

UNIZETO



POWSZECHNE  
CENTRUM CERTYFIKACJI



instrukcja użytkownika

# Exchange Enterprise Edition 2003

Użycie certyfikatów niekwalifikowanych  
w oprogramowaniu Microsoft Exchange 2003

wersja 1.2

# Spis treści

<b>1. WSTĘP</b> .....	<b>3</b>
<b>2. TWORZENIE CERTYFIKATÓW</b> .....	<b>3</b>
2.1. TWORZENIE WNIOSKU O CERTYFIKAT CSR .....	3
2.2. TWORZENIE CERTYFIKATU NA PODSTAWIE UTWORZONEGO ŻĄDANIA CSR.....	10
2.3. POBIERANIE I INSTALOWANIE CERTYFIKATU NA SERWERZE .....	12
2.4. POBIERANIE CERTYFIKATÓW POŚREDNICH.....	18
2.5. IMPORT CERTYFIKATÓW POŚREDNICH.....	18
<b>3. KONFIGUROWANIE SERWERA EXCHANGE DO POŁĄCZEŃ HTTPS</b> .....	<b>22</b>
<b>4. IMPORT/EKSPORT CERTYFIKATÓW SERWERA</b> .....	<b>23</b>

## 1. Wstęp

Exchange jest serwerem pocztowym, przeznaczonym na platformę Windows. Dzięki wbudowanym mechanizmom bezpieczeństwa potrafi nawiązać szyfrowane i autoryzowane połączenie za pomocą protokołu TLS z drugim serwerem SMTP, umożliwiając w ten sposób bezpieczną wymianę informacji. Znajdujące się w pakiecie serwery POP3, NNTP, IMAP posiadają również wsparcie dla certyfikatów x.509, umożliwiając klientom tych serwisów bezpieczny i autoryzowany dostęp. Dokument ten zawiera instrukcję generowania unikalnej pary kluczy oraz CSR, dla serwera Exchange.

## 2. Tworzenie certyfikatów

### 2.1. Tworzenie wniosku o certyfikat CSR

Podczas generowania CSR trzeba podać następujące informacje:

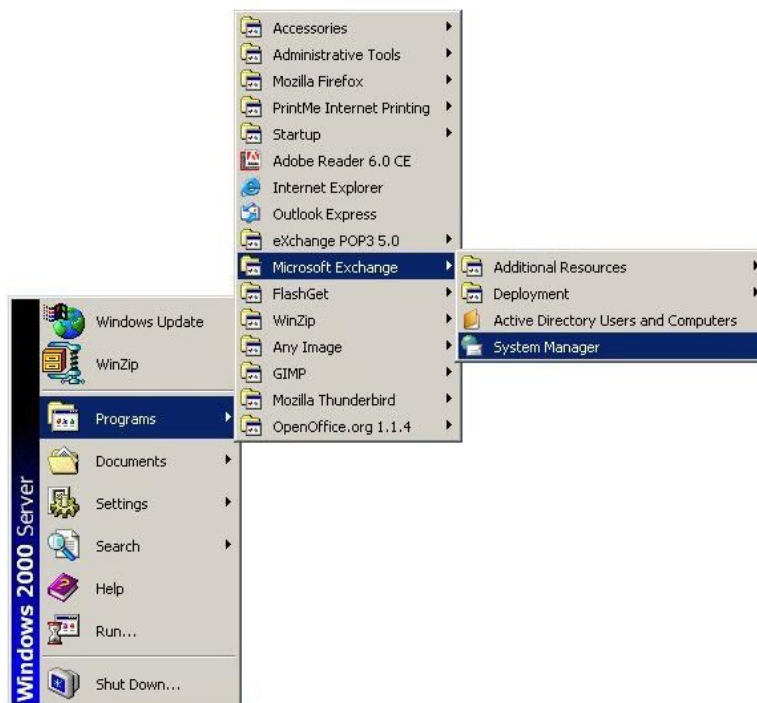
- 🔗 **Type a name for a Certificate** – wprowadź przyjazną nazwę nowotworzonego certyfikatu, np.: Serwer SMTP.
- 🔗 **Organization (O)** – podaj pełną nazwę organizacji / firmy, np.: Unizeto Technologies SA
- 🔗 **Organizational Unit (OU)** – jeżeli zachodzi taka potrzeba, można wypełnić to pole, wstawiając nazwę działu np. Dział Marketingu, Katedra Techniki Ciepłej czy Oddział Pediatrii.
- 🔗 **Common Name (CN)** – wprowadź pełną nazwa DNS (fqdn) lub IP które użytkownik serwera będzie wprowadzał w swoim programie pocztowym, np.: serwera np.: mail.mojserwer.pl .
- 🔗 **Country (C)** – wprowadź dwuliterowy symbol kraju (PL). Należy użyć kodu ISO, np. poprawnym kodem Polski jest PL (duże litery), a nie pl czy RP.
- 🔗 **State/Province (ST)** – podaj nazwę województwa, np.: Zachodniopomorskie, Mazowieckie. Nie stosuj skrótów.
- 🔗 **City/Locality (L)** – podaj nazwę miejscowości, np.: Szczecin, Warszawa.
- 🔗 **File Name** – podaj nazwę pliku, w którym zostanie zapisane żądanie certyfikatu, np.: C:\myreq.csr. Plik z żądaniem trzeba będzie przesłać do CERTUM.

**UWAGA:** Ważne jest też, aby przy wypełnianiu powyższych pól nie używać polskich znaków diakrytycznych: **ą ł ż** oraz znaków specjalnych: **^ & \_ \$ @**.

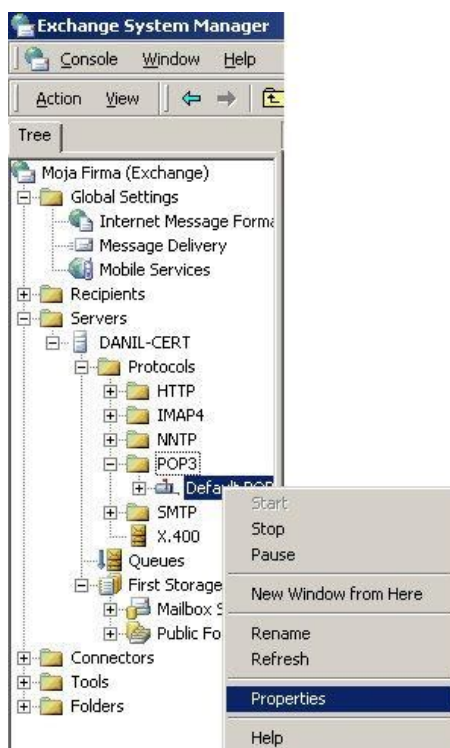
Aby wygenerować żądanie CSR, które zostanie wysłane do CERTUM i podpisane przez jeden z certyfikatów CERTUM, należy zalogować się jako administrator serwera i uruchomić **Exchange**

**System Manager:**

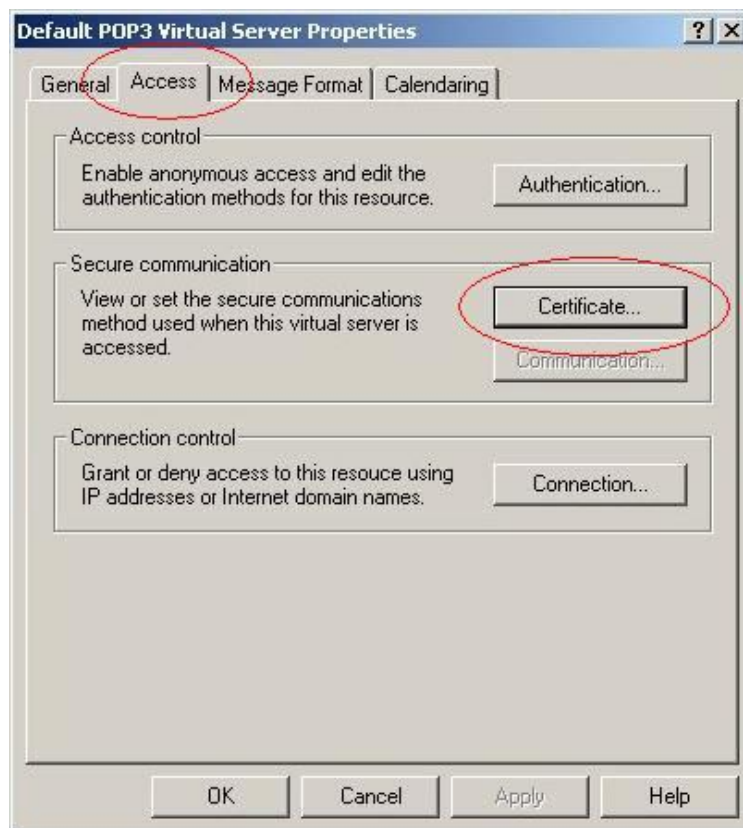
Start -> Programs -> *Microsoft Exchange* -> *System Manager*



