

UNIZETO



POWSZECHNE  
CENTRUM CERTYFIKACJI



instrukcja użytkownika

# Exchange 2007

Konfiguracja protokołu SSL/TLS w serwerze  
pocztowym Exchange 2007

wersja 1.0

# Spis treści

1. GENEROWANIE ŻĄDANIA WYSTAWIENIA CERTYFIKATU .....	3
2. WYSYŁANIE ŻĄDANIA DO CERTUM .....	4
3. INSTALACJA CERTYFIKATÓW POŚREDNICH.....	6
4. INSTALACJA CERTYFIKATU .....	8
5. WYKONYWANIE KOPII ZAPASOWEJ CERTYFIKATU I KLUCZA PRYWATNEGO .....	9

## 1. Generowanie żądania wystawienia certyfikatu

Domyślnie serwer pocztowy Exchange 2007 używa certyfikatu wystawionego samemu sobie. Możliwe jest jednak skonfigurowanie certyfikatu uzyskanego od zaufanego centrum certyfikacji. Aby skonfigurować własny certyfikat należy wygenerować nowe żądanie. Należy otworzyć wiersz zarządzania serwera Exchange (Exchange Management Shell). Należy wpisać następującą komendę:

```
New-ExchangeCertificate -generaterequest -subjectname  
"o=Unizeto Technologies S.A.,ou=Bajeczna,cn=win2008.certum.local" -  
PrivateKeyExportable $true -path c:\win2008.certum.local.csr
```

Znaczenie poszczególnych parametrów jest następujące:

- `generaterequest` – oznacza wygenerowanie nowego żądania i pary kluczy,
- `subjectname` – tutaj powinny zostać wpisane parametry, jakie wystąpią w certyfikacie.

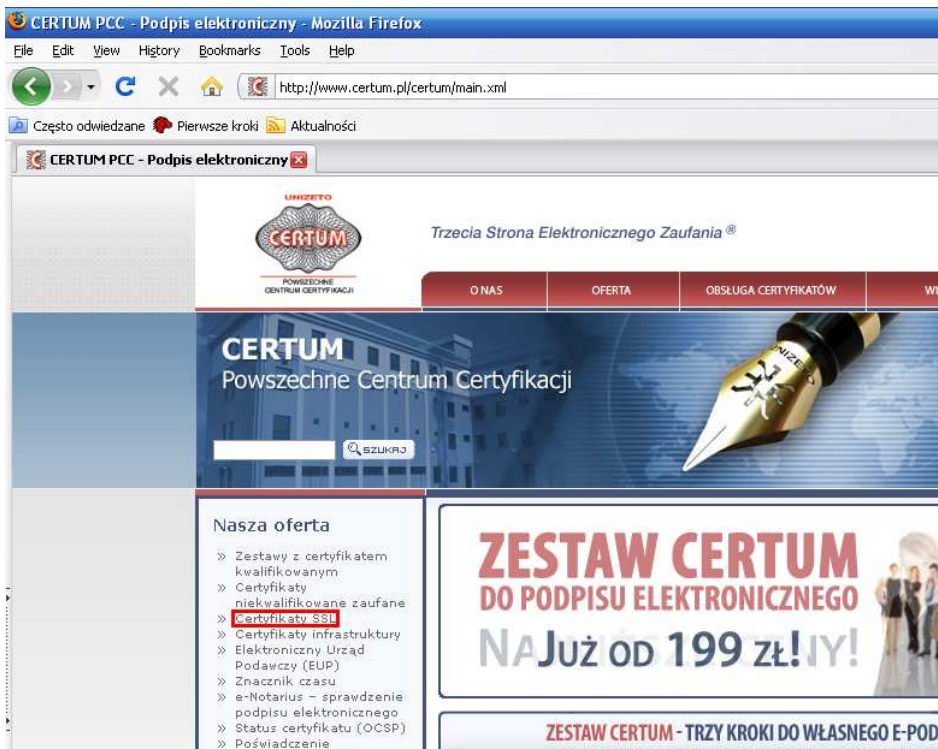
**Uwaga:** Należy używać znaków z zestawu ASCII (bez polskich znaków diakrytycznych).

