

# Instrukcja pozyskania i instalacji certyfikatu SSL/TLS dla **Internet Information Server 6.0**

## Spis treści

Wstęp .....	2
Import oraz instalacja certyfikatów urzędów CC Signet.....	2
<i>Usuwanie certyfikatów urzędów .....</i>	<i>2</i>
<i>Import certyfikatów urzędów.....</i>	<i>2</i>
<i>Import certyfikatu urzędu głównego CC Signet - RootCA .....</i>	<i>3</i>
<i>Import certyfikatu urzędu pośredniego CC Signet - PCA Klasa 2.....</i>	<i>6</i>
<i>Import certyfikatu urzędów końcowych CC Signet - CA Klasa 1 i CA Klasa 2 .....</i>	<i>8</i>
Generowanie pary kluczy oraz wniosku o certyfikat CSR .....	9
Proces pobierania certyfikatu z CC Signet.....	14
Instalacja certyfikatu na serwerze .....	15

## Wstęp

Jest to dokument, który pokaże Ci, jak poprawnie skonfigurować Internet Information Server 6.0, do zestawiania szyfrowanych połączeń w protokole SSL/TLS. Kolejne rozdziały pomogą Ci przejść przez wszystkie etapy tworzenia wniosku o certyfikat oraz instalacji certyfikatu. W efekcie będziesz mógł z łatwością zabezpieczyć swój serwer korzystając z certyfikatów wystawionych przez **Centrum Certyfikacji Signet**.

## Import oraz instalacja certyfikatów urzędów CC Signet

Certyfikat urzędu głównego, urzędu pośredniego oraz urzędów końcowych CC Signet należy ręcznie zaimportować do odpowiednich magazynów certyfikatów na serwerze. Przed przystąpieniem do tej czynności należy bezwzględnie usunąć wszystkie certyfikaty urzędów CC Signet ze swojego serwera, ponieważ w procesie instalacji automatycznej zostały błędnie zaimportowane do nieodpowiednich magazynów.

### Usuwanie certyfikatów urzędów

W celu usunięcia certyfikatów na serwerze proszę uruchomić przeglądarkę Internet Explorer i wykonać poniższe kroki:

Proszę przejść do *menu Tools / Internet Options / Content / Certificates*

W zakładce *Intermediary Certification Authorities* usuwamy wszystkie certyfikaty urzędów pośrednich i końcowych:

- CC Signet - CA Klasa 1
- CC Signet - CA Klasa 2
- CC Signet - PCA Klasa 2

W zakładce *Trusted Root Certification Authorities* usuwamy wszystkie certyfikaty urzędu głównego (czasami zdarza się, że zostały zainstalowane kilkakrotnie):

- CC Signet - RootCA

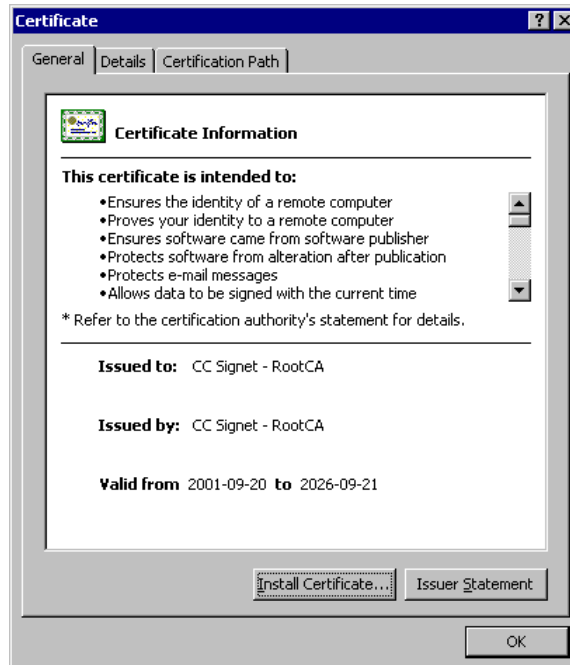
### Import certyfikatów urzędów

Podstawowym krokiem, jaki należy wykonać przed korzystaniem z certyfikatu SSL/TLS wystawionego przez centrum certyfikacji jest import certyfikatów urzędów tego centrum. Elementy te można zaimportować bezpośrednio ze strony WWW repozytorium centrum certyfikacji. Dla Centrum Certyfikacji Signet taką stroną jest <http://www.signet.pl/repozytorium/>. Po wejściu na stronę należy zaimportować certyfikaty wszystkich urzędów poprzez kliknięcie na każdy link oznaczony jako PEM i zapisać je na dysku.

