

UNIZETO



POWSZECHNE
CENTRUM CERTYFIKACJI



instrukcja użytkownika

POSTFIX (SMTP) + POP3 + SSL

Użycie certyfikatów niekwalifikowanych
w oprogramowaniu POSTFIX

wersja 1.4

Spis treści

1. WSTĘP.....	3
2. TWORZENIE KLUCZY I CERTYFIKATU DLA DEMONÓW SMTP I POP3	3
2.1. GENEROWANIE WNIOSKU O CERTYFIKAT (CSR)	3
2.2. TWORZENIE CERTYFIKATU NA PODSTAWIE UTWORZONEGO ŻĄDANIA (CSR)	5
2.3. IMPORTOWANIE CERTYFIKATÓW	7
3. INSTALOWANIE KLUCZY I CERTYFIKATU SERWERA ORAZ CERTYFIKATÓW CERTUM CA. 9	9
3.1. INSTALOWANIE KLUCZY I CERTYFIKATÓW W POSTFIX	9
3.2. INSTALOWANIE KLUCZY I CERTYFIKATÓW W POP3S	9
4. KONFIGUROWANIE POSTFIX DO OBSŁUGI PROTOKOŁU SMTP W OTOCZENIU SSL	10
5. EKSPORT KLUCZY (DO PACZKI PFX).....	10

1. Wstęp

Postfix jest zaawansowanym serwerem pocztowym, przeznaczonym głównie na platformę Unix. Dzięki wbudowanym mechanizmom bezpieczeństwa potrafi nawiązać szyfrowane i autoryzowane połączenie za pomocą protokołu TLS z drugim serwerem SMTP, lub klientem poczty elektronicznej, umożliwiając w ten sposób bezpieczną wymianę informacji.

Niniejszy dokument zawiera instrukcję generowania unikalnej pary kluczy oraz CSR, dla serwera Postfix. Więcej informacji znajdziecie Państwo na oficjalnych stronach projektu: www.postfix.org.

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

- Serwer MTA Postfix – www.postfix.org
- Demon POP3 – tutaj w postaci pakietu `imap-2002d-2.src.rpm`
- Biblioteka OpenSSL – www.openssl.org

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

Zanim zabierzemy się za konfigurowanie bezpiecznych połączeń pocztowych przekonajmy się czy:

- Serwer DNS jest odpowiednio skonfigurowany (dodany wpis MX).
- Sendmail jest skonfigurowany z protokołem SMTP.
- Sendmail jest zintegrowany z agentem POP3 (lub IMAP) z paczki IMAP.
- Dodani zostali użytkownicy poczty wraz z hasłami (`addusr/passwd`).
- Klient poczty jest skonfigurowany.

... i czy cały mechanizm działa poprawnie.

[Przy pisaniu tej instrukcji, Autor korzystał z dystrybucji: Red Hat Enterprise Linux 4.](#)

2. Tworzenie kluczy i certyfikatu dla demonów SMTP i POP3

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>.

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
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:
OpenSSL> █
```

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

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 zostanie 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:

- **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.
- **City or 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.mojserwer.pl`, `mojadomena.pl`, `*.mojserwer.pl`.

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

Pamiętajmy, że w pole **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) [GB]:PL
State or Province Name (full name) [Berkshire]:Zachodniopomorskie
Locality Name (eg, city) [Newbury]:Szczecin
Organization Name (eg, company) [My Company Ltd]:Moja Firma
Organizational Unit Name (eg, section) []:Oddział w Moja Firma
Common Name (eg, your name or your server's hostname) []:poczta.mojserwer.pl
```


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.moja.domena.pl upewnijmy się, że ta nazwa widnieje w tym polu)!!!

Upewniwszy się co do poprawności wprowadzonych danych należy potwierdzić załączone oświadczenie klikamy **Aktywuj**.