Nie wszystkie pola są obowiązkowe. Zależnie od klasy zakupionego certyfikatu w mogą znaleźć się różne zestawy pól. W tym przypadku są to:

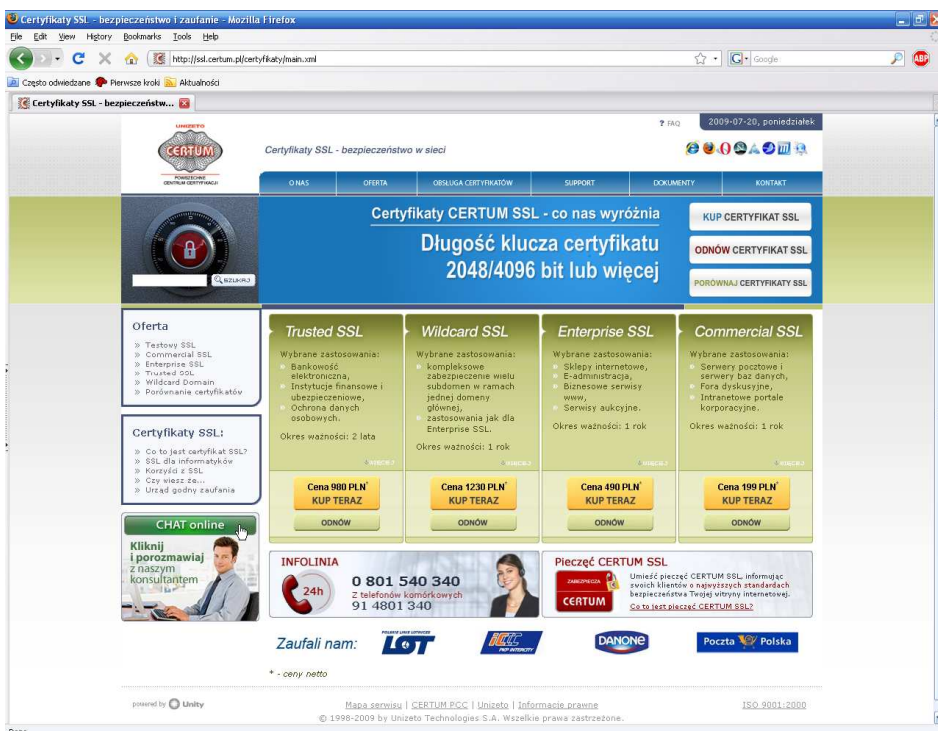
- `o` – nazwa organizacji, jaka zostanie umieszczona w certyfikacie, w tym przypadku Unizeto Technologies S.A.
- `ou` – jednostka organizacyjną w firmie. Może to być np. „Dział sprzedaży”
- `cn` – nazwa powszechna. Najważniejsze pole. Zawiera nazwę domeny pod jaką widoczny jest serwer poczty w Internecie.
- Inne pola. Opis, jakie pola można umieścić w żądaniu znajdują się na stronie MSDN:  
<http://technet.microsoft.com/en-us/library/aa998840.aspx>
- `PrivateKeyExportable $true` – zaznacza generowaną parę kluczy jako eksportowalną. Oznacza to, że można wykonać kopię zapasową klucza prywatnego i certyfikatu bez użycia dodatkowych narzędzi.
- `path` – ścieżka do pliku, w którym zostanie zapisane żądanie wystawienia certyfikatu.

## 2. Wysłanie żądania do CERTUM

Po wygenerowaniu żądania należy wysłać je do CERTUM celem uzyskania certyfikatu. Proszę wejść na stronę certum.pl i wybrać „Certyfikaty SSL”:



Zostanie zaprezentowana oferta CERTUM. Proszę zapoznać się z naszą ofertą i wybrać typ certyfikatu, który najlepiej będzie pasował do Państwa potrzeb.



Proszę kliknąć na przycisk „Kup teraz” przy wybranym typie certyfikatu i zalogować się na naszym portalu. Jeśli nie posiadają Państwo konta na naszym portalu proszę je utworzyć i zalogować się.

W kolejnym kroku wypełnia się pola związane z zamówieniem certyfikatu.