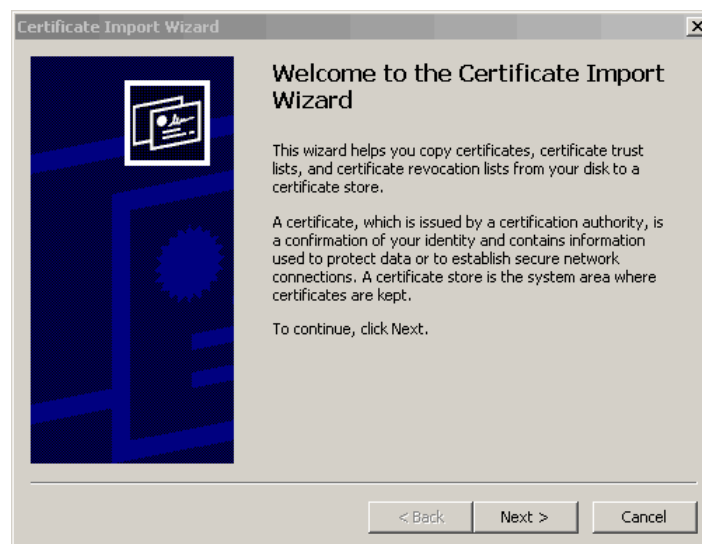
CC Signet - RootCA	<a href="http://www.signet.pl/repozytorium/rootca/rootca_pem.crt">http://www.signet.pl/repozytorium/rootca/rootca_pem.crt</a>
CC Signet - CA Klasa 1	<a href="http://www.signet.pl/repozytorium/klasa1/ca1_pem.crt">http://www.signet.pl/repozytorium/klasa1/ca1_pem.crt</a>
CC Signet - CA Klasa 2	<a href="http://www.signet.pl/repozytorium/klasa2/ca2_pem.crt">http://www.signet.pl/repozytorium/klasa2/ca2_pem.crt</a>
CC Signet - PCA Klasa 2	<a href="http://www.signet.pl/repozytorium/klasa2/pca2_pem.crt">http://www.signet.pl/repozytorium/klasa2/pca2_pem.crt</a>

## Import certyfikatu urzędu głównego CC Signet - RootCA

Klikamy dwukrotnie na pobranym certyfikacie *rootca\_pem.crt*



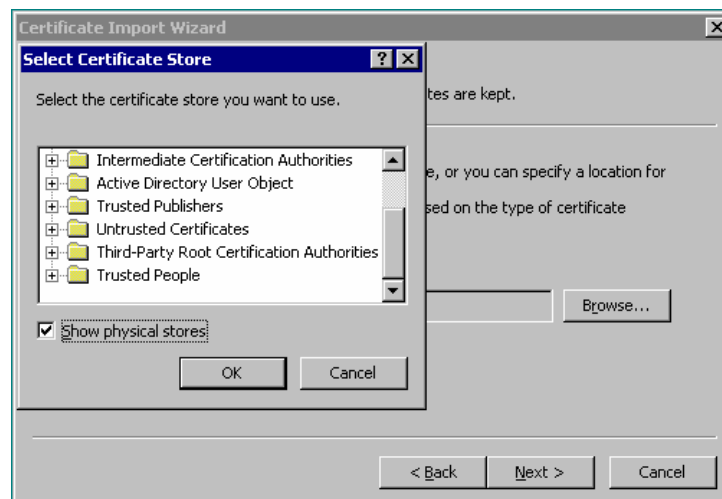
W celu uruchomienia kreatora instalacji klikamy na **Install Certificate**.



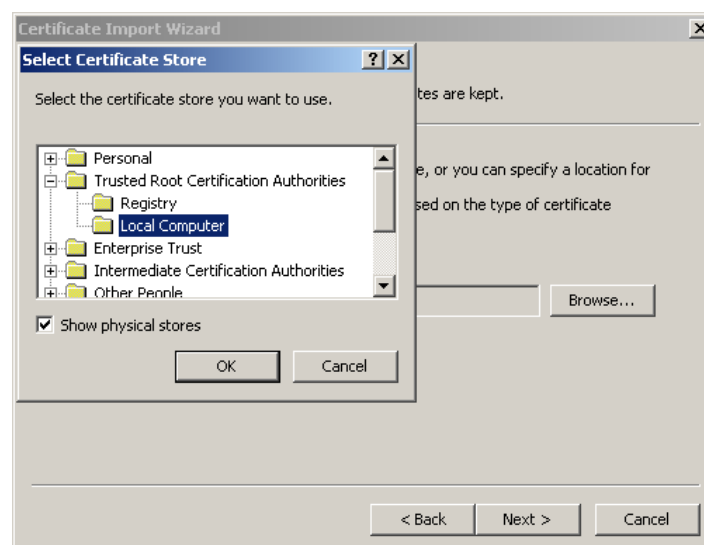
Klikamy **Next**.



Wybieramy *Place all certificates in the following store* i klikamy na *Browse*.  
Pojawia się dodatkowe okno.



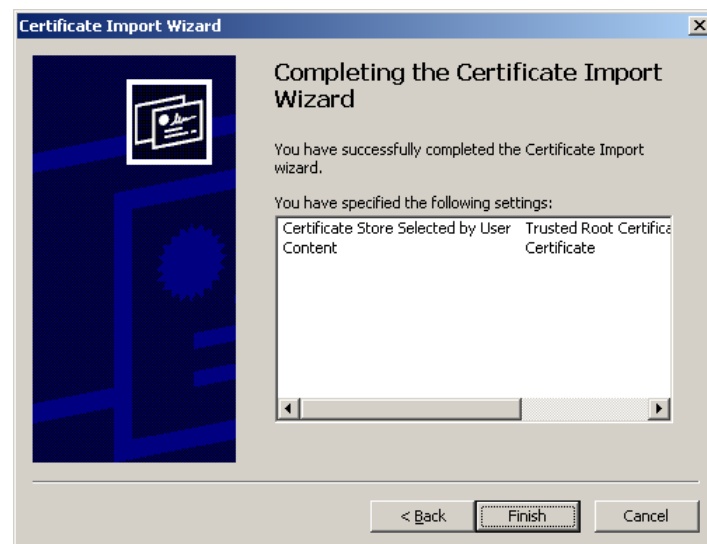
Zaznaczamy *Show physical stores*.



W magazynie *Trusted Root Certification Authorities* wybieramy *Local Computer*.  
Akceptujemy wybór magazynu klikając *OK*.



Klikamy *Next*.



