

UNIZETO



POWSZECHNE  
CENTRUM CERTYFIKACJI



instrukcja użytkownika

# Internet Information Service (IIS) 7.0

Konfiguracja protokołu SSL w oprogramowaniu

Internet Information Services 7.0

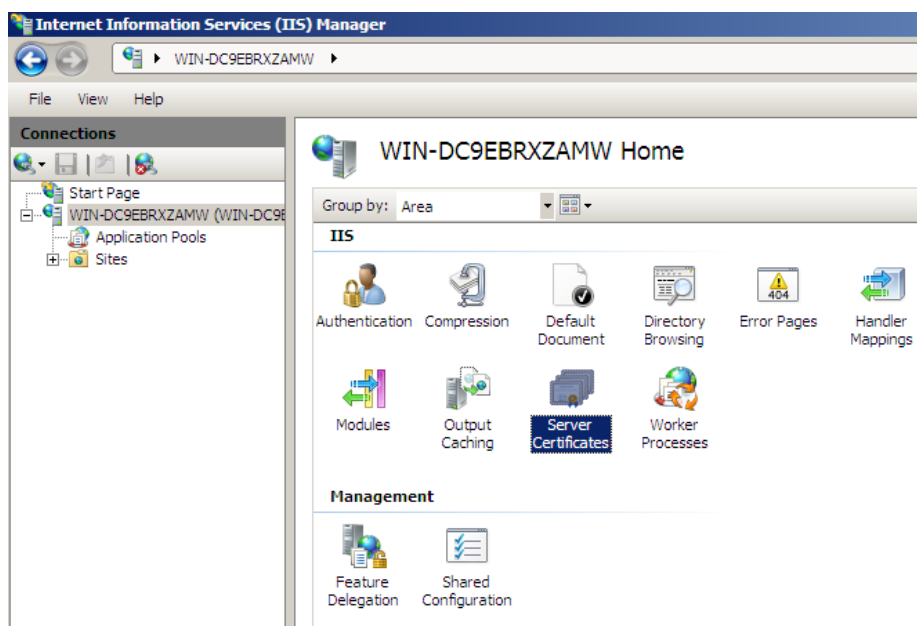
wersja 1.2

## Spis treści

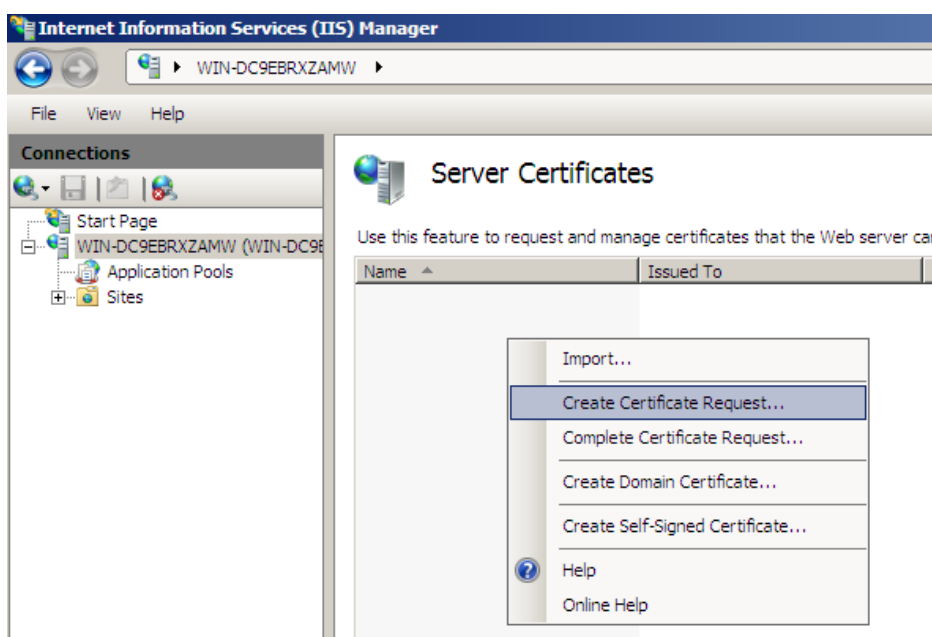
1. GENEROWANIE ŻĄDANIA .....	3
2. WYSYŁANIE ŻĄDANIA DO CERTUM .....	5
3. INSTALACJA CERTYFIKATÓW NA SERWERZE.....	7
4. UWIERZYTELNIANIE KLIENTÓW NA PODSTAWIE CERTYFIKATÓW KLUCZA PUBLICZNEGO. ....	12
5. WYKONYWANIE KOPII ZAPASOWEJ KLUCZA PRYWATNEGO I CERTYFIKATU .....	17

