

UNIZETO



POWSZECHNE
CENTRUM CERTYFIKACJI



instrukcja użytkownika

VSFTPd 2.0.1+

Użycie certyfikatów niekwalifikowanych w
oprogramowaniu VSFTPd

wersja 1.2

Spis treści

1. WSTĘP	3
2. TWORZENIE KLUCZY I CERTYFIKATU DLA DEMONA VSFTPD.....	3
2.1. GENEROWANIE WNIOSKU O CERTYFIKAT (CSR).....	3
2.2. TWORZENIE CERTYFIKATU NA PODSTAWIE UTWORZONEGO ŻĄDANIA (CSR)	4
2.3. IMPORTOWANIE CERTYFIKATÓW.....	6
3. POBIERANIE CERTYFIKATÓW CERTUM CA I CERTYFIKATÓW POŚREDNICH.....	7
4. INSTALOWANIE KLUCZA PRYWATNEGO I CERTYFIKATÓW W VSFTPD.....	8
5. KONFIGUROWANIE VSFTPD DO POŁĄCZEŃ W OTOCZENIU SSL.....	8

1. Wstęp

VSFTPD jest darmowym (BSD), bezpiecznym, wysokiej jakości, spełniającym wszelkie standardy serwerem FTP. Bardzo dobrze sprawdza się zarówno dla użytku domowego jak i dla wszelkiego rodzaju organizacji czy dużych firm. Jest bardzo przyjazny dla administratorów (obsługuje m.in. język polski) i dobrze współpracuje z wieloma różnymi usługami (m.in. LDAP czy SQL). Dzięki integracji z biblioteką OpenSSL zapewnia użytkownikom pełną poufność i integralność danych.

Aby właściwie skonfigurować połączenia SSL na linii klient-serwer potrzebne będą następujące komponenty:

- Serwer Pure-FTPd – www.vsftpd.beasts.org
- Biblioteka OpenSSL – www.openssl.org
- Kompatybilny klient

Jeżeli Twoja dystrybucja Linuksa nie obejmuje powyższych składników, ściągnij je i zainstaluj. Przy pisaniu tej instrukcji, Autor korzystał z dystrybucji: Red Hat Enterprise Linux 4.

2. Tworzenie kluczy i certyfikatu dla demona VSFTPD

2.1. Generowanie wniosku o certyfikat (CSR)

W celu wygenerowania kluczy i wniosku o certyfikat, 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
```

```
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 dyskietce 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 serwerem poczty:

1. **Country (C)** - dwuliterowy symbol kraju (PL). Należy użyć kodu ISO, np. poprawnym kodem Polski jest PL (duże litery), a nie pl czy RP.
2. **State / Province (ST)** - nazwa województwa, np.: Zachodniopomorskie. Nie należy stosować skrótów
3. **City or Locality (L)** - nazwa miasta lub wsi, np.: Szczecin, Kozia Wolka, Warszawa.
4. **Organization Name (O)** - pełna nazwa swojej organizacji / firmy, np.: Moja Firma
5. **Organizational Unit (OU)** - jeżeli zachodzi taka potrzeba, można wypełnić to pole, wstawiając nazwę działu np. Oddział w Moja Firma
6. **Common Name (CN)** - bardzo ważne pole. Musi się tutaj znaleźć pełna nazwa DNS (fqdn) serwera np.: www.mojserwer.pl, mojadomena.plm *.mojserwer.pl.

UWAGA: Używanie znaków specjalnych % ^ \$ _ lub polskich znaków diakrytycznych: źżćął przy podawaniu tych informacji, spowoduje nieprawidłowe wygenerowanie certyfikatu !!!

Pamiętajmy, że w polu Common Name musimy wpisać nazwę fqdn naszego serwera, np. poczta.mojserwer.com, pop3.mojadomena.pl, smtp.test.com.pl:

```
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_
```

