

UNIZETO



POWSZECHNE  
CENTRUM CERTYFIKACJI



instrukcja użytkownika

# SENDMAIL (SMTP) + POP3 + SSL

Użycie certyfikatów niekwalifikowanych  
w oprogramowaniu Sendmail

wersja 1.2

# Spis treści

<b>1. WSTĘP.....</b>	<b>3</b>
<b>2. TWORZENIE KLUCZY I CERTYFIKATU DLA DEMONÓW SMTP I POP3.....</b>	<b>3</b>
2.1. GENEROWANIE WNIOSKU O CERTYFIKAT (CSR).....	3
2.2. TWORZENIE CERTYFIKATU NA PODSTAWIE UTWORZONEGO ŻĄDANIA (CSR) .....	5
2.3. POBIERANIE CERTYFIKATÓW CERTUM CA I CERTYFIKATÓW POŚREDNICH.....	6
2.4. INSTALOWANIE CERTYFIKATÓW POŚREDNICH I CERTUM CA.....	7
2.5. POBIERANIE CERTYFIKATU SERWERA.....	7
2.6. INSTALOWANIE KLUCZA PRYWATNEGO SERWERA .....	8
2.7. INSTALOWANIE CERTYFIKATU SERWERA.....	9
<b>3. KONFIGUROWANIE SENDMAILA DO OBSŁUGI SMTP W OTOCZENIU SSL.....</b>	<b>9</b>
<b>4. UWIERZYTELNIANIE WZGLĘDEM SERWERA NA PODSTAWIE CERTYFIKATU KLIENTA.....</b>	<b>9</b>
<b>5. KONFIGUROWANIE DEMONA POP3 DO OBSŁUGI W OTOCZENIU SSL.....</b>	<b>10</b>
5.1. INSTALOWANIE KLUCZA PRYWATNEGO W POP3S.....	10
5.2. INSTALOWANIE CERTYFIKATU SERWERA W POP3S .....	10
5.3. INSTALOWANIE CERTYFIKATU CERTUM CA I CERTYFIKATU POŚREDNIEGO.....	10
<b>6. EKSPORT KLUCZY I CERTYFIKATÓW.....</b>	<b>10</b>

## 1. Wstęp

Sendmail/TLS jest zaawansowanym wrapperem SMTP, przeznaczonym na profesjonalną platformę Unix. Umożliwia nawiązanie bezpiecznego i autoryzowanego połączenia za pomocą protokołu TLS z klientem poczty elektronicznej. Dokument ten zawiera instrukcję generowania unikalnej pary kluczy oraz żądania certyfikatu (CSR), dla serwera Sendmail i demona POP3. Więcej informacji znajdziesz na oficjalnych stronach projektu Sendmail ([www.sendmail.org](http://www.sendmail.org)).

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

- Serwer MTA Sendmail – [www.sendmail.org](http://www.sendmail.org)
- Demon POP3 – tutaj w postaci pakietu `imap-2002d-2.src.rpm`
- Biblioteka OpenSSL – [www.openssl.org](http://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 dla Sendmaila (i agenta POP3), 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 dyskietce 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, Koźnia 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.plm \*.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
```



**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](http://poczta.mojserwer.com) upewnijmy się, że ta nazwa widnieje w tym polu)!!!

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

### Pobierz certyfikat Private SSL 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**

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

## 2.3. Pobieranie certyfikatów Certum CA i certyfikatów pośrednich

Aby pobrać certyfikat Certum CA lub certyfikaty pośrednie należy wejść na stronę [www.certum.pl](http://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 urządzeń sieciowych	<input type="button" value="Instaluj"/>

[do góry](#)

Wyświetlił się interesujący nas certyfikat, który zaznaczymy myszką, wkleimy do pliku i zapiszemy.

**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.

## 2.4. Instalowanie certyfikatów pośrednich i Certum CA

W paczce *ca-bundle.crt* (dostępnej pod adresem: <http://www.certum.pl/keys/ca-bundle.crt>), 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 CERTUM 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 (zdefiniowanego w pliku *sendmail.mc*), np.:

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

Restartujemy serwer poleceniem:

```
#sendmail restart
```

Instalacja certyfikatu, CERTUM CA i certyfikatów pośrednich została zakończona pomyślnie.

## 2.5. Pobieranie certyfikatu serwera

Po wykonaniu powyższych czynności możemy wejść na stronę, której adres otrzymaliśmy pocztą elektroniczną i aktywować certyfikat (umieścić certyfikat 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:

### Instalacja certyfikatu

<b>Private SSL Server</b>	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 ją pobrać ze strony [www.certum.pl](http://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*:

## Wyszukaj certyfikat (niekwalifikowany)

<b>Private SSL Server</b>	Ważny do: 17-06-2007	
Podmiot: 10.100.10.122		
Numer: 0x37D85		
Status: <b>Ważny</b>		
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.

## 2.6. Instalowanie klucza prywatnego serwera

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.:

```
/usr/share/ssl/certs/server.key
```

Zdejmujemy hasło z klucza prywatnego, aby klucz prywatny nie był w formie zaszyfrowanej (nieczytelnej dla niektórych wersji Sendmaila) :

```
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:

```
#chmod 400 /etc/share/ssl/certs/server.key
```

Właścicielem pliku *server.key* powinien być *root*.