Kończymy import klikając *Finish*.



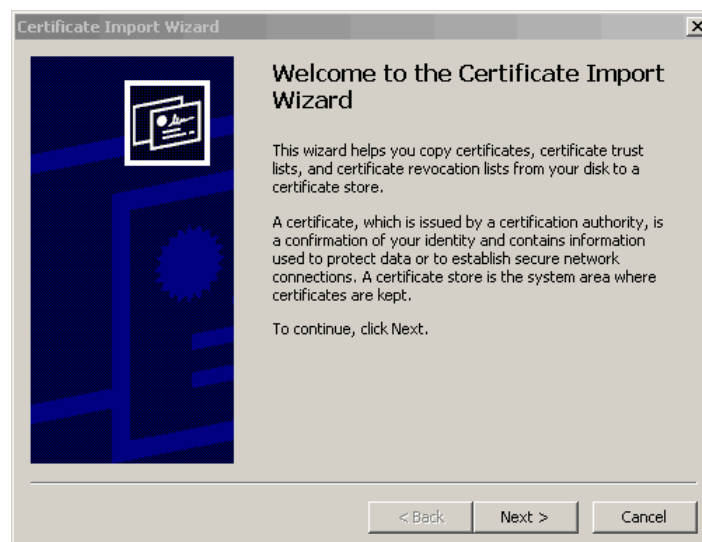
Powyższy komunikat informuje, że proces instalacji został zakończony sukcesem.

## Import certyfikatu urzędu pośredniego CC Signet - PCA Klasa 2

Klikamy dwukrotnie na pobranym certyfikacie *pca2\_pem.crt*



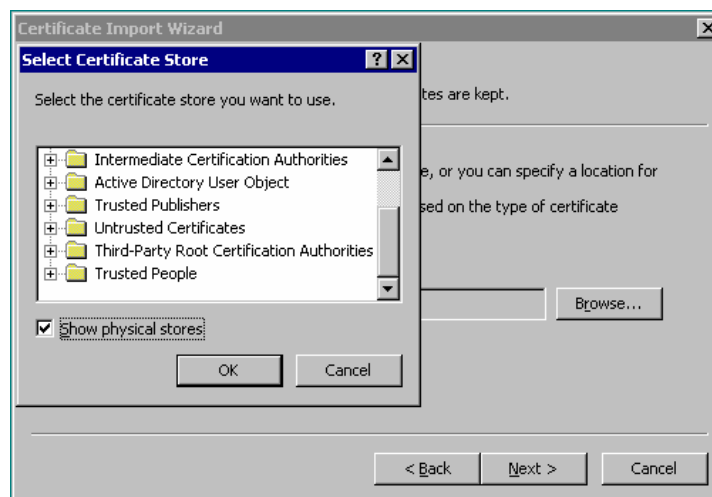
W celu uruchomienia kreatora instalacji klikamy na **Install Certificate**.



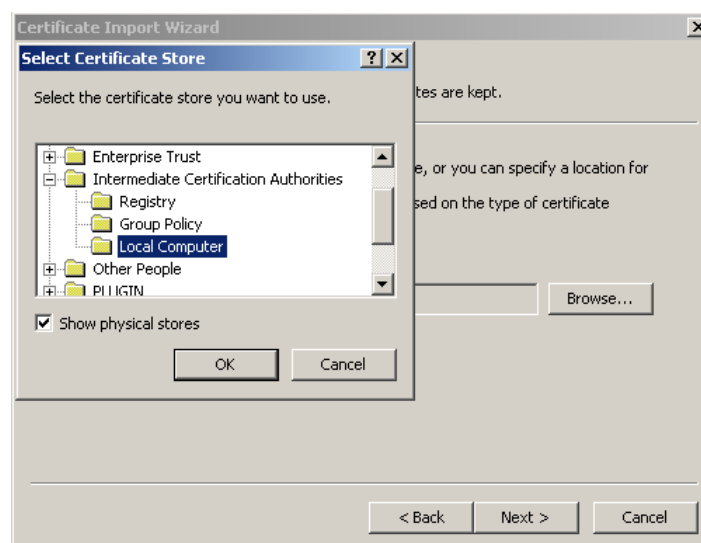
Klikamy **Next**.



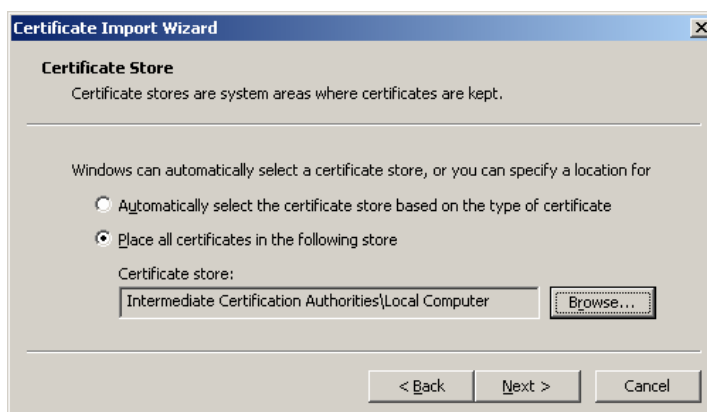
Wybieramy *Place all certificates in the following store* i klikamy na *Browse*.  
Pojawia się dodatkowe okno.



