

UNIZETO



POWSZECHNE
CENTRUM CERTYFIKACJI



instrukcja użytkownika

VSFTPd 2.0.1+

Użycie certyfikatów niekwalifikowanych w
oprogramowaniu VSFTPd

wersja 1.3

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	5
3. POBIERANIE CERTYFIKATÓW CERTUM CA I CERTYFIKATÓW POŚREDNICH	9
4. INSTALOWANIE KLUCZA PRYWATNEGO I CERTYFIKATÓW W VSFTPD.....	9
5. KONFIGUROWANIE VSFTPD DO POŁĄCZEŃ W OTOCZENIU SSL	10

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) [I: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-----
MIIDMCCApkCAQAwgZoxGzAZBgNVBAMTEmRsdWJhY3oudW5pemV0by5wbDEhMB8G
A1UECxMYRHppYWwgT2Nocm9ueSBJbmcZvcmlhY2ppMRswGQYDVQQKEhJVbml6ZXRv
IFNwLiB6IG8uby4xETAPBgNVBACTCFN6Y3plY2luMRswGQYDVQQIExJaYWNob2R2Ru
aW9wb2lvcnNraWUxXzAjBgNVBAYTAlBMMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQC8JvRqRPbltoZyvmJfXCef5PIcyLMQv6Z2A10j2GMoeKBCCyZF1kHoDzWW
0ZF54FrTZhyKwYqfgiHO5duLfJSBqb/PTzovZH9qXUtxl+zQIhcJnA4Z/jKyWHG1
X7LULc9u2bas/vWwQZWYvxeqNMW4RZ+LU9Qqm9b/YD2qtOZ2qwIDAQABoIIBUzAa
BgorBgEEAYI3DQIDMQwWCjUuMC4yMTk1LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYD
VR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQIC
MYHuMIHrAgEBH1oATQBpAGMAcGvBvAHMAbwBmAHQAIAbsAFMAQQAgAFMAQwBoAGEA
bgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkA
ZABLAHIDgYkAXxNuAz6gcBaZUdef8WQ2PAroKMW8sprcKv7QD2encz6/Wct9DZ5C
kGynLGy0f+Lff7ViSDJqxYWaJ68ddqgXyAqIilF63kivPTiC6yxLaNX65v3cnKfX
4UrUrGXZtub7M7/NuxSipOW0Vv7yCHganypxDyRzp6IhulEnL4APEH4AAAAAAAAA
ADANBgkqhkiG9w0BAQUFAAOBgQAsTG3Hu00fFzNTekFo/fb3tKsmuS/1rCCB5sQK
iNpWGZ8Z8+TmqBB0Tuz4FPTkeSqLpWv1ORfmxMKPIu10dC3QwRP2E//oMPnaU807
IJIDwn2VZ7qQ/h0KcWoWSPmvt7J0KKshdGgAF7P6AYc7W4yA9B9nPeyEzQRW0t4D
YBApPQ==
-----END NEW CERTIFICATE REQUEST-----
```

Po zalogowaniu do systemu CERTUM, mając wygenerowane żądanie oraz złożone zamówienie w sklepie, wypełniamy formularz zgłoszeniowy i wklejamy żądanie CSR na stronie CERTUM. W tym celu wybierz menu **Aktywacja certyfikatów**. Następnie wybierz typ certyfikatu SSL i aktywuj go przyciskiem **Aktywuj**.

Nazwa usługi	Data zamówienia	Numer zamówienia	Status płatności	Status aktywacji
Commercial SSL wydanie, Ważność : 1 rok	15 marzec 2011	ZoZE/001835/MS/15/03/2011	Oczekiwanie na płatność	Certyfikat nieaktywny