2.2. Tworzenie certyfikatu na podstawie utworzonego żądania (CSR)

Wygenerowane w kroku poprzedni żądanie powinno mieć postać podobną do poniższej:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDMCCApkCAQAwZoxGzAZBgNVBAMTEmRsdWJhY3oudW5pemV0by5wbDEhMB8G
A1UECxMYRHppYWwgT2Nocm9ueSBJbmcZvcmlhY2ppMRswGQYDVQQKEExJVbml6ZXRv
IFNwLiB6IG8uby4xETAPBgNVBACTCFNY3plY2luMRswGQYDVQQIExJaYWNob2Ru
aW9wb2lvcnNraWUxZAJBgNVBAYTAlBMMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQC8JvRqRPbltoZyvmjfxCef5PIcyLMQv6z2A10j2GMoeKBCCyZF1kHoDsWw
0ZF54FrTZhyKwYqfgiHO5duLfJSBqb/PTzovZH9qXUtxl+zQIhcJnA4Z/jKyWHGL
X7LULc9u2bas/vWwQZwYvxeqNMW4RZ+LU9Qqm9b/YD2qtOZ2qwIDAQABOIIIBUzAa
BgorBgEEAYI3DQIDMQwWCjUuMC4yMTk1LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYD
VR0PAQH/BAQDAgTwMBMGAlUdJQQMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQIC
MYHuMIHrAgEBHloATQBpAGMAcGvVAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEA
bgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkA
ZABLAHIDgYkAXxNuAz6gcBaZUdef8WQ2PArOKMw8sprcKv7QD2encz6/Wct9DZ5C
kGynLGy0f+Lff7ViSDJqxYWaJ68ddqgXyAqIilF63kivPTiC6yxLaNX65v3cnKFx
4UrUrGXZtub7M7/NuxSipOW0Vv7yCHganypxDyRzp6IhulEnL4APEH4AAAAAAAAA
ADANBgkqhkiG9w0BAQUFAAOBgQAsTG3Hu00fFzNTekFo/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 -> Oferta -> Certyfikaty niekwalifikowane -> Zabezpieczanie serwerów -> Serwery SSL i na dole strony wybieramy Kup certyfikat).

Pobierz certyfikat Test SSL (niekwalifikowany)

Żądanie certyfikatu

W poniższe pole wstaw żądanie certyfikatu (CSR).

Żądanie certyfikatu można wygenerować:

- korzystając z generatora dostępnego na stronach CERTUM ([wygeneruj CSR](#))