Klikamy prawym przyciskiem myszki na protokół, dla którego chcemy wprowadzić transmisję danych w osłonie **SSL**, po czym wybieramy *Properties*:



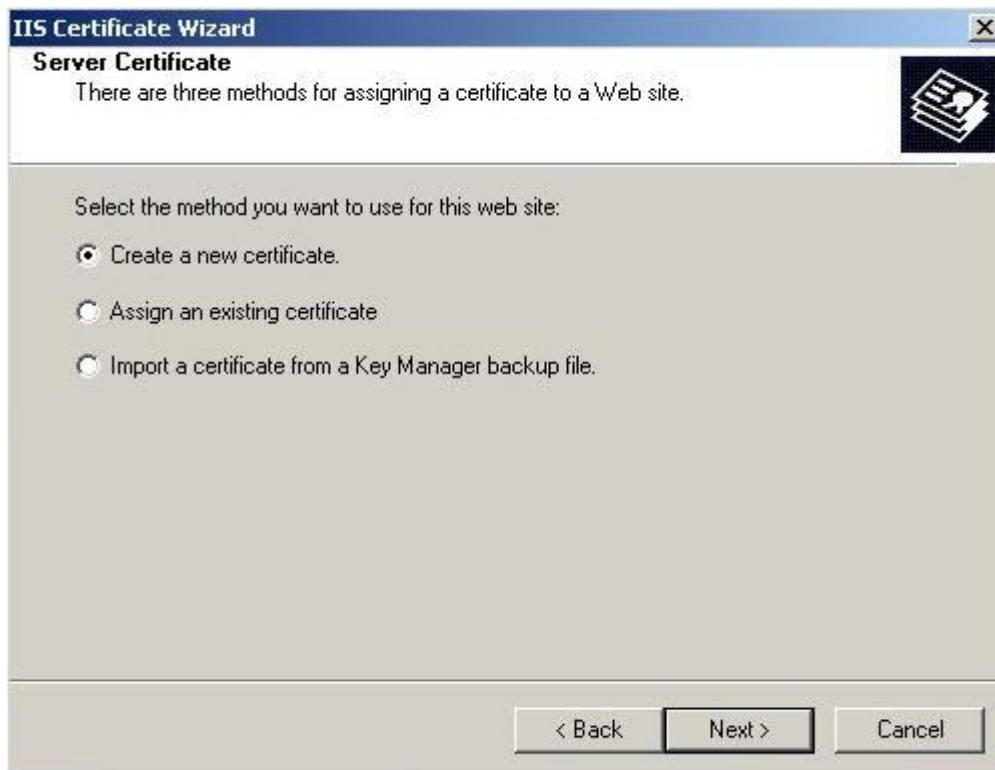
Z okna *Properties* wybieramy zakładkę *Access* klikamy na *Certificate*:



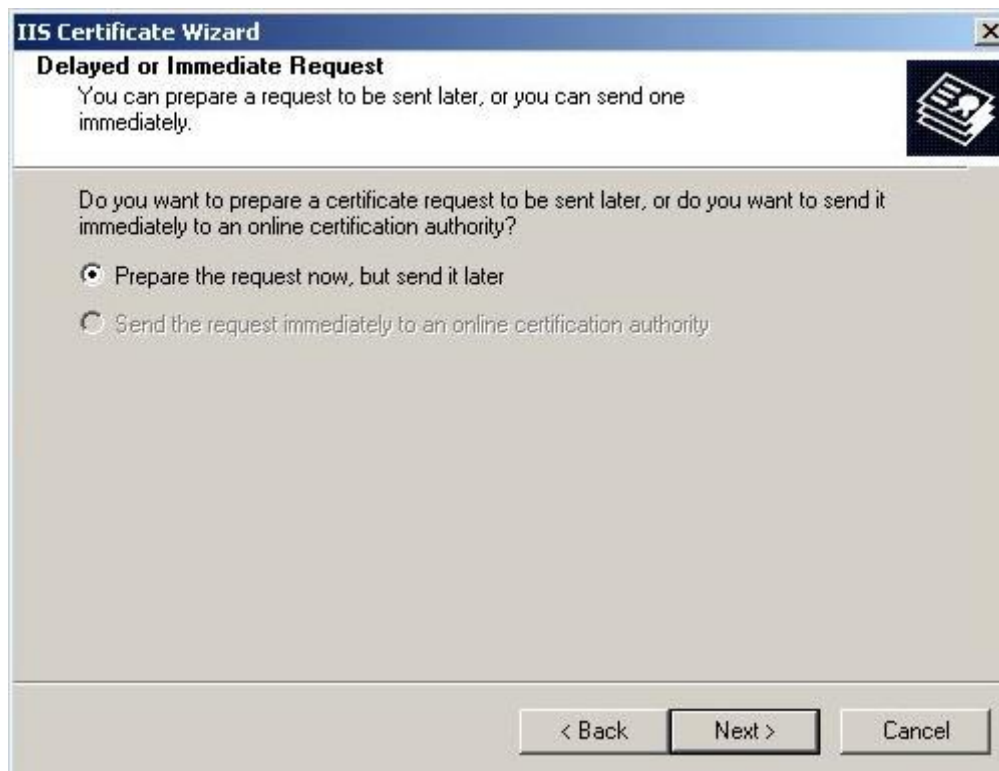
W ten sposób uruchomimy kreatora, który poprowadzi nas przez proces generowania żądania CSR:



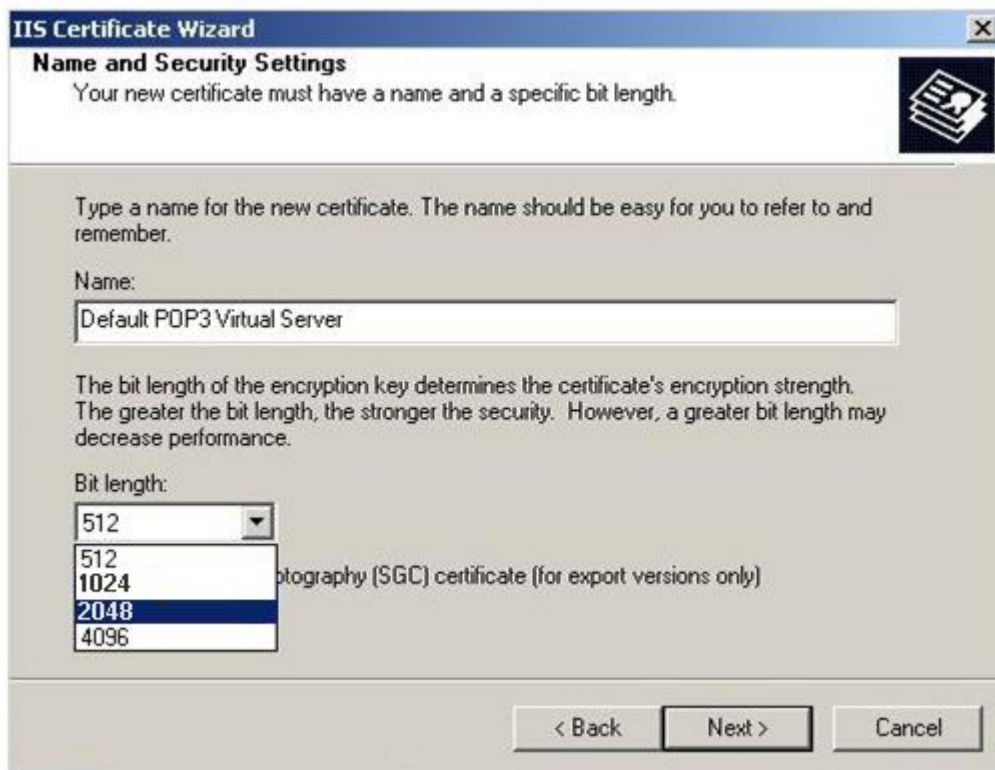
Zaznaczamy opcję *Create a new certificate*:



Zostawiamy domyślną opcję:



Wprowadzamy nazwę dla naszego Certyfikatu oraz wybieramy długość klucza (2048 bity to wartość wystarczająca):