Wybierz **CSR** jako sposób dostarczenia klucza do certyfikatu. Następnie przejdź do kolejnego kroku przyciskiem **Dalej**.

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi: **Commercial SSL**
wydanie, Ważność : 1 rok

Wybierz sposób dostarczenia kluczy dla certyfikatu

Generowanie pary kluczy
 CSR

Szczegółowe informacje na temat sposobów przygotowania żądania CSR, uzyskasz w zakładce Pomoc lub za pośrednictwem operatora naszej infolinii.

Dalej >>

Wklej **żądanie CSR**, przejdź do kolejnego kroku przyciskiem **Dalej**.

Dane adresowe	Dane do certyfikatu:
Narzędzia	Kraj Polska
Newsletter	Email gguczyk@gmail.com
	Domena moja.domena.pl

Prosimy o dokładną weryfikację danych do certyfikatu. Po dokonaniu aktywacji usługi, zmiana danych nie będzie możliwa.

Struktura certyfikatu:

Podmiot E=gguczyk@gmail.com,
CN=moja.domena.pl, C=PL

Alt. nazwa podmiotu dNSName=moja.domena.pl

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 określone.

Usługi certyfikacyjne świadczone są zgodnie z zasadami określonymi w Kodeksie Postępowania Certyfikacyjnego (KPC). Ustawa przez nzwolanie, istnieje integralna, częścią niniejszego oświadczenia. Kodeks Postępowania...

Potwierdzam
oświadczenie *

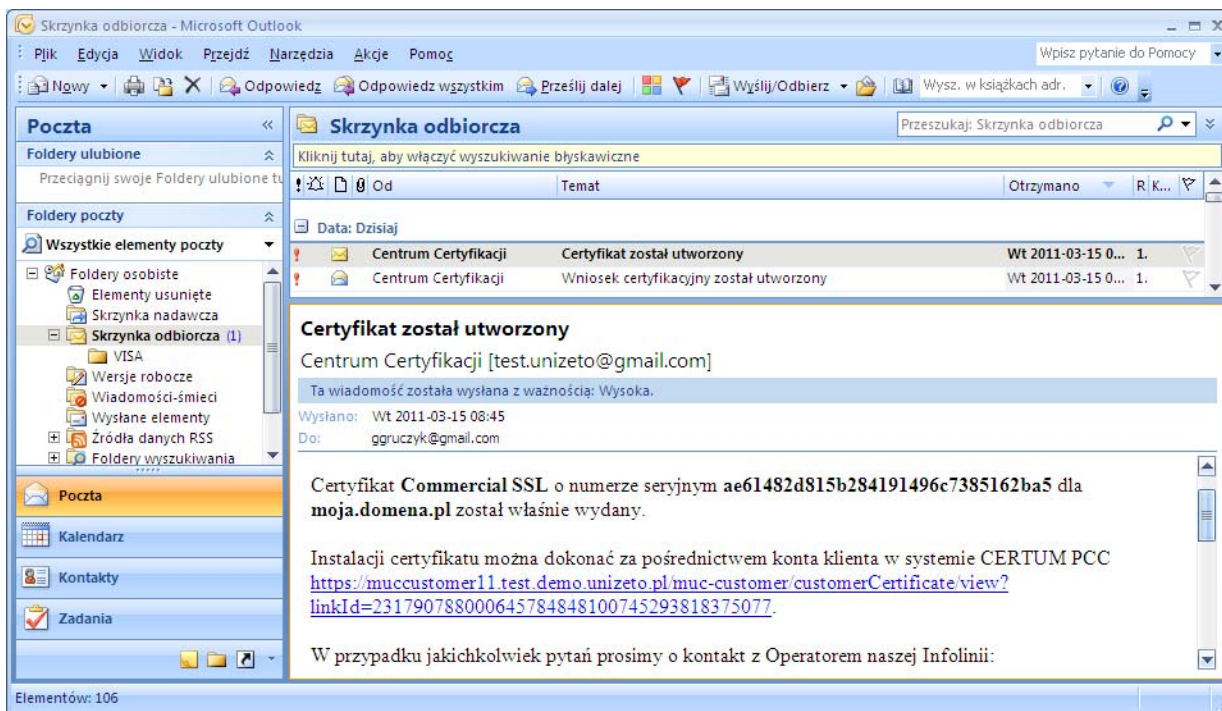
[<< Wstecz](#) [Aktywuj](#)

Żądanie certyfikatu zostało wysłane do Centrum Certyfikacji. Na konto email podane w żądaniu zostaną przesłane informacje dalszego postępowania.

2.3. Importowanie certyfikatów

Po wykonaniu powyższej procedury z poprzedniego punktu otrzymamy stosownego e-maila z linkiem instalacyjnym umożliwiającym aktywację certyfikatu (umieszczenie certyfikatu w naszym repozytorium dostępnym na stronach www).

W tym celu należy odebrać email a następnie postępować zgodnie z treścią wiadomości.



Po kliknięciu na link instalacyjny, na ekranie pojawi się strona WWW.

The screenshot shows the 'Certyfikat' (Certificate) page in the Certum portal. On the left is a navigation menu with options like 'Kody elektroniczne', 'Aktywacja certyfikatów', and 'Zarządzanie certyfikatami'. The main content area displays the following certificate details:

- Numer seryjny: ae61482d815b284191496c7385162ba5