## 1. Generowanie żądania

Konfigurację protokołu SSL w serwerze Internet Information Services należy rozpocząć od wygenerowania żądania wystawienia certyfikatu. Aby tego dokonać należy uruchomić Menedżera konfiguracji IIS i w prawym panelu kliknąć na węzeł z nazwą konfigurowanego serwera. W prawym panelu należy dwukrotnie kliknąć ikonę „Certyfikaty Serwera” (ang. „Server Certificates”):



W nowo utworzonym oknie należy kliknąć prawym przyciskiem myszy i z menu kontekstowego wybrać polecenie utworzenia nowego żądania certyfikatu (ang. Create certificate Request).



Zostanie uruchomiony kreator przeprowadzający proces generowania żądania. Pierwszym krokiem jest podanie informacji o podmiocie, które zostaną umieszczone w certyfikacie.

**Request Certificate** [?] [X]

**Distinguished Name Properties**

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

Organizational unit:

City/locality:

State/province:

Country/region:

Previous Next Finish Cancel

Najważniejszym polem jest „Nazwa powszechna” (ang. Common Name). Należy tam wpisać nazwę serwera, pod jaką będzie dostępny serwer w sieci. Na przykład jeżeli strona WWW będzie dostępna pod adresem <http://mojafirma.pl> to w tym polu należy umieścić [mojafirma.pl](http://mojafirma.pl). Jeżeli planowany jest zakup certyfikatu typu wildcard to przed nazwą domeny należy dopisać gwiazdkę i kropkę. Nazwą powszechną w takim przypadku powinien być ciąg znaków \*.mojafirma.pl.

Należy także zwrócić uwagę na kolejne pola. W szczególności należy zwrócić uwagę na pola Organizacja, Miasto, Województwo oraz Kraj. Należy wypełnić je zgodnie ze stanem faktycznym, gdyż CERTUM będzie weryfikować poprawność podanych danych.

Po upewnieniu się, że wprowadzone dane są poprawne należy kliknąć przycisk Dalej.

Kolejnym krokiem jest dobór parametrów generowanej pary kluczy. Należy wybrać klucz RSA o długości przynajmniej 2048 bit.

**Uwaga!** CERTUM nie certyfikuje kluczy o długości mniejszej niż 2048! Jest to związane z wymaganiami NIST dotyczącymi długości kluczy kryptograficznych.

Ostatnią częścią procesu wysyłania żądania jest wybór miejsca, w którym zostanie ono zapisane. Po wskazaniu nazwy pliku zostanie wygenerowana para kluczy oraz zapisane zostanie żądanie.

## 2. Wysyłanie żądania do CERTUM

Po zalogowaniu do systemu CERTUM, mając wygenerowane żądanie oraz złożone zamówienie w sklepie, wypełniamy formularz zgłoszeniowy i wklejamy żądanie CSR na stronie CERTUM. W tym celu wybierz menu **Aktywacja certyfikatów**. Następnie wybierz typ certyfikatu SSL i aktywuj go przyciskiem **Aktywuj**.