Dane adresowe

Narzędzia

Newsletter

Dane do certyfikatu:

Kraj Polska

Email ggruczyk@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=ggruczyk@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 POWINIENIŚ 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 (KDC). Ustawa przez nrzwzwołania.etstie.sie.integralna.czećria.niniateczano.oświadczenia_Kodeks.Postępowania

Potwierdzam oświadczenie *

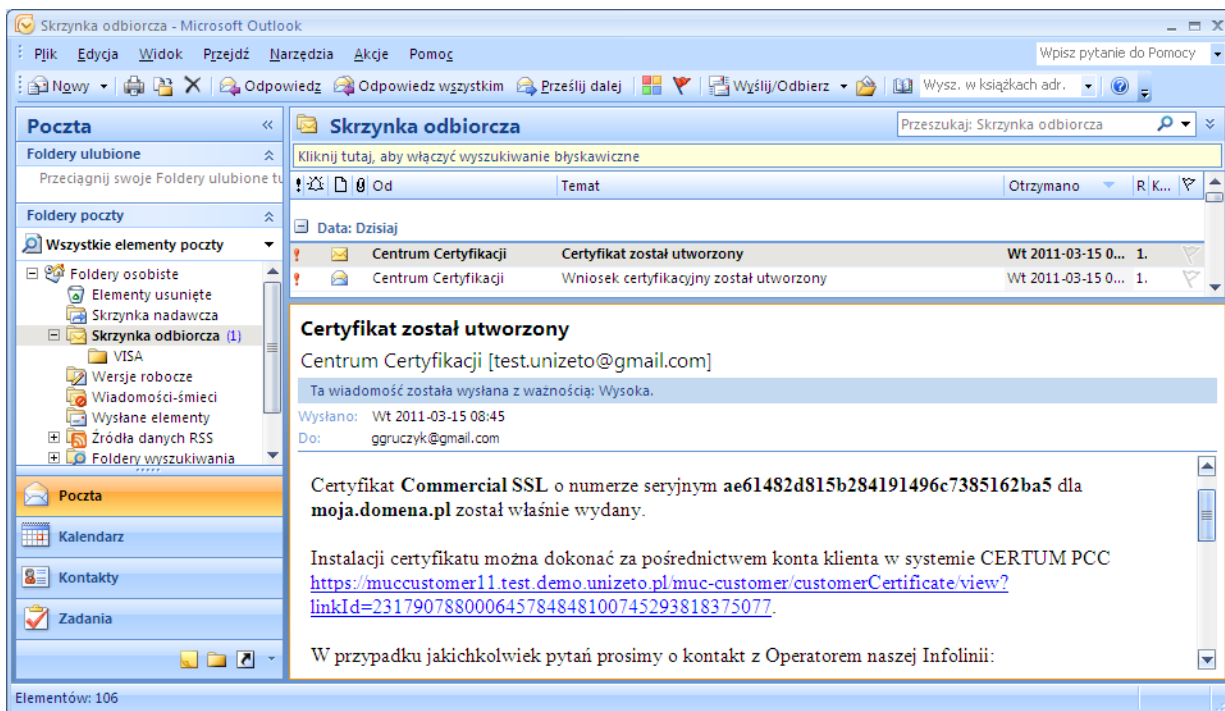
<< Wstecz Aktywuj

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

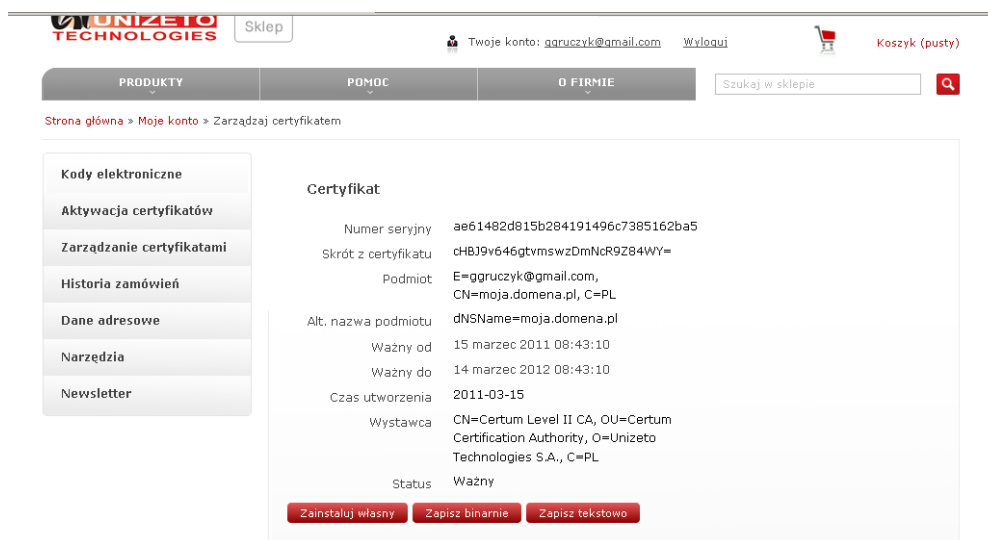
2.3. Importowanie certyfikatów

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.



