/TLS w danym Goście Wirtualnym.

SSLCipherSuite

ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL – określa zestaw szyfrów stosowanych podczas transmisji zaszyfrowanych danych.

SSLCertificateFile – określa plik z certyfikatem serwera

SSLCertificateKeyFile – określa plik z kluczem prywatnym pasującym do certyfikatu określonego parametrem SSLCertificateFile

SSLCACertificateFile – definiuje ścieżkę do pliku z certyfikatami urzędów pośrednich.

Analogicznie powinna wyglądać definicja Wirtualnego Hosta dla drugiej witryny:

```
<VirtualHost 10.100.10.110:443>

DocumentRoot "C:/Program Files/Apache Software
Foundation/Apache2.2/htdocs/strona2.local"
ServerName strona2.local
```

```
ServerAdmin admin@certum.pl
ErrorLog "C:/Program Files/Apache Software
Foundation/Apache2.2/logs/error.log"
TransferLog "C:/Program Files/Apache Software
Foundation/Apache2.2/logs/access.log"

SSLEngine on

SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

SSLCertificateFile "C:/Program Files/Apache Software
Foundation/Apache2.2/SSL/strona2.local/strona2.local.pem"

SSLCertificateKeyFile "C:/Program Files/Apache Software
Foundation/Apache2.2/SSL/strona2.local/strona2.local.key"

SSLCACertificateFile "C:/Program Files/Apache Software
Foundation/Apache2.2/SSL/ca-bundle.cer"

</VirtualHost>
```

Należy zwrócić uwagę na adres przypisany Wirtualnemu Hostowi. W poprzednim przypadku ostatni oktet adresu IP to 109, teraz – 110. Należy pamiętać, aby dwóm różnym witrynom przypisać dwa różne certyfikatu i pasujące do nich klucze prywatne.