The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Name and Security Settings' step. The title bar reads 'IIS Certificate Wizard' and the subtitle is 'Name and Security Settings'. Below the subtitle, it says 'Your new certificate must have a name and a specific bit length.' There is a small icon of a certificate in the top right corner. The main area contains instructions: 'Type a name for the new certificate. The name should be easy for you to refer to and remember.' Below this is a 'Name:' label and a text box containing 'Default POP3 Virtual Server'. Another instruction follows: 'The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.' Below this is a 'Bit length:' label and a dropdown menu. The dropdown menu is open, showing options: 512, 1024, 2048 (which is highlighted), and 4096. To the right of the dropdown, there is a note: 'Cryptographic (SGC) certificate (for export versions only)'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Wpisujemy unikalną nazwę i oddział firmy (organizacji):

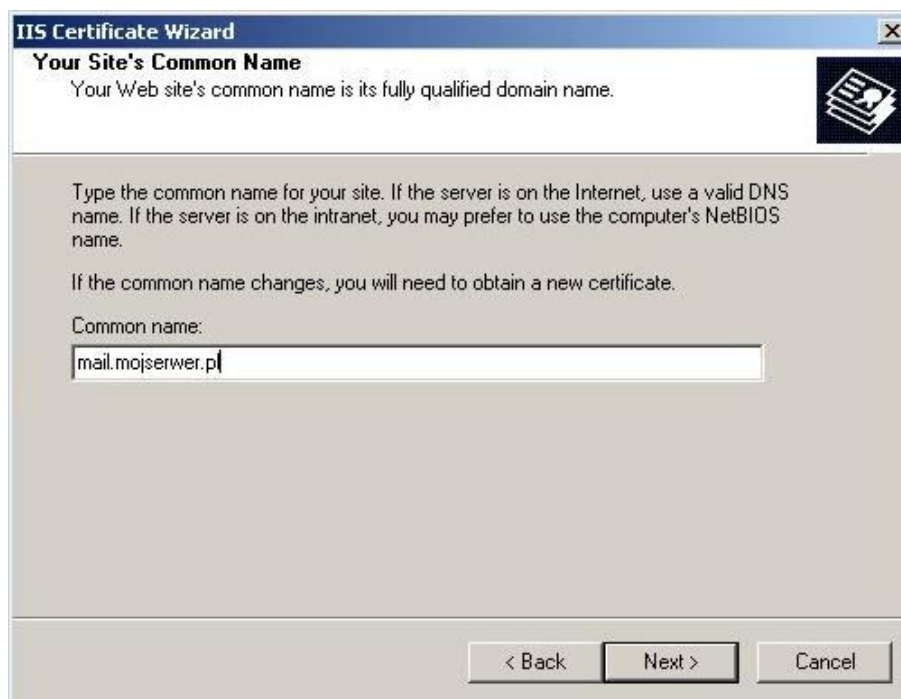
**UWAGA:** Używanie znaków specjalnych % ^ \$ \_ lub polskich znaków diakrytycznych: Żółć przy podawaniu tych informacji spowoduje nieprawidłowe wygenerowanie certyfikatu!!!



The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Organization Information' step. The title bar reads 'IIS Certificate Wizard' and the subtitle is 'Organization Information'. Below the subtitle, it says 'Your certificate must include information about your organization that distinguishes it from other organizations.' There is a small icon of a certificate in the top right corner. The main area contains instructions: 'Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.' Below this is another instruction: 'For further information, consult certification authority's Web site.' There are two labels: 'Organization:' and 'Organizational unit:'. Below each label is a dropdown menu. The 'Organization:' dropdown menu contains the text 'Moja Firma'. The 'Organizational unit:' dropdown menu contains the text 'Oddział w Moja Firmą'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

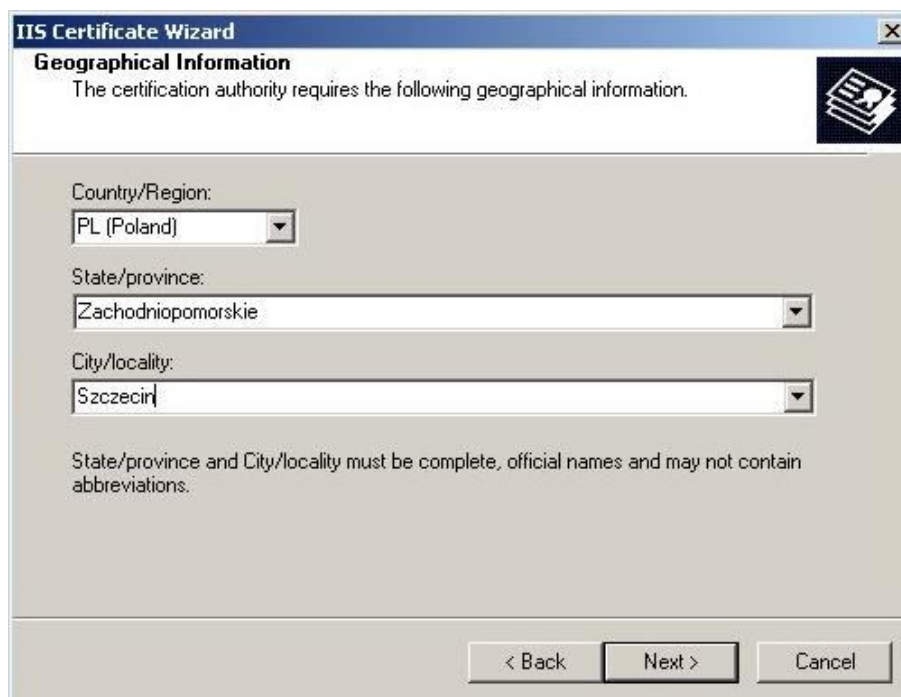
Teraz wprowadzamy nazwę pospolitą (Common Name) swojego serwera:

**UWAGA:** Jest to bardzo ważne pole i musi się tutaj znaleźć pełna nazwa DNS (fqdn) lub IP serwera np.: mail.mojserwer.pl (adres ten użytkownik korzystający z serwera będzie musiał wprowadzić w swoim oprogramowaniu)



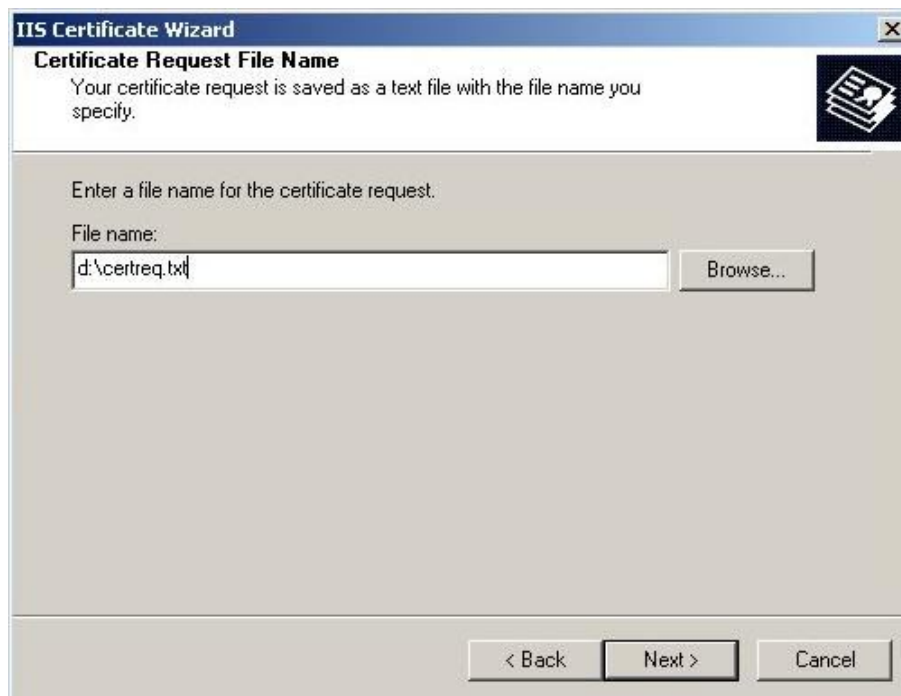
The screenshot shows the 'IIS Certificate Wizard' window at the 'Your Site's Common Name' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Your Site's Common Name' with a sub-heading 'Your Web site's common name is its fully qualified domain name.' Below this, there is explanatory text: 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name. If the common name changes, you will need to obtain a new certificate.' A text input field labeled 'Common name:' contains the text 'mail.mojserwer.pl'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Na zakończenie wpisujemy dane geograficzne dotyczące naszego certyfikatu...:



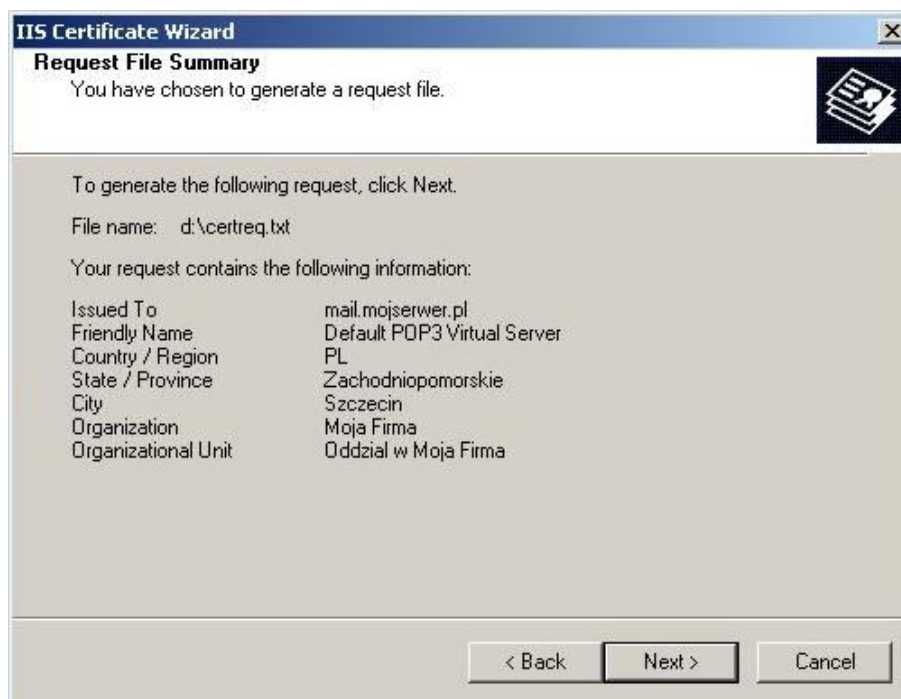
The screenshot shows the 'IIS Certificate Wizard' window at the 'Geographical Information' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Geographical Information' with a sub-heading 'The certification authority requires the following geographical information.' Below this, there are three dropdown menus: 'Country/Region:' with 'PL (Poland)' selected, 'State/province:' with 'Zachodniopomorskie' selected, and 'City/locality:' with 'Szczecin' selected. A note at the bottom states: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

... i podajemy plik, w którym kreator zapisze nasz certyfikat:



The screenshot shows the 'IIS Certificate Wizard' window at the 'Certificate Request File Name' step. The text reads: 'Your certificate request is saved as a text file with the file name you specify.' Below this, it says 'Enter a file name for the certificate request.' There is a text input field containing 'd:\certreq.txt' and a 'Browse...' button to its right. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

W podsumowaniu sprawdzamy czy dane, które umieściliśmy w certyfikacie są poprawne. Jeżeli nie, wracamy do pól formularza (klikając na *back*) i poprawiamy niewłaściwe pola:



The screenshot shows the 'IIS Certificate Wizard' window at the 'Request File Summary' step. The text reads: 'You have chosen to generate a request file.' Below this, it says 'To generate the following request, click Next.' The file name 'd:\certreq.txt' is displayed. It then lists the information contained in the request:

Issued To	mail.mojserwer.pl
Friendly Name	Default POP3 Virtual Server
Country / Region	PL
State / Province	Zachodniopomorskie
City	Szczecin
Organization	Moja Firma
Organizational Unit	Oddzial w Moja Firma

At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Kreator poinformuje nas o prawidłowym wygenerowaniu żądania CSR (oprócz żądania w rejestrach znajduje się już także klucz prywatny):



## 2.2. Tworzenie certyfikatu na podstawie utworzonego żądania CSR

Wygenerowane w kroku poprzednim żądanie powinno mieć postać podobną jak poniżej:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDMCCApkCAQAwgZoxGzAZBgNVBAMTEmRsdWJhY3oudW5pemV0by5wbDEhMB8G
A1UECXMpYRHpYWwgT2Nocm9ueSBJamZvcmlhY2ppMRswGQYDVQQKEExJVbml6ZXRv
IFNwLiB6IG8uby4xETAPBgNVBACtCFN6Y3plY2luMRswGQYDVQQIEExJaYWNob2Ru
aW9wb21vcnNraWUxZCZAJBgNVBAYTA1BMMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQC8JvRqRpb1toZyvMjfxCef5PIcyLMQv6Z2A10j2GMoeKBCCyZF1kHoDswW
0ZF54FrTZhyKwYqfghiH05duLfJsbqb/PTzovZH9qXUtxl+zQIhcJnA4Z/jKyWHG1
X7LUlC9u2bas/vWwQZwYvxeqNMW4RZ+LU9Qqm9b/YD2qtOZ2qwIDAQABOIIIBUzAa
BgorBgEEAYI3DQIDMQwWCjUuMC4yMTk1LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYD
VR0PAQH/BAQDAgTwMBMGAlUdJQQMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQIC
MYHuMIHrAgEBHloATQBpAGMAcgbVAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEA
bgBuAGUAbAAgAEMAcb5AHAAdABvAgcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkA
ZABLAHIDgYkAXxNuAz6gcBaZUdef8WQ2PAroKMW8sprcKv7QD2encz6/Wct9D25C
kGynLgy0f+Lff7ViSDJqxyWaj68ddqgXyAqIilF63kiVPTiC6yxLaNX65v3cnKFx
4UrUrGXztub7M7/NuxSipOW0Vv7yCHganypxDyRzp6IhulEnL4APEH4AAAAAAAAA
ADANBgbkqhkiG9w0BAQUFAAOBgQAsTG3Hu00fFzNTekFo/fb3tKsmuS/1rCCB5sQK
iNpWGZ8Z8+TmqBB0Tuz4FPTkeSqLpWv1ORfmxMKPIul0dC3QwRP2E//oMPnaU807
IJIDwn2VZ7qQ/h0KcWoWSPmvt7J0KKshdGgAF7P6AYc7W4yA9B9nPeyEzQRW0t4D
YBApPQ==
-----END NEW CERTIFICATE REQUEST-----
```

Mając wygenerowane żądanie wypełniamy formularz zgłoszeniowy i wklejamy CSR na stronie CERTUM ([www.certum.pl](http://www.certum.pl) -> *Oferta* -> *Certyfikaty niekwalifikowane* -> *Zabezpieczanie serwerów* -> *Serwery SSL* i na dole strony wybieramy *Kup certyfikat*).

Pobierz certyfikat Private SSL Server (niekwalifikowany)

— **Żądanie certyfikatu** —

W poniższe pole wstaw żądanie certyfikatu zgodne z PKCS#10.

```
MIIBzzCCATgCAQAwY4xCzAJBgNVBAYTAiBMMRswGQYDVQQLExJ6YWNob2RuaW9w
b21vcnNraWUxETAPBgNVBAClTCFN6Y3plY2luMQ8wDQYDVQQKEwZDZlJ0dW0x
BgNVBAMTDTEwLjEwMC4xMC4xMjIxJjAkBgkqhkiG9w0BCQEFW21wcm9zemtpZ
XdpY3pAY2VydHVTLnBsMIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQD2S6
Bhg0AW+ATNUOY5ufN0L5skYKbDS8kYgu1B5Mu+V9H+zHYaHHyCd5t3O6E2Rt5
0QTFzTjVegprM+XAVCUB8YuIhbAJS4XquArShc3Xc76cGTO/dF/Qg9c+fbhKbm
ZvTkyKY3ZwHwpTdo3AREHTPXJ4un/JKQI8xS3s05ulEQIDAQABoAAwDQYJKo
ZIhvcNAQEEBQADgYEA0XSd57qDeikfyf1HV4JGk+1j55yiD2m1nql1GiDZg6
ZII4xv8beYjf4Wu8KkKbKdH0wSfQT8JoXNs2hri5KiaJ6JUg79j4U4jZSP+82
oDDvk8pZbf5uKnJcfB2WrPF7II+WuBd6q4WCVTioLhqlG8iLaS6fyEXDOvwXWDqj
P+I=
-----END 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

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](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 i instalowanie certyfikatu na serwerze

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:

### 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

 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

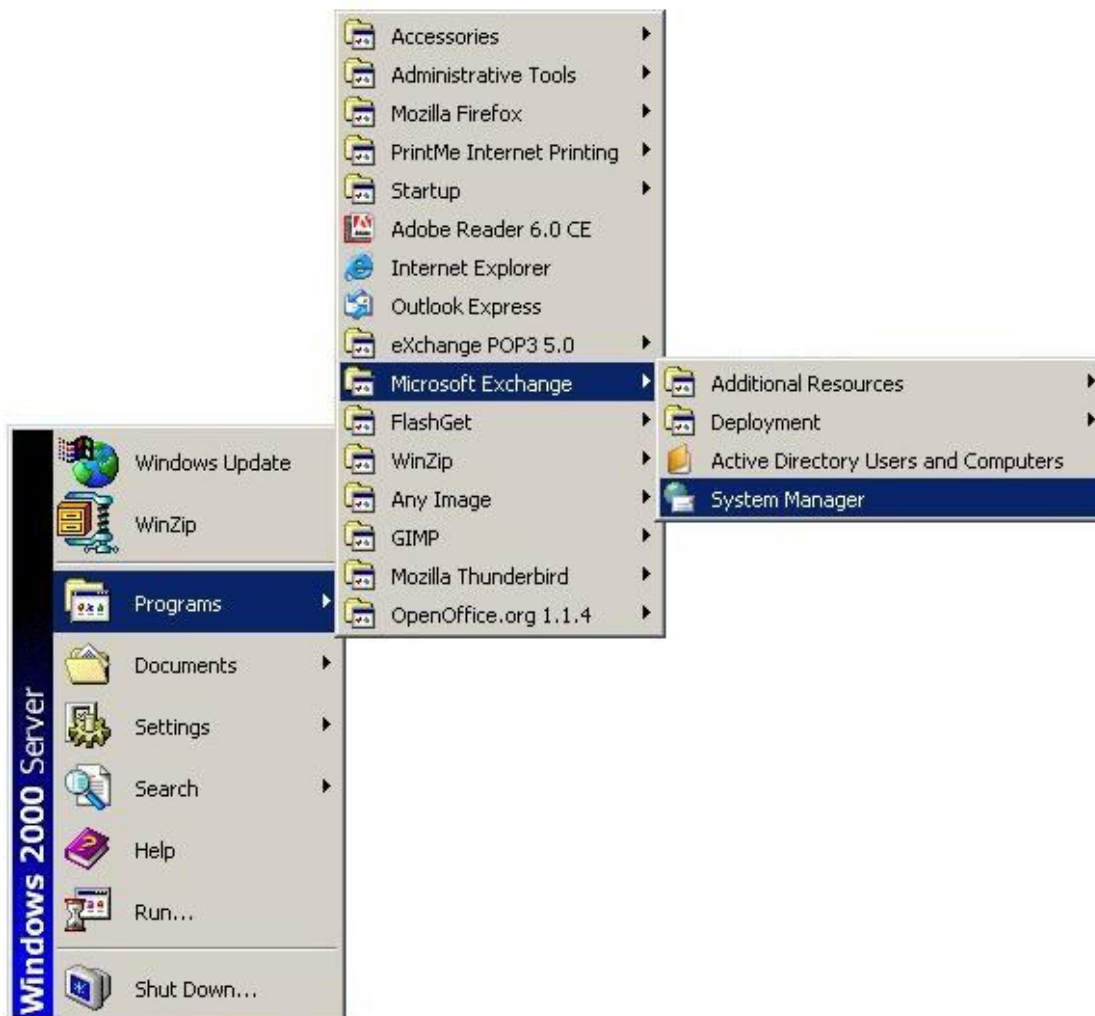
Dla interesującego nas certyfikatu wybieramy opcję *Zapisz tekstowo* lub *Zapisz binarnie*:

### Wyszukaj certyfikat (niekwalifikowany)

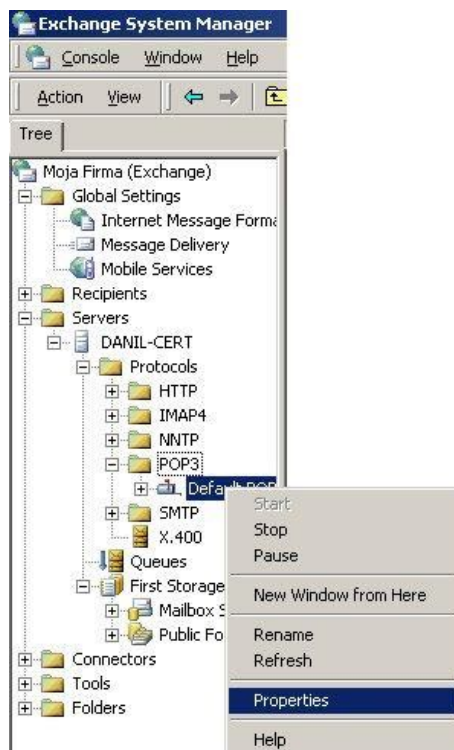
<b>Private SSL Server</b>	Ważny do: 17-06-2007	
Podmiot: 10.100.10.122 Numer: 0x37D85 Status: <b>Ważny</b>		
Zainstaluj własny	Zapisz binarnie	Zapisz tekstowo

Aby zainstalować certyfikat na serwerze należy zalogować się jako administrator serwera i uruchomić **Exchange System Manager**:

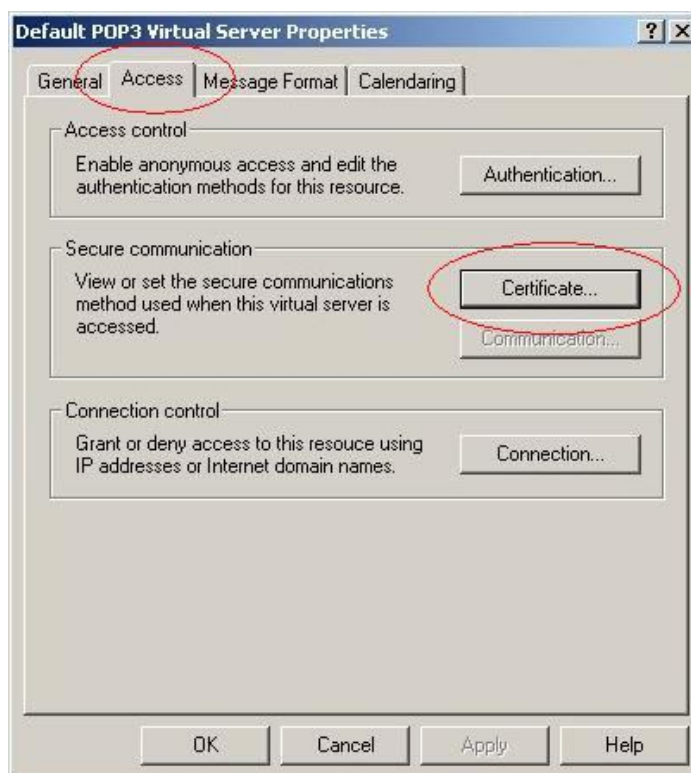
Start -> Programs -> *Microsoft Exchange* -> *System Manager*



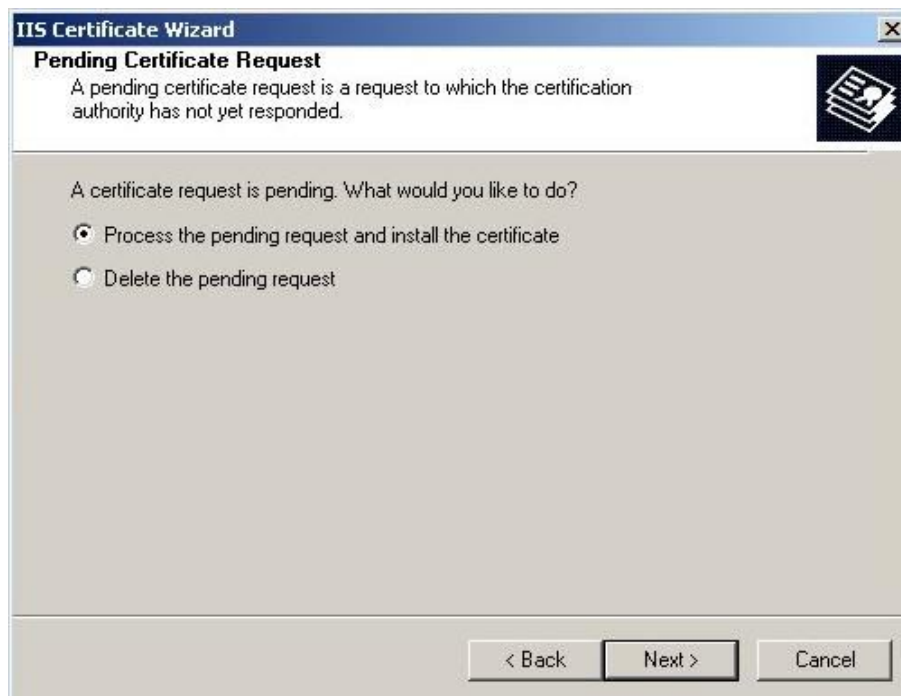
Klikamy prawym przyciskiem myszki na protokół, dla którego chcemy wprowadzić transmisję danych w osłonie **SSL**, po czym wybieramy *Properties*:



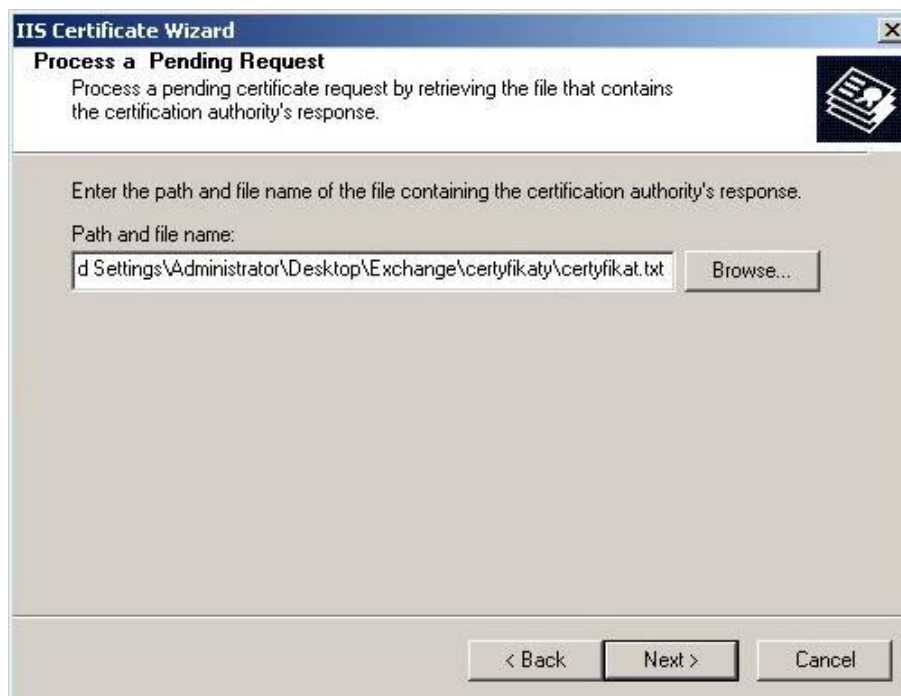
Z okna *Properties* wybieramy zakładkę *Access* klikamy na *Certificate*:



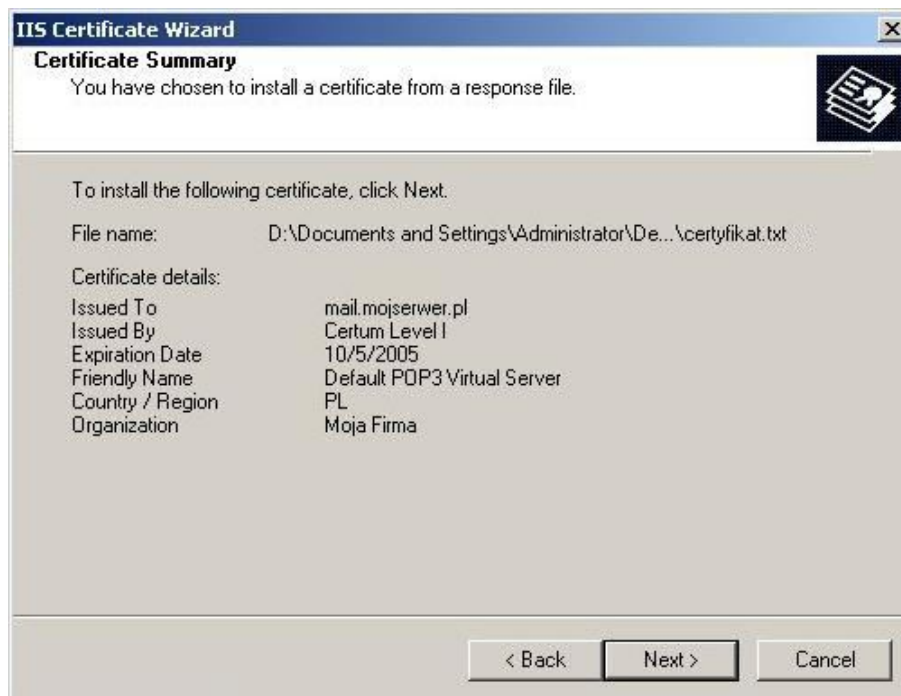
Zaznaczamy *Process the pending request and install the certificate* :



Wskazujemy kreatorowi plik, w którym zapisaliśmy certyfikat serwera:



Zaprezentowane zostaną dane dotyczące serwera, które zapisane są w certyfikacie.



Kreator poinformuje nas o zakończeniu pracy:



Certyfikat został zainstalowany na naszym serwerze.

## 2.4. Pobieranie 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.

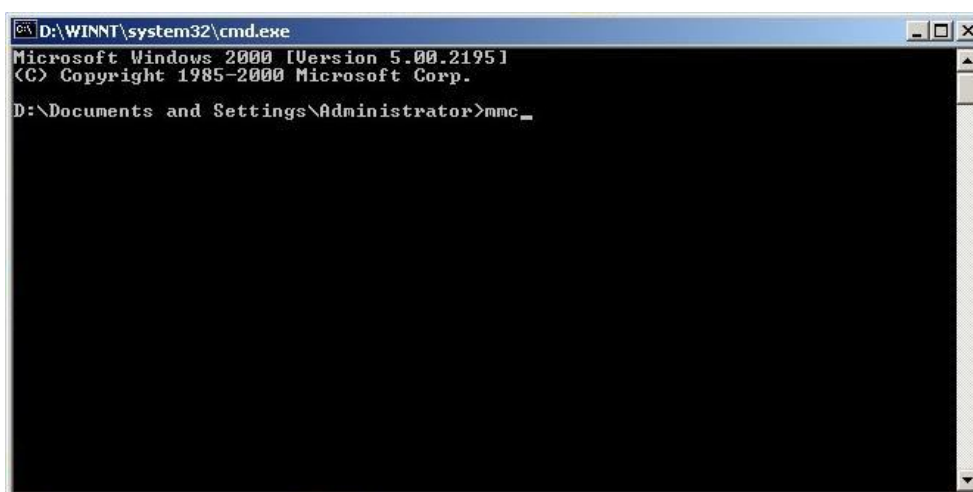
**UWAGA:** W celu wklejania do pliku certyfikatu prezentowanego na stronie należy skopiować fragment tekstu od linii "--BEGIN CERTIFICATE --" do "--END CERTIFICATE--", używając do tego celu edytora tekstowego np. Notepad i myszki. **Nie należy używać do tej operacji Worda, czy innego procesora tekstowego!**

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.

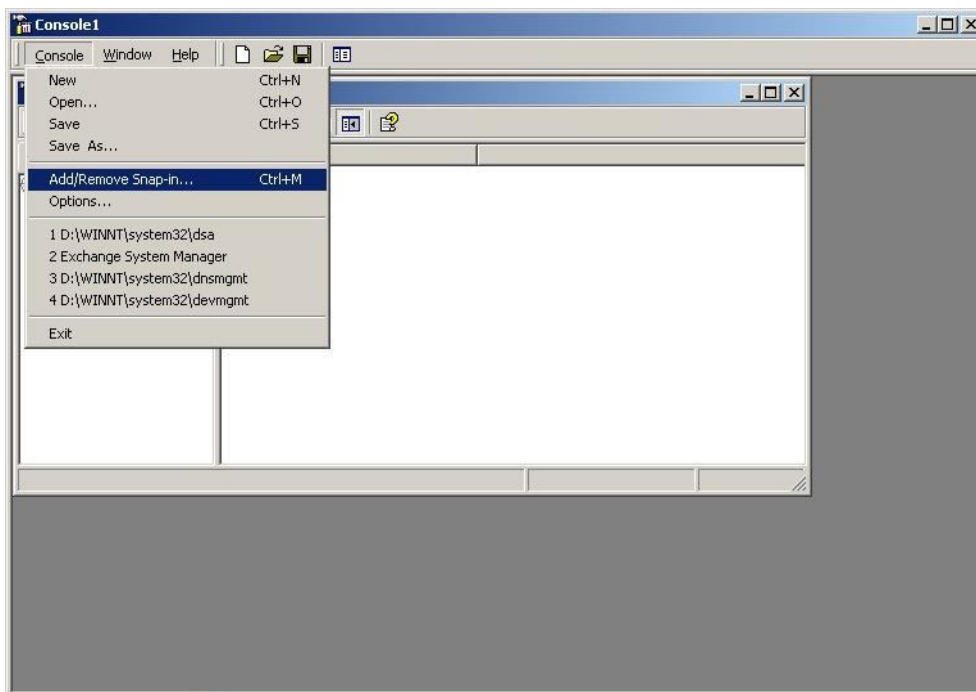
## 2.5. Import certyfikatów pośrednich

Konieczne jest utworzenie specjalnej konsoli do administrowania i zarządzania certyfikatami umieszczonymi w bazie certyfikatów komputera (standardowy wizard Windowsa łączy się z rejestrami określonego użytkownika), chyba, że konsola została utworzona już wcześniej-wtedy dostępna jest z menu *Narzędzia Administracyjne*.