Strona główna > Obsługa certyfikatów > Kup certyfikat Enterprise SSL (niekwalifikowany)

### Kup certyfikat Enterprise 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](#))

```
-----BEGIN NEW CERTIFICATE REQUEST-----
BDATBgNVHSUEDDAKBggrBgEFBQcDATB4BgkqhkiG9w0BCQ8EazBpMA4GCCqGSIb3
DQMCAsIAgDAOBggqhkiG9w0DBAICAIAwCwYJYIZIAW UDBAEqMAsGCW CGSAFIawQB
LTALBgghkgBZQMEAsIwCwYJYIZIAW UDBAEFMAsGBSsOAwIHMAoGCCqGSIb3DQMH
MB0GA1UdDgQW BBS6ZvbFEYh vTVDtnrEGbZe abnXLp DANBgkqhkiG9w0BAQUFAAO
AQEANKAe xHCqQch ZtEOOW /vBTAdIrvZa5kLRIDi5VW bOEDPbTgfemjBhI1VaXcFI
kHt7Kp2FXVeAajGILu7h5/Z7GJM8kjMHb xXDkEaZnsDYICR 7TtWJDz bOk118n4nFT
8IgAbJnTfXupASAw/gd49BEs3cJR/X/hcQUdppYRhtkKpJ/AbZpVZh97uBb0/LCu
5+0EyIfDStRcZHU5ohK7SKW YGpn5V2yDf0E6tkXDp9GraG2vV44cujiCtqav+oZ
HZGRu5uJICRnmNCwMtoIMZ64tVI2SsAJ6wCm uMfn9Z+tMWIXR93itrTHOk e r7Mtw
R YUIE2zDdSgvNQ8uc0eaj3rVYA=
-----END NEW CERTIFICATE REQUEST-----
```

**Uwaga!**  
W żądaniach CSR klucze kryptograficzne muszą być długości co najmniej 2048 bit (dla algorytmów RSA lub DSA) oraz 571 bit (dla algorytmów EC: NIST K-571 oraz NIST B-571). Żądania CSR z kluczami kryptograficznymi o długości krótszej niż wymienione powyżej nie zostaną przyjęte do realizacji.

**Adres email**

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

E-mail:

**Dane do faktury**

Nazwa:

NIP:

Ulica i nr:

Kod:

Miasto:

Najważniejszym polem jest „Żądanie certyfikatu”. Należy wkleić tutaj żądanie wygenerowane w punkcie poprzednim. Proszę otworzyć plik z żądaniem w edytorze tekstu (Notatnik, Notepad++) i skopiować cały ciąg znaków od „-----BEGIN NEW CERTIFICATE REQUEST-----” oraz „-----END NEW CERTIFICATE REQUEST-----”.

**Uwaga:** Należy skopiować cały ciąg, łącznie z wyżej wymienionymi ciągami znaków.

**Uwaga!** Exchange 2007 generuje żądanie z przerwą przed znacznikiem -----END NEW CERTIFICATE REQUEST----- . Należy usunąć tą przerwę.

Następnie proszę uzupełnić dane do faktury – będą one potrzebne do wystawienia faktury. Proszę nie zapomnieć o podaniu adresu e – mail. Będą na niego przesyłane wszelkie informacje związane z obsługą certyfikatów. Może to być np. wiadomość z linkiem aktywacyjnym albo przypomnienia o wygasaniu certyfikatu.

W kolejnym kroku proszę wybrać formę płatności, przeczytać uważnie oświadczenie a następnie je zaakceptować. Na koniec proszę wcisnąć przycisk „Dalej”.

Miasto:

---

**– Proszę wybrać formę płatności**

Kwotę 597.80PLN (490PLN + 22% VAT) zapłać przelewem internetowym (eCard)  
 Kwota została uregulowana za pomocą karty aktywacyjnej  
 Kwotę 597.80PLN (490PLN + 22% VAT) zapłać przelewem tradycyjnym

---

**– Oświadczenie**

ZANIM ZŁOŻYSZ WNIOSEK O WYDANIE CERTYFIKATU, POTWIERDZISZ GO, BĄDŹ UŻYJESZ DO REALIZACJI PIERWSZEGO PODPISU POWINIENES 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.

Potwierdzam oświadczenie

---

Następnym krokiem będzie weryfikacja domeny. Można tego dokonać w dwojaki sposób. Pierwszy sposób polega na weryfikacji domeny i adresu e – mail. Weryfikacja domeny polega na umieszczeniu specjalnego znacznika na weryfikowanej stronie. Weryfikacja adresu e – mail polega na kliknięciu w specjalny odnośnik w wiadomości przesłanej na podany adres e – mail.

Drugi sposób weryfikacji to przesłanie dokumentów. Osoba prowadząca proces uzyskania certyfikatu przesyła dokumenty, na podstawie których CERTUM można zweryfikować przynależność domeny do organizacji.