Po tych czynnościach restartujemy serwer poleceniem:

```
#sendmail restart
```

Instalacja klucza prywatnego została zakończona pomyślnie.

## 2.7. Instalowanie certyfikatu serwera

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

```
/usr/share/ssl/certs/server.crt
```

Po tych czynnościach restartujemy serwer poleceniem:

```
#sendmail restart
```

Instalacja certyfikatu serwera została zakończona pomyślnie.

**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 *sendmail.mc*:

```
define(`confCACERT_PATH',`/usr/share/ssl/certs')dnl
define(`confCACERT',`/usr/share/ssl/certs/ca-bundle.crt')dnl
define(`confSERVER_CERT',`/usr/share/ssl/certs/ca-bundle.crt')dnl
define(`confSERVER_KEY',`/usr/share/ssl/certs/ca-bundle.crt')dnl
```

**W tym przypadku klucz prywatny musi znajdować się na pierwszym miejscu w paczce *ca-bundle.crt*!**

## 3. Konfigurowanie Sendmaila do obsługi SMTP w otoczeniu SSL

W celu instalacji kluczy i certyfikatów w Sendmailu edytujemy plik *sendmail.mc* i odkomentowujemy linijki:

- wymuszające bezpieczne połączenie:

```
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS',`EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5
LOGIN PLAIN')dnl
```

- ścieżkę oraz pliki z kluczami:

```
define(`confCACERT_PATH',`/usr/share/ssl/certs')dnl
define(`confCACERT',`/usr/share/ssl/certs/ca-bundle.crt')dnl
define(`confSERVER_CERT',`/usr/share/ssl/certs/server.crt')dnl
define(`confSERVER_KEY',`/usr/share/ssl/certs/server.key')dnl
```

- nasłuchiwanie serwera na porcie smtps (465):

```
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTPA, M=s')dnl
```

## 4. Uwierzytelnianie względem serwera na podstawie certyfikatu klienta

Szczegółowe informacje na ten temat znaleźć można poprzez serwis <http://www.sendmail.org/~ca/email/starttls.html#STARTTLS>

## 5. Konfigurowanie demona POP3 do obsługi w otoczeniu SSL

Aby klienci mogli odbierać pocztę korzystając z bezpiecznego połączenia należy skonfigurować demona POP3 do obsługi certyfikatów CERTUM.

### 5.1. Instalowanie klucza prywatnego w POP3S

Aby zainstalować klucz prywatny należy do pliku *ipop3d.pem* (przy instalacji paczki należy podać ścieżkę dla tego pliku – w przeciwnym razie zostanie zainstalowany domyślnie) skopiować plik z kluczem prywatnym *server.key*.

**UWAGA:** Należy wcześniej zdjąć hasło z klucza prywatnego:

```
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>
```

### 5.2. Instalowanie certyfikatu serwera w POP3S

W celu zainstalowania certyfikatu serwera należy dodać do pliku *ipop3d.pem* (używając polecenia *cat*) certyfikat naszego serwera *server.crt*.

### 5.3. Instalowanie certyfikatu CERTUM CA i certyfikatu pośredniego

Aby zainstalować certyfikat CERTUM CA i certyfikat pośredni należy dodać do pliku *ipop3d.pem* (używając polecenia *cat*) kolejno:

- certyfikat pośredni odpowiadający klasie certyfikatu naszego serwera np. CERTUM Level II
- certyfikat główny CERTUM CA, który "wydał" certyfikaty pośrednie

Restartujemy serwer pop3s:

```
#xinetd restart
```

## 6. Eksport kluczy i certyfikatów

Aby wyeksportować klucz i certyfikat z serwera należy skopiować pliki z kluczem prywatnym *server.key* i certyfikatem *server.crt* w bezpieczne miejsce. Aby utworzyć z tych plików paczkę pfx należy wykonać polecenie:

```
openssl pkcs12 -export -out klucze.p12 -inkey server.key -in server.crt
```

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

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