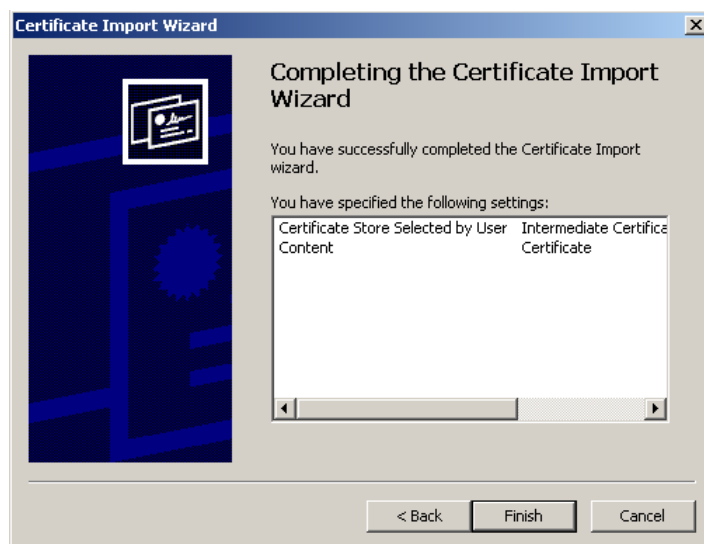
Zaznaczamy *Show physical stores*.



W magazynie *Intermediate Certification Authorities* wybieramy *Local Computer*.  
Akceptujemy wybór magazynu klikając *OK*.



Klikamy *Next*.



Kończymy import klikając *Finish*.



Powyższy komunikat informuje, że proces instalacji został zakończony sukcesem.

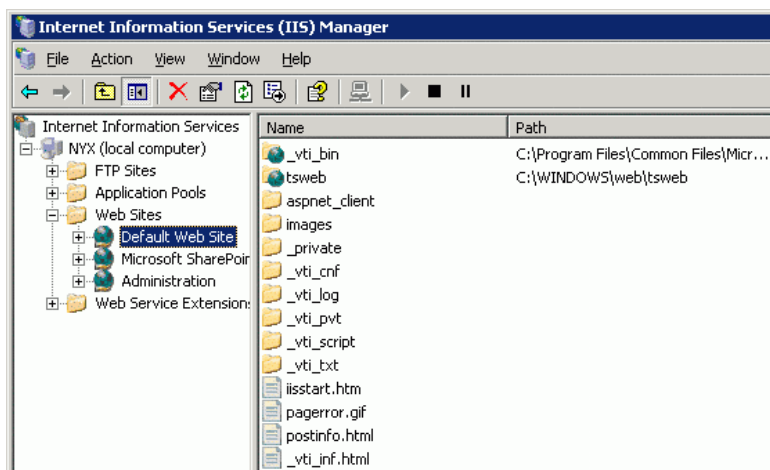
### ***Import certyfikatu urzędów końcowych CC Signet - CA Klasa 1 i CA Klasa 2***

Certyfikaty urzędów końcowych CC Signet - CA Klasa 1 (ca1\_pem.crt) i CC Signet - CA klasa 2 (ca2\_pem.crt) importujemy do tego samego magazynu i według identycznego schematu jak certyfikat urzędu pośredniego CC Signet - PCA Klasa 2.

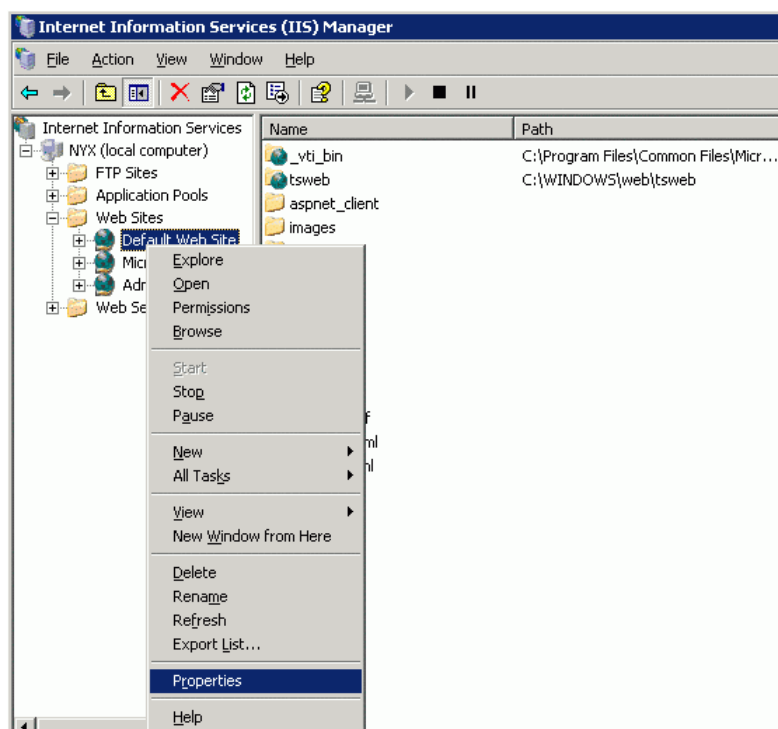
## Generowanie pary kluczy oraz wniosku o certyfikat CSR

Pierwszym krokiem do pozyskania certyfikatu dla serwera jest wygenerowanie pary kluczy kryptograficznych (są one generowane w procesie tworzenia CSR) oraz poprawnego wniosku o certyfikat. Aby utworzyć nowy wniosek o certyfikat należy przejść następujące kroki:

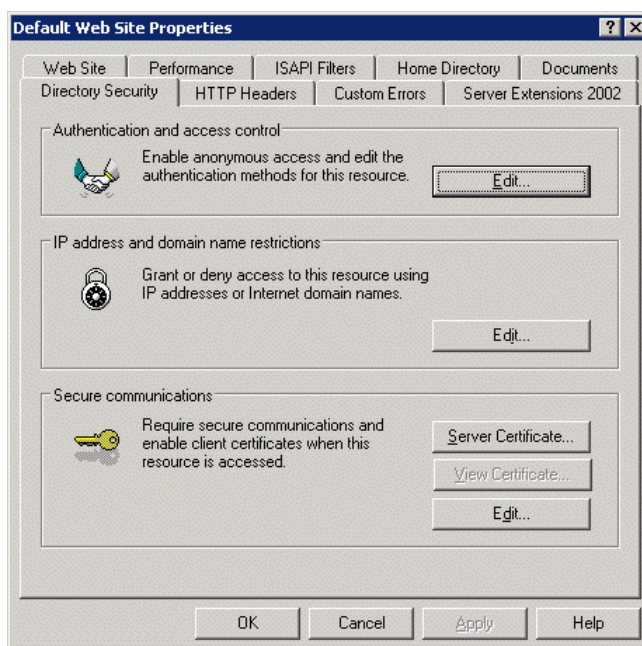
Otwieramy **Internet Services Manager** (lub konsolę MMC zawierającą snap-in IIS)



Przechodzimy do strony, dla której chcemy uruchomić bezpieczną komunikację po SSL/TLS.



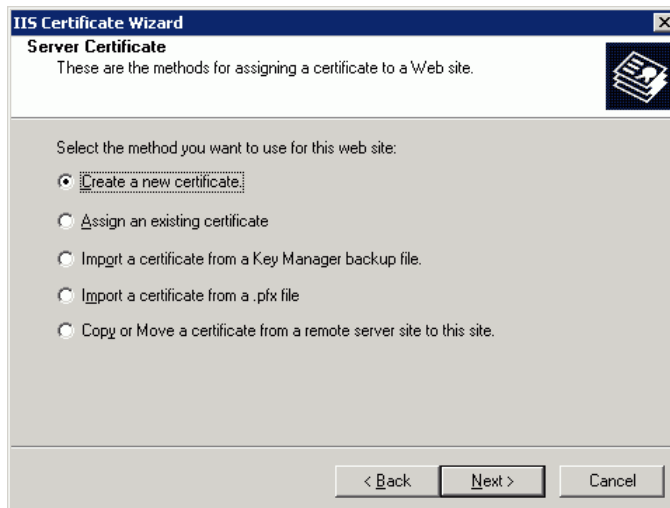
Klikamy prawym klawiszem myszy na wybranej stronie i przechodzimy do właściwości - **Properties**.



Przechodzimy do zakładki *Directory Security*.  
W sekcji *Secure communications* klikamy na *Server Certificate*.



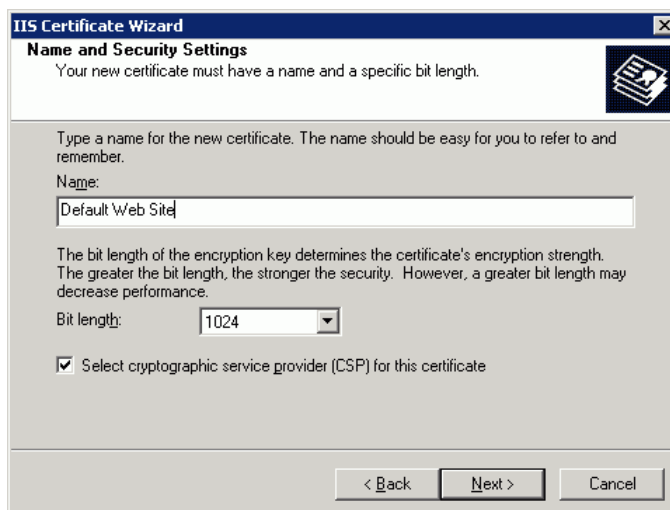
Uruchamiamy kreatora klikając *Next*.



Wybieramy opcję *Create a new certificate* i klikamy *Next*.



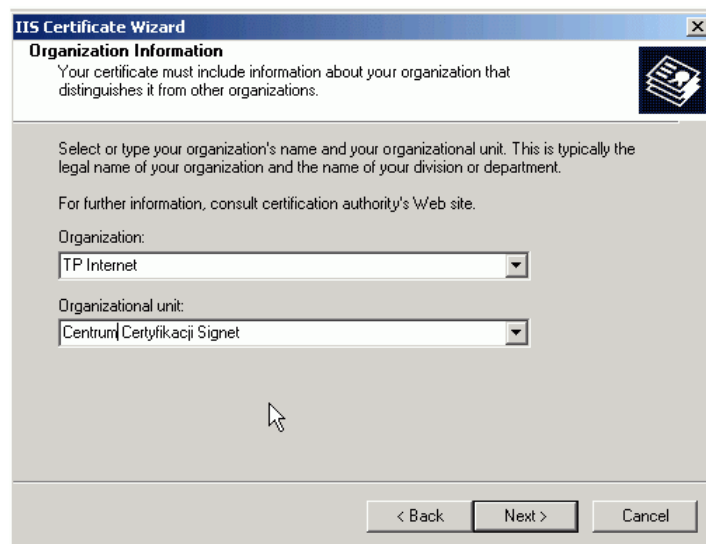
Wybieramy *Prepare the request now, but send it later* i klikamy *Next*.