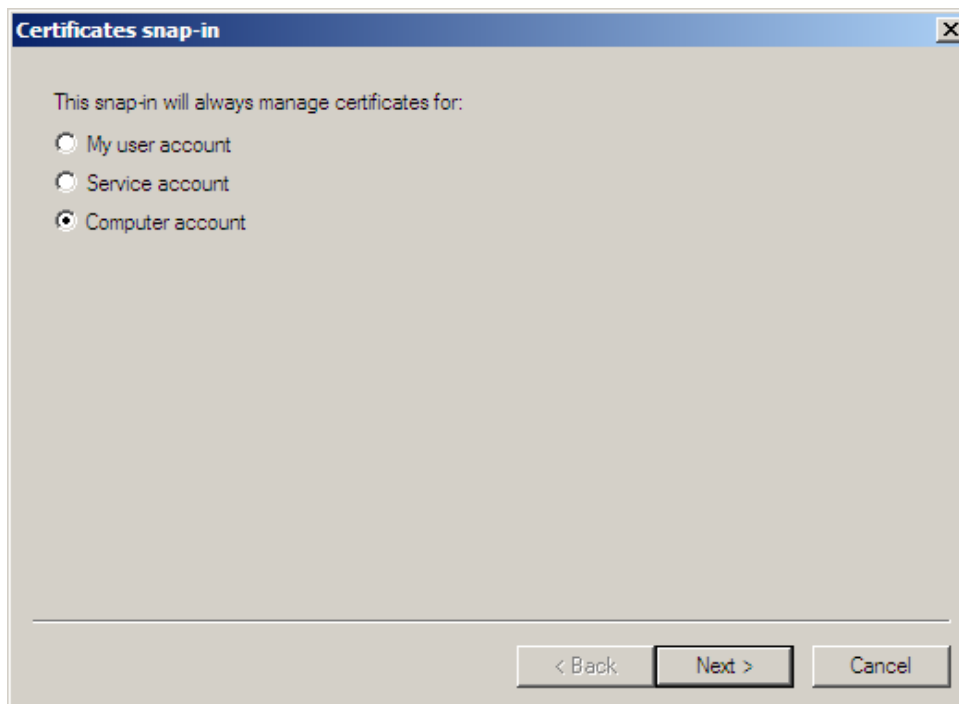
### 3. Instalacja certyfikatów pośrednich

Bardzo ważnym elementem są certyfikaty urzędów pośrednich. Należy je zainstalować na serwerze WWW aby przeglądarka internetowa poprawnie zweryfikowała wystawcę certyfikatu.

Proszę wejść na stronę [certum.pl](http://certum.pl) i z górnego menu wybrać „Obsługa certyfikatów” a następnie „Zaświadczenia i klucze”. Proszę zapisać certyfikaty urzędów Certum Level I CA, Certum Level II CA, Certum Level III CA oraz Certum Level IV CA. Proszę wybrać certyfikaty dla serwerów SSL/TLS.