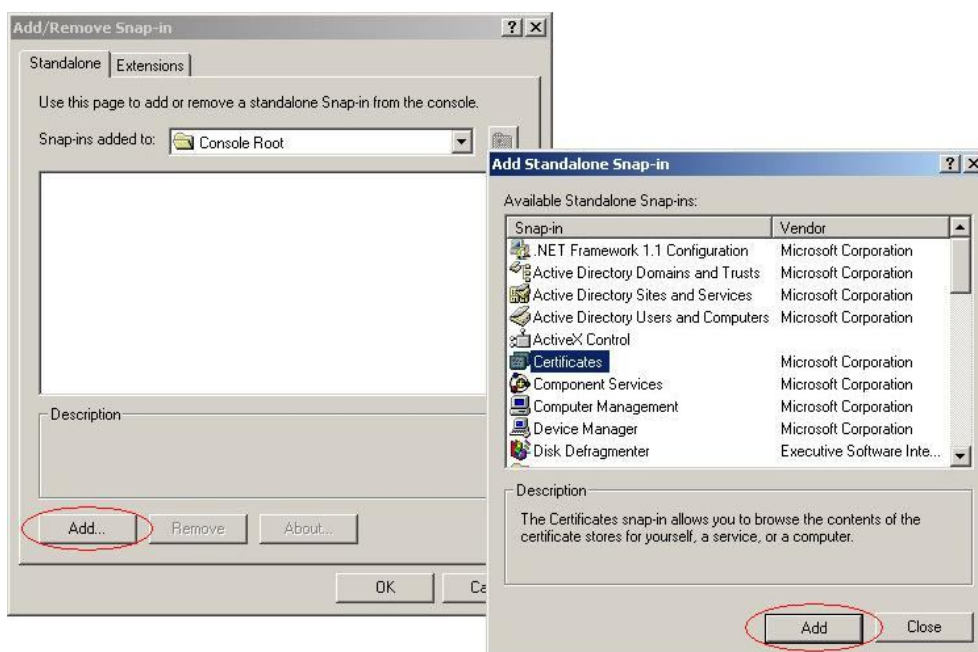
W tym celu utworzenia konsoli uruchamiamy z linii komend polecenie **mmc:**



W otwartej konsoli wybieramy z górnego menu opcję *Dodaj/Usuń przystawkę* lub wciskamy kombinację klawiszy *ctrl + M*:



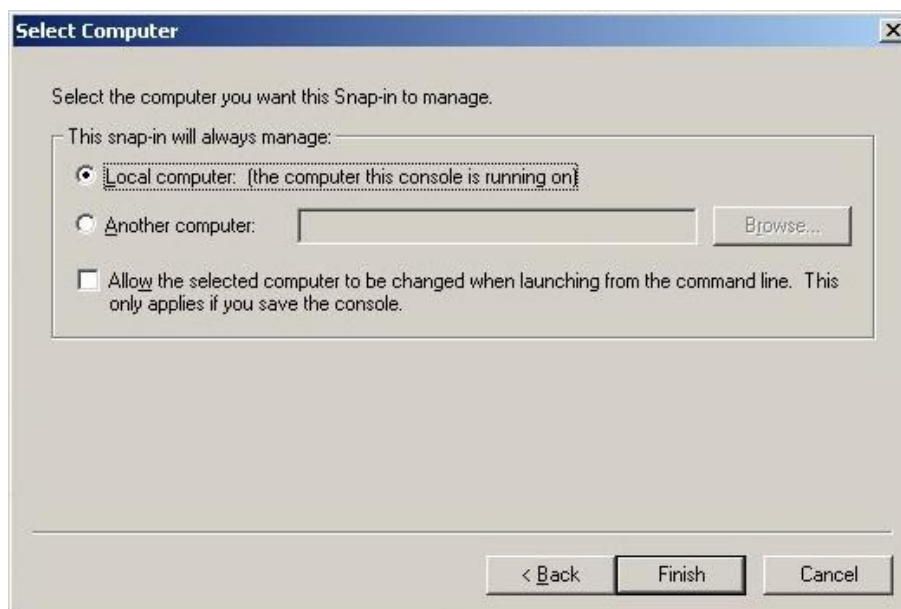
Wybieramy opcję *dodaj*, po czym przystawkę *Certyfikaty*:



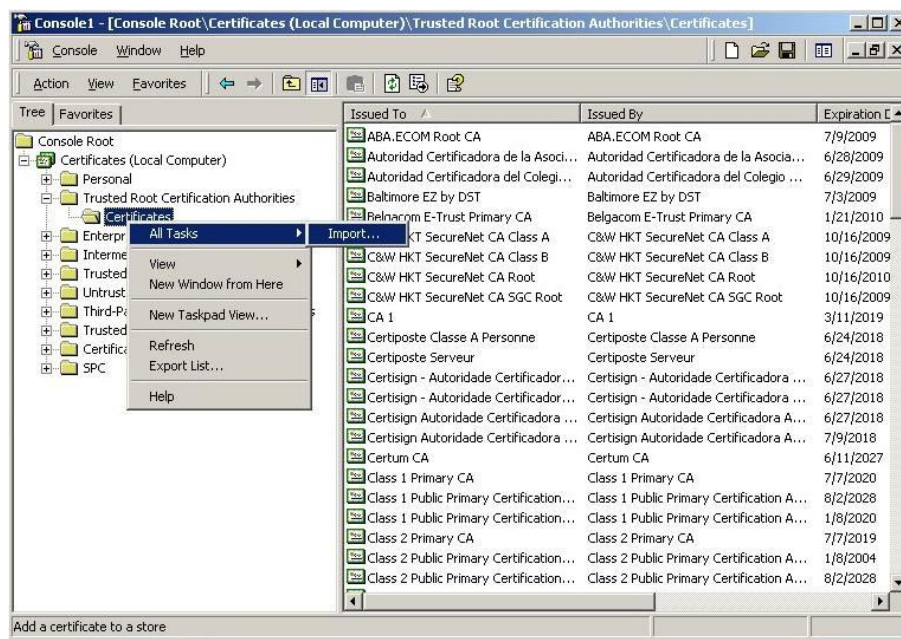
Zaznaczamy opcję *Konto komputera*:



Zostawiamy domyślne ustawienia (jeśli operacja dotyczy komputera lokalnego):



Wchodzimy do konsoli - opcja Certyfikaty ma teraz opcje podrzędne - po jej otwarciu przechodzimy do wskazanych opcji (**Zaufane główne urzędy certyfikacji, Pośrednie urzędy certyfikacji, Zaufane główne urzędy innych firm**) i dodajemy certyfikaty pośrednie (najlepiej dodawać wszystkie certyfikaty - Certum CA i Certum Level I-IV do wszystkich magazynów; praktycznie zaś wystarcza dodanie certyfikatów pośrednich do magazynu *Pośrednich urzędów certyfikacji*). Główny certyfikat (Certum CA) i certyfikaty pośrednie (Level I-IV) można pobrać ze strony: [http://www.certum.pl/certum/cert,certyfikaty\\_zaswiadczenia\\_klucze.xml](http://www.certum.pl/certum/cert,certyfikaty_zaswiadczenia_klucze.xml).



Klikając prawym przyciskiem myszy na katalogach Certyfikaty poszczególnych magazynów wybieramy opcję *All Taks* -> *Import* - tu już pojawia się znany wizerunek.