PRODUKTY POMOC O FIRMIE Szukaj w sklepie

Strona główna » Moje konto » Aktywacja certyfikatów

Kody elektroniczne  
**Aktywacja certyfikatów**  
Zarządzanie certyfikatami  
Historia zamówień  
Dane adresowe  
Narzędzia  
Newsletter

### Aktywacja certyfikatów

Nazwa usługi: Commercial SSL  
Status aktywacji:   
Numer zamówienia:   
Status płatności:   
**Szukaj**

Nazwa usługi	Data zamówienia	Numer zamówienia	Status płatności	Status aktywacji
Commercial SSL, 1 rok Wydanie	20 lipca 2011	ZoZE/026009/MS/20/07/2011	Oczekiwanie na płatność	Certyfikat nieaktywny

**Aktywuj**

Wybierz **CSR** jako sposób dostarczenia klucza do certyfikatu. Następnie przejdź do kolejnego kroku przyciskiem **Dalej**.

PRODUKTY POMOC O FIRMIE Szukaj w sklepie

Strona główna » Moje konto » Edycja szczegółów aktywacji

Kody elektroniczne  
**Aktywacja certyfikatów**  
Zarządzanie certyfikatami  
Historia zamówień  
Dane adresowe  
Narzędzia  
Newsletter

### Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi: **Commercial SSL, 1 rok Wydanie**

Wybierz sposób dostarczenia kluczy dla certyfikatu  
 Generowanie pary kluczy  
 CSR

Szczegółowe informacje na temat sposobów przygotowania żądania CSR, uzyskasz w zakładce Pomoc lub za pośrednictwem operatora naszej infolinii.

**Dalej >>**

Wklej **żądanie CSR**, przejdź do kolejnego kroku przyciskiem **Dalej**.

PRODUKTY POMOC O FIRMIE Szukaj w sklepie

Strona główna » Moje konto » Edycja szczegółów aktywacji

Kody elektroniczne  
Aktywacja certyfikatów  
Zarządzanie certyfikatami  
Historia zamówień  
Dane adresowe  
Narzędzia  
Newsletter

### Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi: Commercial SSL, 1 rok  
Wydanie

CSR \*

```
-----BEGIN CERTIFICATE REQUEST-----
MIICCAQAYCAQAwVjE1MAkGA1UEBhMCU2EwDQYJKoZIhvcNAQEBBQADSwAwSAJB
LnBzMIIBIjANBgkqhkiG9w0BAQEFAAQCAQ8AMIIBIjCgYCAQEAlnawcFJLXACTJG+
eeQWSeoD8dy6GTWUjvd29QjF17FYeeRUS1CefKjbd4d6cmUGNnsDIYH/q3pLE
N4v4jK4e9gTUheYvLcobF9bYpRXIiANMsOa3mU1J4n9Dg2dEx098q299198NRQ
7sn1puCu/LkOeGesuR1eXm8vCZF+Y1ju2+o1QFG+JL7NuIN8jST3vts8vuc84fI
Z1FX1qvCJ2+1FCZK2H9W6K/cob6G0VQavU5zb3V5IbnVwOHe+nAK1U7e1ZegDcH
bHq2cansUVR471993CSBSIUegkxjWFl4vFE012HPh3jmvDb4CgkRbBmq06
7epYB+1DAQASoaAaQVY7toZ1hvch2QF8Q2d9g8BAMNbo0UNW0e4+5D98NT6gVv
d99g4CSkbtUcobNdM2zPelMcOvrvZ0PpSR/Gr5eS6N8eHbt5NhsVLoRjLkCIXS/z
71h/datjSv1pVd1U9q1A0suR729suQd9jP1MRVX1mu/ua3kgwHe3XpSAK80Gzvv
IdBBOZB89Vp0p0aYcLKJbqoBsanFv2zocrcayY1MgW5T8mXatazBqDYA27VH2ZFF
DF8x2fKdqeKawI/+mYQCUV7M0AVSx76pavvF4qbuemJ36McUuYy5c0uIt/DyJ
JV5TMI11YH1ynNeeFj2DnH8MTvRvT2UACWb1Pz4j6nxV5Q1Lp4WNSG0W718FE=
-----END CERTIFICATE REQUEST-----
```

<< Wstecz 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).