- Skrót z certyfikatu: cHBj9v646gtvmswzDmNcR9Z84WY=
- Podmiot: E=ggruczyk@gmail.com, CN=moja.domena.pl, C=PL
- Alt. nazwa podmiotu: dNSName=moja.domena.pl
- Ważny od: 15 marzec 2011 08:43:10
- Ważny do: 14 marzec 2012 08:43:10
- Czas utworzenia: 2011-03-15
- Wystawca: CN=Certum Level II CA, OU=Certum Certification Authority, O=Unizeto Technologies S.A., C=PL
- Status: Ważny

At the bottom of the details, there are three buttons: 'Zainstaluj własny', 'Zapisz binarnie', and 'Zapisz tekstowo'.

Zapisz certyfikat w postaci binarnej *.cer lub tekstowej *.pem

UWAGA: W przypadku utraty pliku z certyfikatem, możemy ją pobrać ze strony www.certum.pl -> Narzędzia -> Certyfikaty.

The screenshot shows the 'Certyfikaty' (Certificates) page. It features a search form with the following fields:

- Email: ggruczyk@gmail.com
- Numer seryjny: ae61482d815b284191496c7385162ba5

A 'Szukaj' (Search) button is located below the search fields. Below the search form is a table listing certificates:

Nr seryjny	Profil certyfikatu	Podmiot	Ważny od	Ważny do	Status
ae61482d815b284191496c7385162ba5	Commercial SSL	E=ggruczyk@gmail.com, CN=moja.domena.pl, C=PL	15 marzec 2011 08:43:10	14 marzec 2012 08:43:10	Ważny

Below the table, there is a detailed view of the selected certificate, showing its fields (E, CN, C, dNSName) and two buttons: 'Zapisz binarnie' and 'Zapisz tekstowo'.

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

Nr seryjny	Profil certyfikatu	Podmiot	Ważny od	Ważny do	Status
ae61482d815b284191496c7385162ba5	Commercial SSL	E=ggruczyk@gmail.com, CN=moja.domena.pl, C=PL	15 marzec 2011 08:43:10	14 marzec 2012 08:43:10	Ważny 

E	ggruczyk@gmail.com	
CN	moja.domena.pl	
C	PL	
dNSName	moja.domena.pl	

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*.

Wyświetli 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 SSL, certyfikat poziomu III należy pobrać w sytuacji, gdy posiadamy certyfikat typu Trusted SSL / Trusted Wildcard SSL, certyfikat poziomu II należy pobrać w sytuacji, gdy posiadamy certyfikat typu Commercial SSL; 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 umożliwił 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
```