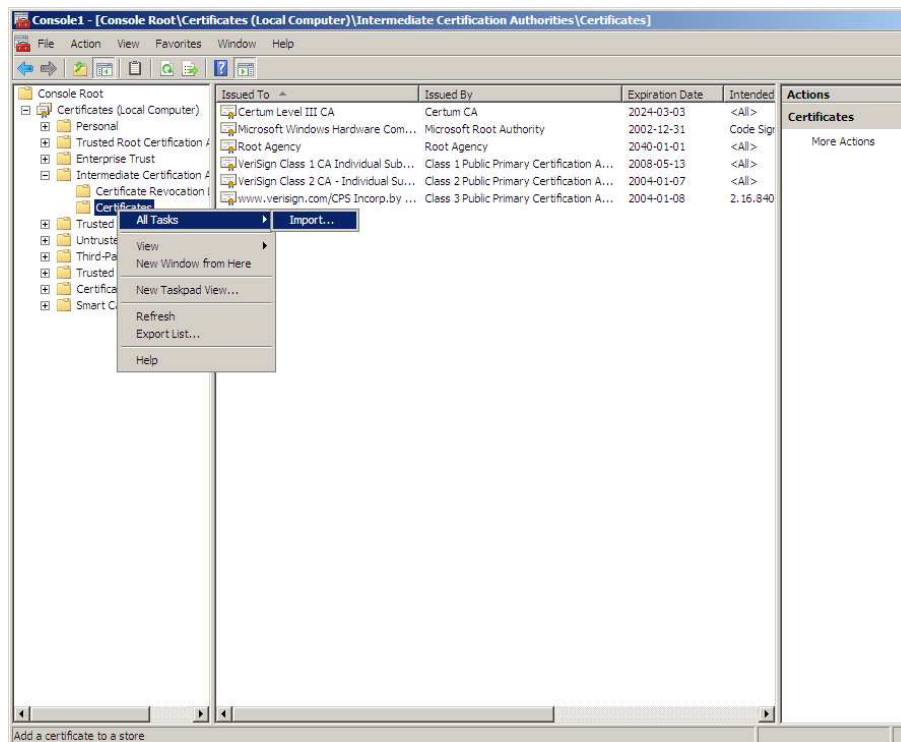
Proszę wcisnąć kombinację klawiszy [WinKey + R] wpisać polecenie `mmc.exe`. Zostanie uruchomiony edytor przystawek MMC. Z menu „Plik” należy wybrać pozycję „Dodaj/Usuń przystawkę”. W nowym oknie trzeba kliknąć przycisk „Dodaj” a następnie wskazać przystawkę „Certyfikaty” i wcisnąć przycisk „Dodaj”.

Pojawi się okno podobne do następującego:



Proszę wybrać opcję Konta komputera (ang. „Computer account”) i kliknąć przycisk „Dalej”. Na następnym ekranie proszę wskazać komputer lokalny i kliknąć przycisk „Zakończ”.

W lewym panelu nowo otwartego okna proszę rozwinąć gałąź „Certyfikaty urzędów pośrednich”. Proszę kliknąć prawym przyciskiem myszy na folder „Certyfikaty” i z menu kontekstowego wybrać pozycję „Wszystkie zadania” a następnie „Importuj...”.



Kreator poprowadzi Administratora poprzez proces instalacji certyfikatów pośrednich. Należy wskazać certyfikat urzędu Certum Level I CA i jako magazyn do instalacji wybrać „Pośrednie urzędy certyfikacji” (taki powinien być domyślny wybór).

Opisane wyżej kroki należy powtórzyć dla certyfikatów urzędów Cetum Level II CA, Cetum Level III CA, oraz Cetum Level IV CA.

## 4. Instalacja Certyfikatu

Po poprawnej weryfikacji otrzymają Państwo wiadomość e – mail z ID instalacyjnym. Będzie ona podobna do wiadomości przedstawionej na poniższej grafice:

```
Szanowni Państwo,  
  
Dokumenty do certyfikatu klasy 3.2 "Enterprise Web Server"  
zostały zweryfikowane, certyfikat został wygenerowany  
i jest gotowy do pobrania.  
  
Dane certyfikatu:  
+-----+  
Nr seryjny: 0x4A6AF  
Podmiot: win2008.certum.local  
Firma: Unizeto Technologies S.A.  
  
Ważny od: 17-07-2009 14:01:44  
Ważny do: 17-07-2010 14:01:44  
+-----+  
  
ID instalacyjne certyfikatu: 87d69e4819ad2a82087b74b0ae5199e52c5bcef6  
  
Proszę wkleić ID na stronie:  
https://www.certum.pl/install/  
  
--  
Zespół Unizeto CA  
info@certum.pl
```

Aby aktywować certyfikat proszę wejść na stronę podaną w wiadomości i wkleić ID instalacyjne certyfikatu. Po wciśnięciu przycisku „Aktywuj” pojawi się nowa strona, z której można pobrać gotowy certyfikat. Proszę zapisać certyfikat na dysk wybierając opcję „Zapisz binarnie” i zapisać certyfikat na dysk twardy serwera.