PRODUKTY POMOC O FIRMIE Szukaj w sklepie

Strona główna » Moje konto » Edycja szczegółów aktywacji

Kody elektroniczne  
Aktywacja certyfikatów  
Zarządzanie certyfikatami  
Historia zamówień  
Dane adresowe  
Narzędzia  
Newsletter

### Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi: Commercial SSL, 1 rok  
Wydanie

Dane do certyfikatu:

Początek ważności certyfikatu: 2011-07-20

Koniec ważności certyfikatu: 2012-07-19

Domena \*: moja.domena.pl

Kraj \*: Polska

Email: mojadres@moja.domena.pl

<< Wstecz 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 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**.

**Aktywacja**

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi: **Commercial SSL, 1 rok**  
Wydanie

---

**Dane do certyfikatu:**

Początek ważności certyfikatu: 20 lipca 2011  
Koniec ważności certyfikatu: 19 lipca 2012  
Kraj: Polska  
Email: mojadres@moja.domena.pl  
Domena: moja.domena.pl

**Prosimy o dokładną weryfikację danych do certyfikatu. Po dokonaniu aktywacji usługi, zmiana danych nie będzie możliwa.**

---

**Struktura certyfikatu:**

Podmiot: E=mojadres@moja.domena.pl,  
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 (KPC), kt6w, przez nczw6lanie, state, sie, integralna, cz6cicia, niniejszego, oświadczenia...Kodeks Post6powania.