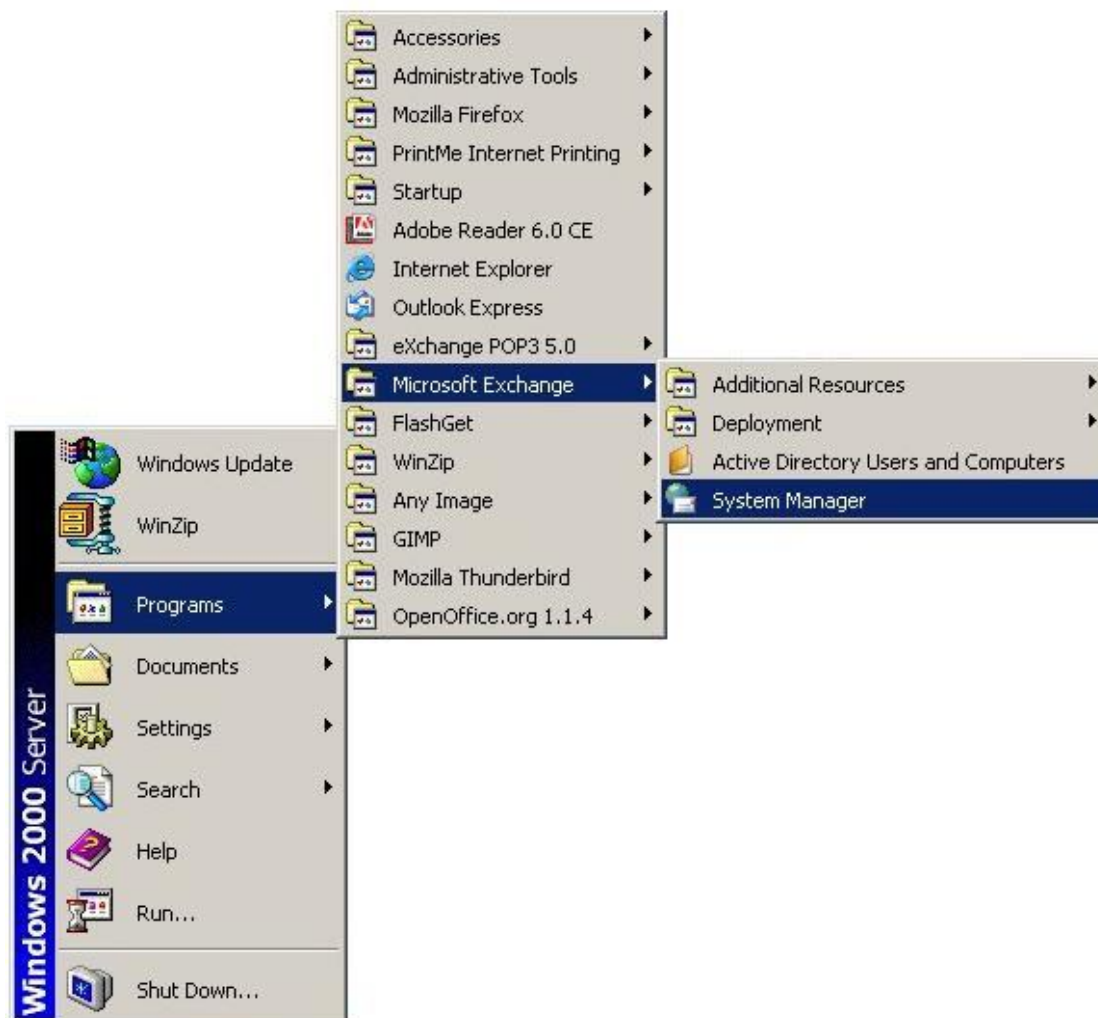
Po zakończeniu importu, serwer (nie tylko usługę) należy ponownie uruchomić.

Po zaimportowaniu certyfikatu do wskazanych kontenerów Exchange uzyskuje informacje, które pozwalają użytkownikowi zbudować pełną ścieżkę certyfikacji (wraz z certyfikatem Certum CA znajdującym się w bazie oprogramowania klienta).

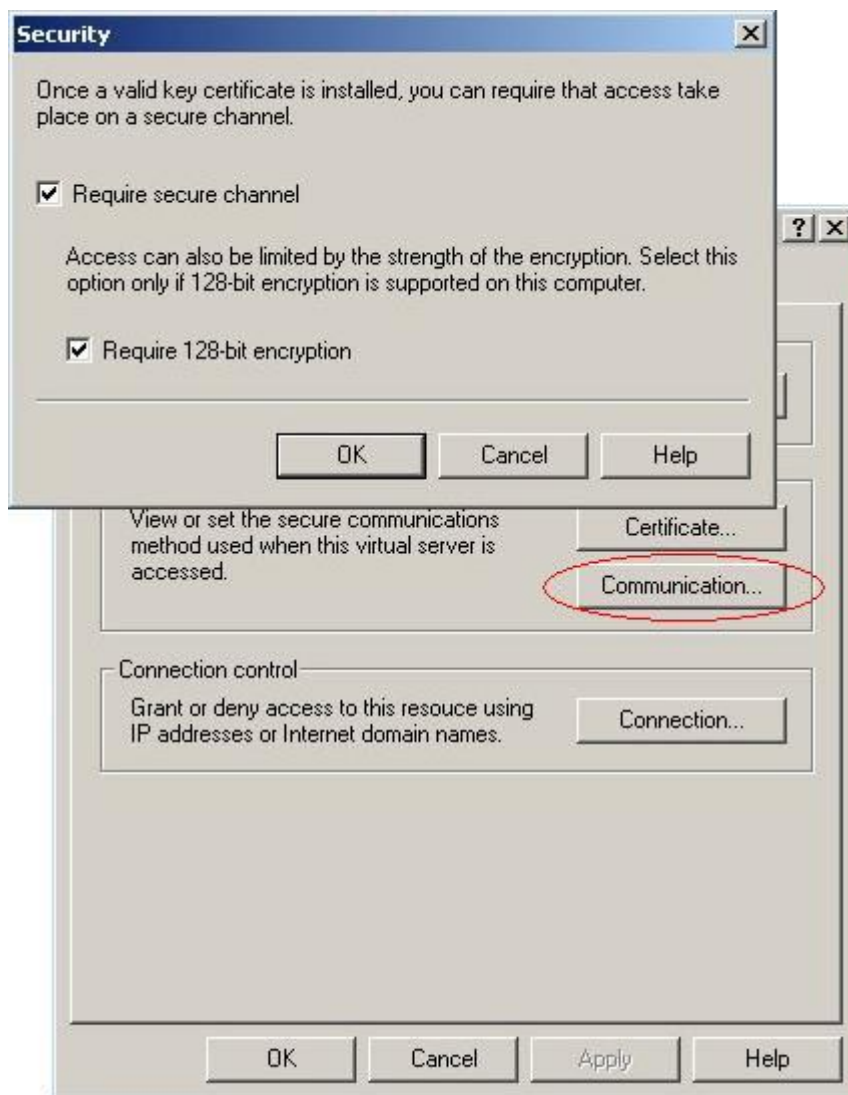
### 3. Konfigurowanie serwera Exchange do połączeń https

Aby nasz serwer obsługiwał szyfrowane połączenia należy zalogować się jako administrator serwera i uruchomić **Exchange System Manager**:

Start -> Programs -> *Microsoft Exchange* -> *System Manager*



Z okna *Properties* wybieramy zakładkę *Access* klikamy na *Communication* i zaznaczamy opcje *Require secure channel* i *Require 128-bit encryption*:



#### 4. Import/Eksport certyfikatów serwera

W celu importu/eksportu certyfikatu serwera (wraz z kluczem prywatnym) konieczne jest utworzenie specjalnej konsoli do administrowania i zarządzania certyfikatami umieszczonymi w bazie certyfikatów komputera (standardowy wizard Windowsa łączy się z rejestrami określonego użytkownika), chyba, że konsola została utworzona już wcześniej-wtedy dostępna jest z menu w Narzędziach Administracyjnych w Panelu Sterowania (patrz punkt powyżej).

W celu zaimportowania certyfikatu serwera po uruchomieniu konsoli przechodzimy do opcji *Personal* i z menu *Action* -> *All tasks*, wskazujemy polecenie *Import...* Pojawi nam się kreator, który poprowadzi nas przez proces importowania. W kreatorze należy wykonać następujące czynności:

- Wskazać plik z kopią kluczy i certyfikatu (w formacie \*.pfx)
- Podać hasło dla klucza prywatnego i zaznaczyć opcję *Oznacz klucz jako eksportowalny*

- Zakończyć kreatora

W celu wyeksportowania certyfikatu serwera po uruchomieniu konsoli przechodzimy do opcji Personal i wybieramy certyfikat, dla którego chcemy utworzyć kopię. W tym celu z menu Action -> All tasks, wskazujemy polecenie Export... Pojawi nam się kreator, który poprowadzi nas przez proces eksportowania. W kreatorze należy wykonać następujące czynności:

- Zaznaczyć opcję Eksport z kluczem prywatnym
- NIE zaznaczać opcji Usuń klucz prywatny po udanym eksporcie
- Podać hasło, które będzie chroniło eksportowany klucz prywatny
- Podać nazwę pliku, do którego zapisana zostanie kopia zapasowa
- Zakończyć kreatora