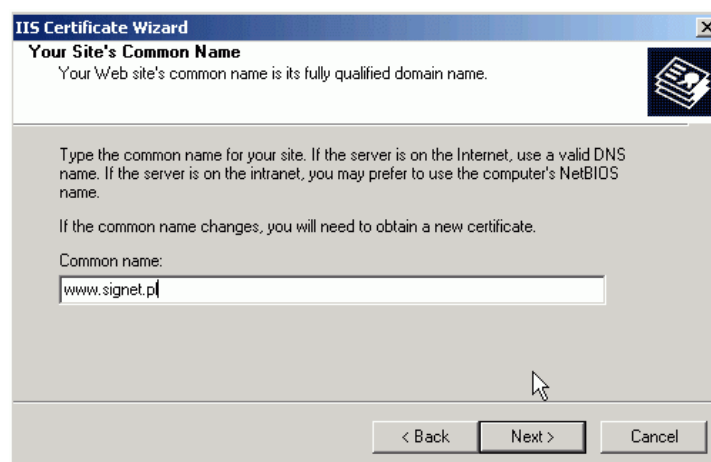
Wybieramy nazwę dla certyfikatu, długość klucza i klikamy *Next*.



Wybieramy dostawcę usług kryptograficznych. Jeśli nie wiesz, którego wybrać zalecamy *Microsoft RSA SChannel Cryptographic Provider*. Klikamy *Next*.



Wpisujemy nazwę organizacji np. nazwa firmy oraz jednostki organizacyjnej np. dział w firmie. Klikamy *Next*.



Wpisujemy nazwę DNS serwera.

The screenshot shows the 'IIS Certificate Wizard' window at the 'Geographical Information' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Geographical Information' and 'The certification authority requires the following geographical information.' There are three dropdown menus: 'Country/Region' with 'PL (Poland)' selected, 'State/province' with 'MAZ' selected, and 'City/locality' with 'Warszawa' 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 right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Wpisujemy nazwę kraju, województwa i miasta. Klikamy **Next**.

The screenshot shows the 'IIS Certificate Wizard' window at the 'Certificate Request File Name' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Certificate Request File Name' and 'Your certificate request is saved as a text file with the file name you specify.' There is a text box labeled 'File name:' containing 'c:\certreq.txt' and a 'Browse...' button to its right. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Wybieramy ścieżkę zapisu oraz nazwę dla utworzonego wniosku. Wniosek zawiera klucz publiczny serwera oraz wszystkie dane, które zostały wprowadzone w procesie jego tworzenia. Klikamy **Next** i zapisujemy go na dysk.

The screenshot shows the 'IIS Certificate Wizard' window at the 'Request File Summary' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Request File Summary' and 'You have chosen to generate a request file.' It instructs the user: 'To generate the following request, click Next.' The 'File name' is listed as 'f:\certreq.txt'. Below this, it says 'Your request contains the following information:' followed by a table of details.

Issued To	www.signet.pl
Friendly Name	Default Web Site
Country / Region	PL
State / Province	Mazowieckie
City	Warszawa
Organization	TP Internet
Organizational Unit	Centrum Certyfikacji Signet

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Wyświetlone zostaje podsumowanie procesu tworzenia wniosku. Klikamy **Next**.



Proces generacji wniosku został zakończony sukcesem. Klikamy **Finish**, aby zamknąć kreatora.

## Proces pobierania certyfikatu z CC Signet

Wygenerowany przez Państwa wniosek o certyfikat powinien mieć następujący format:

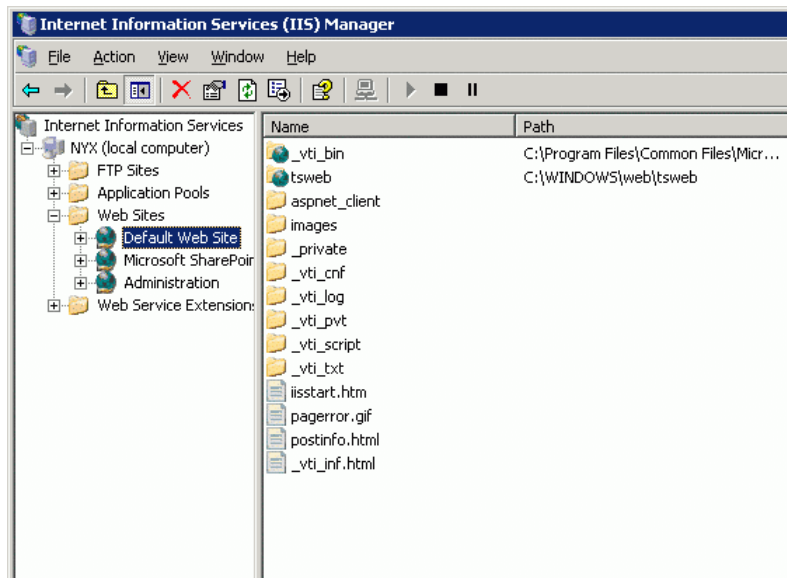
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDIDCCAokCAQAwYoxFjAUBGNVBAMTDXd3dy5zaWduZXQucGwxJDAlBgNVBAsT
G0N1bnRydW0gQ2VydHlmaWthY2ppIFNpZ25ldEUMBIGAlUEChMLVFAgSW50ZXJu
ZXQxETAPBgNVBACTCFdhcnN6YXdhMRQwEgYDVQQIEwtNYXpvd211Y2tpZTELMakG
AlUEBhMCUEwWgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOA3nspwlsGo+M/
wCcpz3zG2o3KEAAFfMhMxoypp+3y jQx8GbCf0YBeDYrWb1Tns5PcVBlApekB8eN8
cM6wjCcubjai xv95DVO86JCyZBzi jEyfxfyMvaffi028CIuElxUP8cCpy/lo4dtq
9hJM5b3lPqalNp/D3oiXxxaRKAq9AgMBAAGgggFTMBoGCisGAQQBgjcNAgMxDBYK
NS4wLjIxOTUuMjAlBgorBgEEAYI3AgEOMScwJTAOBgNVHQ8BAf8EBAMCBPAwEwYD
VR0lBAwwCgYIKwYBBQUHAWEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGKA
YwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHKA
cAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQBfE24DPqBw
Fp1R15/xZDY8Cugoxbyymtwq/tAPZ6dzPr9Zy30NnkQbKcsbLR/4t9/tWJIMmrF
hZonrx12qBfICoiKUXreSK890ILrLEto1frm/dycoXHhStSsZdm25vszv827FKKk
5bRW/vIEBqfKnEPJHonoig6UscvgA8QfgAAAAAAAAAAMA0GCSqGSIb3DQEBBQUA
A4GBAAw/Tv+0jgzRLNKTH/TL3DgPy0fispn+AB15Kqdl7QIearujNNxlYJgXpoKi
awDx18o0QR2UEzzcL/wp9ZOcSU6KHSxtv5yqqC2j7fOHSf11NEb5aX61SC/KUnky
ePacDb8UhdU/o44m/Lptua2fp2jIOZLaX/GpPTzCTDgWCL6Y
-----END NEW CERTIFICATE REQUEST-----
```

Aby otrzymać certyfikat, wygenerowany wniosek należy wkleić na podstronie serwisu [www.signet.pl](http://www.signet.pl) Centrum Certyfikacji Signet oraz przejść procedurę dla produktu, na który się Państwo zdecydujecie. CC Signet sprawdzi poprawność wniosku i po spełnieniu wymagań określonych dla danego produktu odeśle klucz publiczny Państwa serwera opatrzony certyfikatem.