Kolejnym krokiem jest instalacja certyfikatu w serwerze Exchange 2007. W konsoli do zarządzania serwerem proszę wydać polecenie:

```
Import-ExchangeCertificate -path sciezka-do-pliku.cer -friendlyname  
"win2008.certum.local"
```

Poszczególne parametry mają następujące znaczenie:

- path – katalog, w którym zapisany został certyfikatem
- friendlyname – nazwa przyjazna, nazwa, pod którą będzie widoczny certyfikat w magazynie certyfikatów

Następnie należy odnaleźć odcisk palca zainstalowanego certyfikatu. W konsoli zarządzającej należy wydać polecenie:

```
Get-ExchangeCertificate -DomainName "win2008.certum.local"
```

Zostaną wyświetlone zainstalowane certyfikaty i ich odciski palca. Wyjście powinno być podobne do przedstawionego na rysunku.

```
[PS] C:\Windows\System32>Get-ExchangeCertificate -DomainName "win2008.certum.local"
```

Thumbprint	Services	Subject
7E829F05B52C98A498EE07A309A0073836FDD618	IP.WS	CN=win2008.certum.local, O=Unizeto Technolo...
91B2243030641B8992FB3149129ED29ECAA7CCD0	IP..S	CN=WIN2008
6CB3E7545797173B8F037E69DFE63B4E717F3FF1	IP..S	CN=WIN2008

```
[PS] C:\Windows\System32>_
```

Należy skopiować odcisk palca certyfikatu wystawionego przez CERTUM.

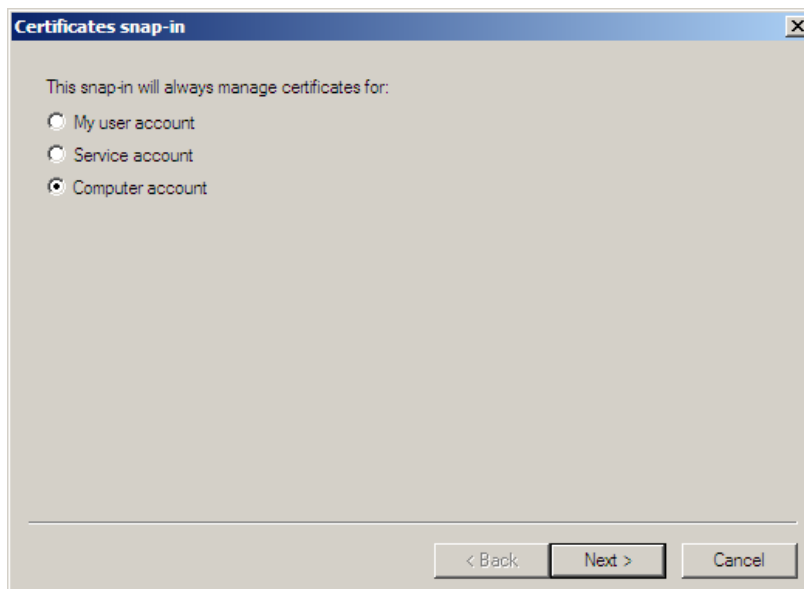
Następną czynnością do wykonania jest przypisanie certyfikatu do poszczególnych usług serwera Exchange. Należy wydać polecenie:

```
Enable-ExchangeCertificate -thumbprint <odcisk-palca> -services  
"IIS, POP, IMAP"
```

Po tej czynności należy uruchomić ponownie serwer. Konfiguracja certyfikatu została ukończona.

## 5. Wykonywanie kopii zapasowej certyfikatu i klucza prywatnego

W oknie „Uruchom” proszę wpisać mmc.exe. Zostanie uruchomiony edytor przystawek MMC. Z menu „Plik” należy wybrać „Dodaj/Usuń przystawkę”. W nowym oknie proszę wybrać „Certyfikaty” i kliknąć przycisk „Dodaj”. W następnym oknie proszę wybrać konto komputera:



W następnym oknie proszę wybrać opcję „Komputer lokalny”. Następnie proszę rozwinąć gałąź „Osobisty” i „Certyfikaty”. Proszę kliknąć prawym przyciskiem myszy na ikonę certyfikatu i z menu kontekstowego wybrać „Wszystkie zadania” a następnie „Eksportuj”. Zostanie uruchomiony kreator eksportu certyfikatu. W czasie eksportu należy zaznaczyć następujące opcje:

- „Tak, eksportuj klucz prywatny” (Krok 1)
- „Włącz silną ochronę klucza prywatnego” (Krok 2)
- „Jeśli to możliwe dołącz wszystkie certyfikaty do ścieżki certyfikacji” (Krok 2)

Po wybraniu tych opcji należy podać hasło chroniące klucz prywatny (Krok 4). W ostatnim kroku należy wskazać lokalizację, w której zostanie zapisany plik w formacie PKCS12. Będzie on zawierał kopię zapasową klucza prywatnego i certyfikatu.