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

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. Instalowanie kluczy i certyfikatu serwera oraz certyfikatów Certum CA

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. Możemy dodać nasz certyfikat na początku pliku *ca-bundle.crt* (od linii "--BEGIN CERTIFICATE --" do "--END CERTIFICATE--")

3.1. Instalowanie kluczy i certyfikatów w Postfix

Do pobranej/utworzonej paczki certyfikatów pozostaje dodać klucz prywatny. Aby tego dokonać wydajemy polecenia:

```
#mv ca-bundle.crt temp.crt
#cat server.key temp.crt > ca-bundle.crt
```

Polecenie spowoduje dopisanie klucza prywatnego do zbioru certyfikatów i zapisanie wyniku do pliku *ca-bundle.crt*, który należy umieścić (wg konfiguracji) w */etc/postfix*. Plik *temp.crt* można usunąć.

Pamiętajmy, aby klucz prywatny nie miał postaci zaszyfrowanej!!!

Aby zdjąć hasło z klucza prywatnego, należy wydać polecenie:

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

Restartujemy serwer poleceniem:

```
#postfix restart
```

Instalacja klucza prywatnego, certyfikatu serwera, certyfikatu Certum CA i certyfikatów pośrednich została zakończona pomyślnie.

3.2. Instalowanie kluczy i certyfikatów w POP3S

W celu instalacji kluczy i certyfikatów należy dodać klucz prywatny (*server.key*) oraz pobrany/utworzony plik z certyfikatami serwera i Certum (*ca-bundle.crt*) dopisać do pliku *ipop3d.pem* (przy instalacji paczki należy podać ścieżkę dla tego pliku).

UWAGA!!! Należy pamiętać, aby klucz prywatny nie był w postaci zaszyfrowanej:

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

Restartujemy serwer pop3s:

```
#xinetd restart
```

Instalacja klucza prywatnego, certyfikatu serwera, certyfikatu Certum CA i certyfikatów pośrednich została zakończona pomyślnie.

4. Konfigurowanie Postfix do obsługi protokołu SMTP w otoczeniu SSL

W celu instalacji kluczy i certyfikatów w Postfix edytujemy plik *master.cf* i odkomentowujemy linijki wymuszające uwierzytelnianie i bezpieczne połączenie:

```
smtps inet n - n - -smtpd -o smtpd_tls_wrappermode=yes -o  
smtpd_sasl_auth_enable=yes  
submission inet n - n - -smtpd -o smtpd_enforce_tls=yes -o  
smtpd_sasl_auth_enable=yes -o smtpd_etrn_restrictions=reject
```

W pliku *main.cf* definiujemy ścieżkę do pliku z kluczem i certyfikatami:

```
smtpd_tls_cert_file = /etc/postfix/ca-bundle.crt  
smtpd_tls_key_file = $smtpd_tls_cert_file
```

W tym przypadku wszystkie potrzebne komponenty umieszczane są w jednym pliku (*ca-bundle.crt*). Postfix odczyta je w następującej kolejności:

- klucz prywatny serwera (niezaszyfrowane)
- certyfikat serwera
- certyfikaty pośrednie (w praktyce potrzebny jest tylko ten certyfikat pośredni, który odpowiada klasą certyfikatowi naszego serwera np. Certum Level IV – dla certyfikatu Trusted SSL)
- główny certyfikat Certum CA

5. Eksport kluczy (do paczki pfx)

Aby wyeksportować klucz i certyfikat z serwera po prostu kopiujemy pliki z kluczem prywatnym *server.key* i certyfikatem *server.crt* w bezpieczne miejsce. Aby utworzyć z tych plików paczkę *pfx* należy z poziomu Openssl-a wpisać:

```
OpenSSL> pkcs12 -export -out klucze.p12 -inkey server.key -in server.crt  
Enter Export Password:  
Verifying - Enter Export Password:  
OpenSSL> █
```