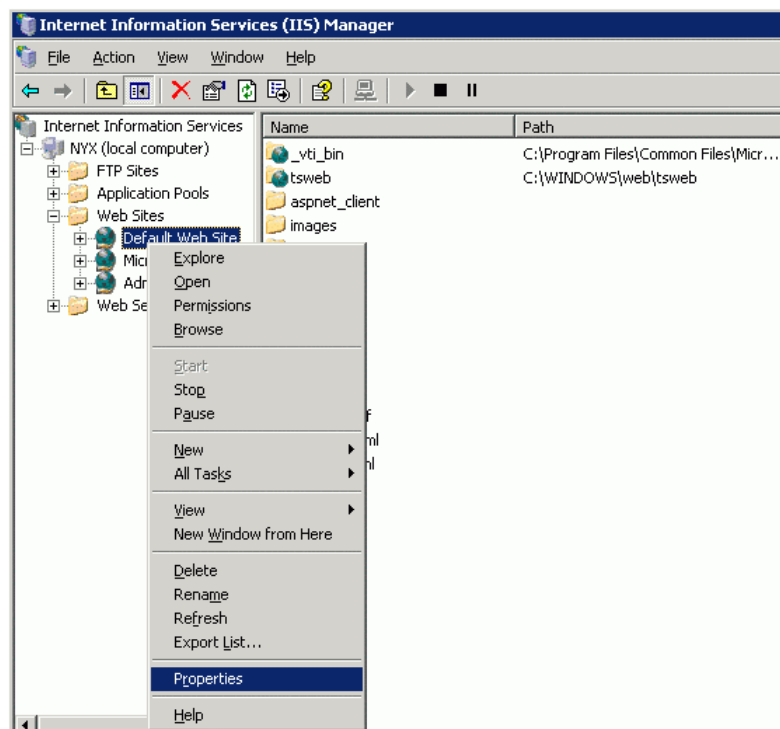
## Instalacja certyfikatu na serwerze

W celu zainstalowania certyfikatu na serwerze należy wykonać następujące kroki:

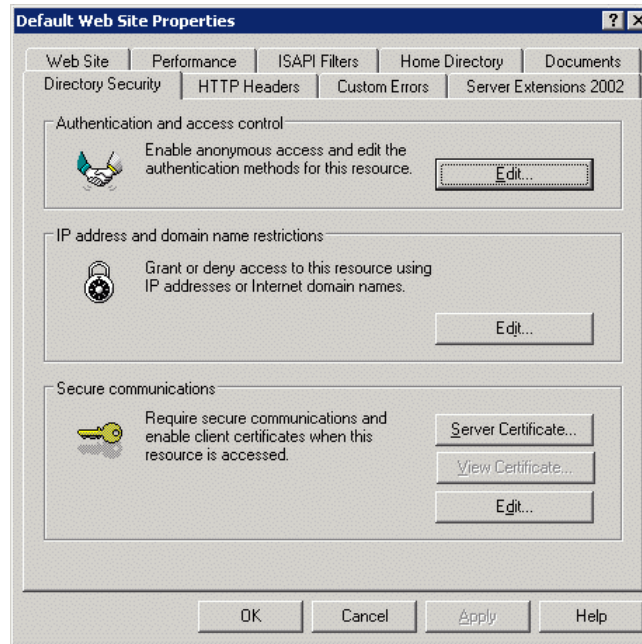
Otwieramy **Internet Services Manager** (lub konsolę MMC zawierającą snap-in IIS).



Przechodzimy do strony, dla której generowaliśmy wniosek o certyfikat.



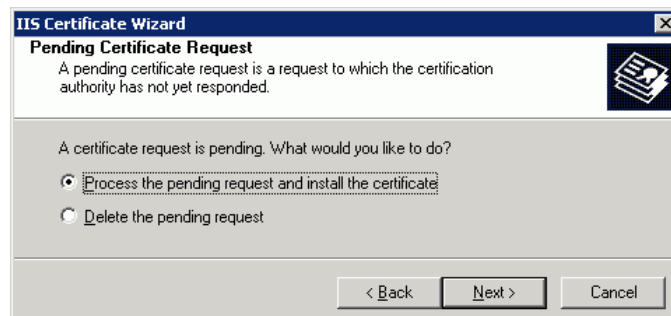
Klikamy prawym klawiszem myszy na wybranej stronie i przechodzimy do właściwości - **Properties**.



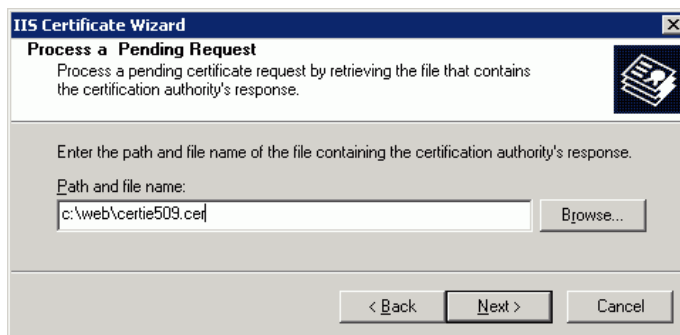
Przechodzimy do zakładki *Directory Security*.  
 W sekcji *Secure communications* klikamy na *Server Certificate*.



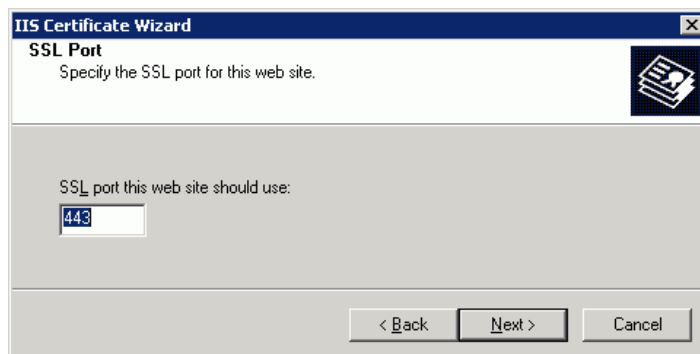
Uruchamiamy kreatora klikając *Next*.



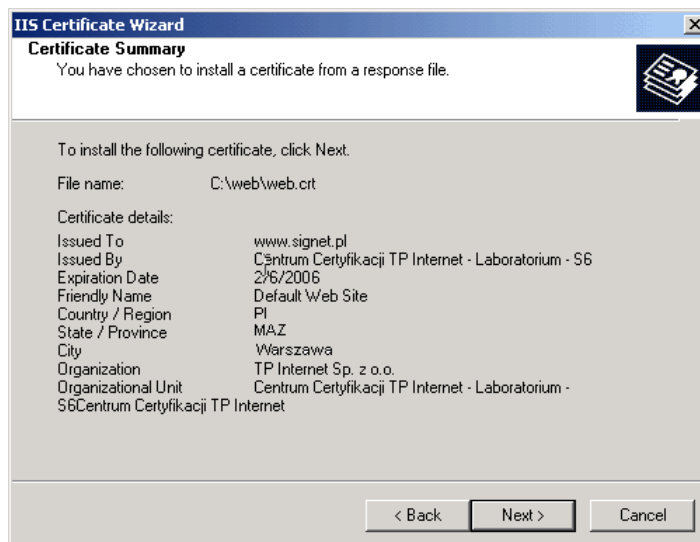
Wybieramy *Process the Pending Request and Install the Certificate*.  
 Klikamy *Next*.



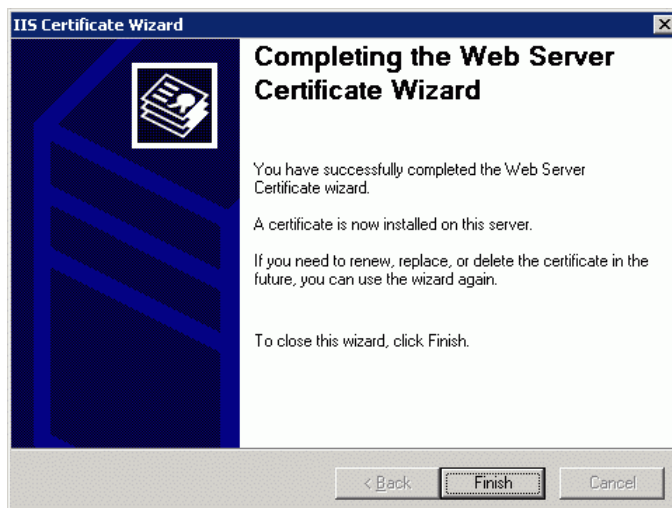
Klikamy **Browse** i podajemy ścieżkę do pliku z certyfikatem. Klikamy **Next**.



Wybieramy port, który serwer będzie wykorzystywał do połączeń SSL/TLS. Domyślnym jest port 443. Klikamy **Next**.



Widzimy ekran potwierdzający. Klikamy **Next**.



Zainstalowany został certyfikat na serwerze. Klikamy **Finish**, aby zamknąć kreatora.

Przetestuj swój serwis, aby mieć pewność, że SSL działa poprawnie.

[https://adres\\_twojej\\_strony](https://adres_twojej_strony).