- na serwerze na którym znajduje się zabezpieczana domena ([pobierz instrukcje dla swojej platformy](#))

```
8YzM+albrFVyoDVY4mJtoCIwxUkV/P9k8Z4EPbqeZiq2QjyhCeAgpM+Aw3IHciL
xyJ2oXN2aFZNxN0jz00yDhVRYZW1wPII+9G3VQIDAQABoAAwDQYJKoZIhvcNAQEF
BQADggEBAAZyFwOIEkTH0fyGKIVi3HOXf5zOc6SR>JgEq2pIa7 9nZ/KPwE/wmLsQ
y47PkrTON0irsmZLWry2WBDXK/ca6Tvvd3L90FQcFvGh5KRqLxLw67Jy7/L546hi
EwCpCjqqgyg/p0yEY+ZDMVxbZH2cInQjaGEEWKukloj2Z07yZiqsEoutR/TDv2DI
dct4A/OccdfdmAZLhlzFFINXenN5w4zd61mIKdx2bD7H23B9nwQhA9udsTOpOMZ
ZThyGKBw4KpdCbKiirdSr19aYBOJ30WMYd4PO0a3ZJI015+2v3DYsgu0+zyztgkh
pFWEJQefoLevjWu8NTz3jtdDI83G/U=
-----END NEW 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 certyfikatu żądasz od organu je wydającego rozpatrzenia i wydania certyfikatu; jednocześnie oświadczasz, że akceptujesz warunki w nim

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 (jeśli kupujemy certyfikat na domenę poczta.mojserwer.com upewnijmy się, że ta nazwa widnieje w tym polu)!

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

Pobierz certyfikat Test SSL (niekwalifikowany)

Weryfikacja danych

i 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
Oddział firmy: Certum
E-mail: jankowalski@unizeto.pl
Firma: 10.100.10.122
Podmiot: **mojadomena.pl**

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

Dalej

Po wykonaniu powyższej procedury zostaniemy poinformowani stosownym e-mailem o dalszych krokach naszych działań.

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).

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

Instalacja certyfikatu

Wpisz numer certyfikatu który dostałeś w mailu od CERTUM:

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:

Private SSL Server	ważny do: 17.06.2007
Podmiot: 10.100.10.122	
Email: mproszkiewicz@certum.pl	
Numer: 0x37D85	
Zapisz binarnie	Zapisz tekstowo

Klikamy *Zapisz tekstowo*, aby zapisać certyfikat jako plik *.pem lub *Zapisz binarnie*, aby zapisać certyfikat jako plik *.cer.

UWAGA: W przypadku utraty pliku z certyfikatem, możemy go pobrać ze strony www.certum.pl -> Obsługa certyfikatów -> Wyszukaj certyfikat (niekwalifikowany).

Wyszukaj certyfikat (niekwalifikowany)

— Wyszukaj certyfikat

1 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:

Szukaj

Dla interesującego nas certyfikatu wybieramy opcję *Zapisz tekstowo* lub *Zapisz binarnie*:

Private SSL Server	Ważny do: 17-06-2007	
Podmiot: 10.100.10.122		
Numer: 0x37D85		
Status: Ważny		
Zainstaluj własny	Zapisz binarnie	Zapisz tekstowo

UWAGA: Pobrany w ten sposób plik zawiera jedynie certyfikat serwera – pozostałe certyfikaty CERTUM można pobrać z działu *Obsługa certyfikatów -> Zaświadczenia i klucze* i dołączyć do pobranego pliku.

3. Pobieranie certyfikatów Certum CA i certyfikatów pośrednich

Aby pobrać certyfikat Certum CA lub certyfikaty pośrednie należy wejść na stronę www.certum.pl do działu *Obsługa certyfikatów -> Zaświadczenia i klucze*. Po wybraniu certyfikatu należy wybrać opcję *Certyfikat dla serwerów WWW*.

Główny klucz urzędu - Certum CA	
Nr seryjny:	10020
Ważny od:	Jun 11 10:46:39 2002 GMT
Ważny do:	Jun 11 10:46:39 2027 GMT
Certyfikat dla Przeglądarek Internetowych	<input type="button" value="Instaluj"/>
Certyfikat dla Serwerów WWW i SSL/TLS	<input type="button" value="Instaluj"/>
Certyfikat dla urzędów sieciowych	<input type="button" value="Instaluj"/>

[do góry](#)

Wyświetlił się interesujący nas certyfikat, który zaznaczymy myszką, wkleimy do pliku i zapiszemy (lub dla wygody dołączamy do pliku z naszym certyfikatem w kolejności nasz certyfikat -> Certum Level I-IV -> Certum CA).

UWAGA: W celu wklejania do pliku certyfikatu prezentowanego na stronie należy skopiować fragment tekstu od linii "--BEGIN CERTIFICATE --" do "--END CERTIFICATE--".

W przypadku pobierania certyfikatów pośrednich, wybieramy interesujący nas certyfikat, np. CERTUM Level IV z listy (Certyfikaty Level IV należy pobrać w przypadku, gdy posiadamy certyfikat typu Trusted, certyfikat poziomu III należy pobrać w sytuacji, gdy posiadamy certyfikat typu Enterprise / Wildcard, certyfikat poziomu II należy pobrać w sytuacji, gdy posiadamy certyfikat typu Commercial; dla certyfikatów typu Private pobierany jest certyfikat klasy I). Pozostała część procesu (zapisanie do pliku) przebiega jak dla certyfikatu Certum CA.

4. Instalowanie klucza prywatnego i certyfikatów w Pure-FTPd

Przed instalacją certyfikatu należy usunąć hasło zabezpieczające pliku z kluczem prywatnym *server.key*:

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

Po usunięciu hasła, plik z kluczem prywatnym łączymy z paczką z certyfikatami *nr_seryjny.pem* (w której znajduje się certyfikat serwera i certyfikaty pośrednie, jeśli je wkleiliśmy wcześniej – patrz rozdział 3 wyżej):

```
cat server.key cert.txt > /etc/ssl/private/pure-ftpd.pem
```

Plik *pure-ftpd.pem* będzie umieszczony w katalogu */etc/ssl/private*. Jest to katalog domyślny, używany przez PureFTPd do przechowywania kluczy i certyfikatów (podczas instalacji można go zmienić). Po przeniesieniu pliku z certyfikatami i kluczem, należy zrestartować serwer.

5. Konfigurowanie Pure-FTPd do połączeń w otoczeniu SSL

Po zainstalowaniu biblioteki OpenSSL, wygenerowaniu kluczy i postawieniu demona FTP, należy skonfigurować serwer tak, aby umożliwić klientom bezpieczne połączenie. Jeżeli nie instalujemy VSFTPd z pakietu to pamiętajmy o zmianie następującej linijki w pliku *builddefs.h*:

```
#undef VSF_BUILD_SSL
```

na:

```
#define VSF_BUILD_SLL
```

Następnie edytujemy plik *vsftpd.conf* i dopisujemy na końcu linijkę:

```
ssl_enable=YES
```

aktywujemy konkretny protokół, np.:

```
ssl_sslv2=YES
#ssl_sslv3=YES
#ssl_tlsv1=YES
```

Domyślnie serwer będzie szukał kluczy w katalogu *certs* (w tym przypadku */usr/share/ssl/certs/vsftpd.pem*). Aby wskazać swoją ścieżkę do paczki z kluczami np. do katalogu */tmp* należy dodać poniższy wpis:

```
rsa_cert_file=/tmp/vsftpd.pem
```