Potwierdzam oświadczenie \*

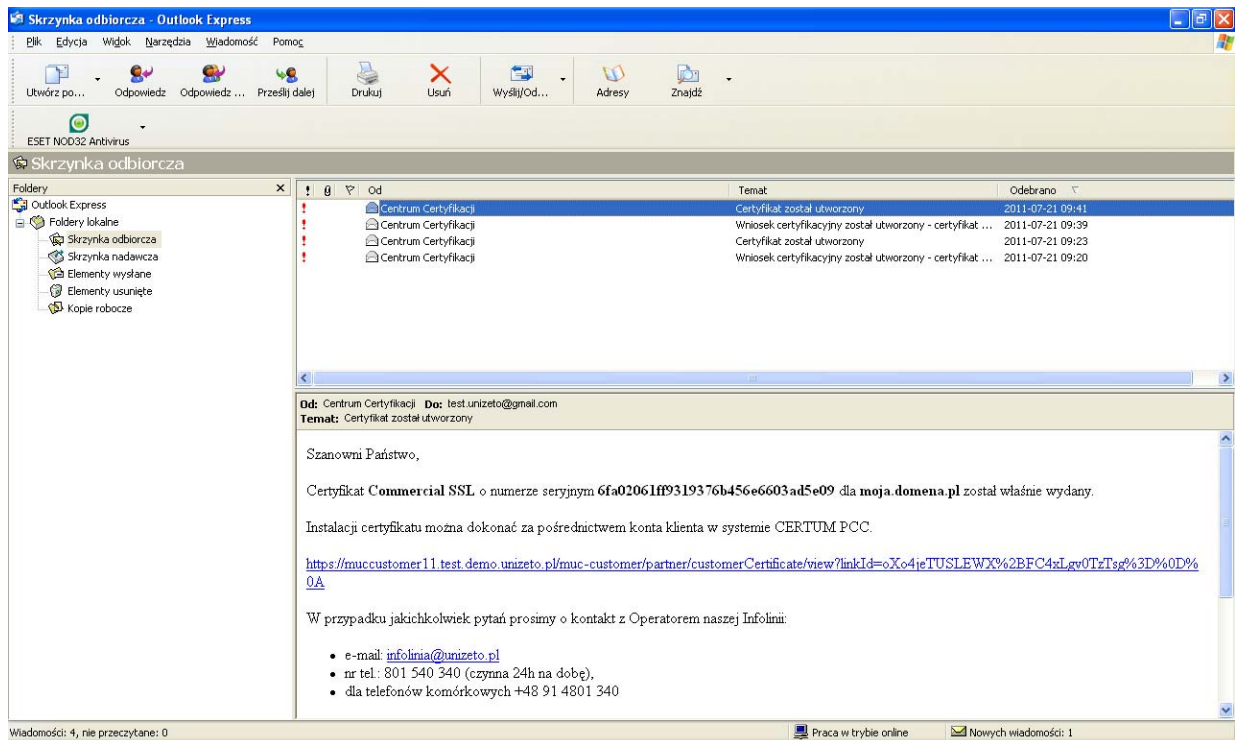
**<< Wstecz Aktywuj**

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

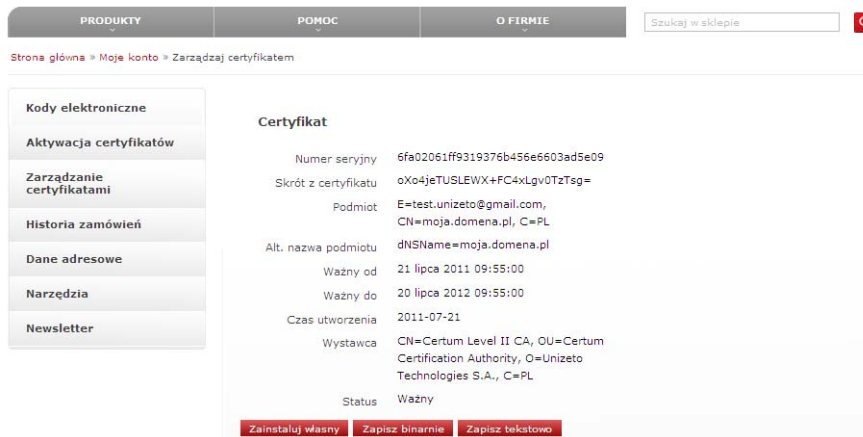
### 3. Instalacja certyfikat6w na serwerze

Po wykonaniu powyższej procedury z poprzedniego punktu otrzymamy stosownego e-maila z linkiem instalacyjnym umożliwiającym aktywacj6 certyfikatu (umieszczenie certyfikatu w naszym repozytorium dost6pnym na stronach www).

W tym celu naleŹy odebrać email a nast6pnie post6pować zgodnie z treściami wiadomoŹci.

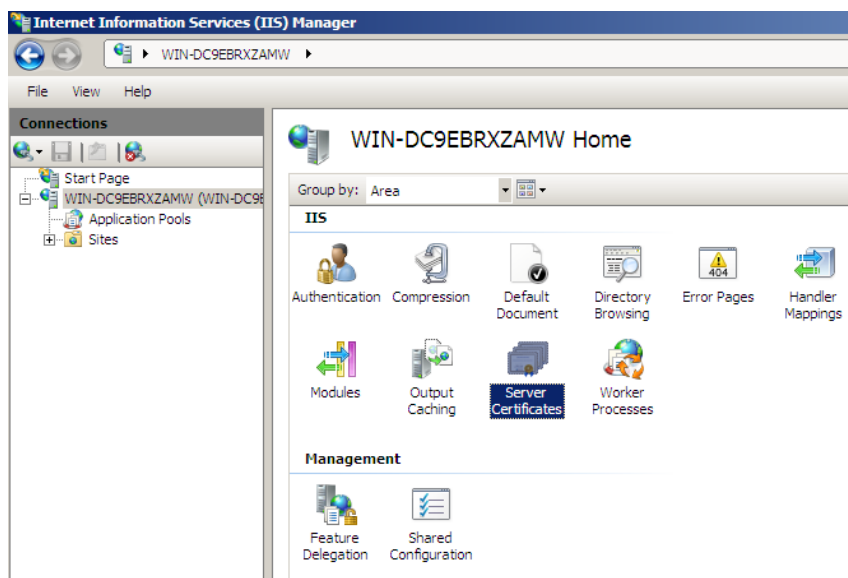


Po kliknięciu na link instalacyjny, na ekranie pojawi się strona WWW.



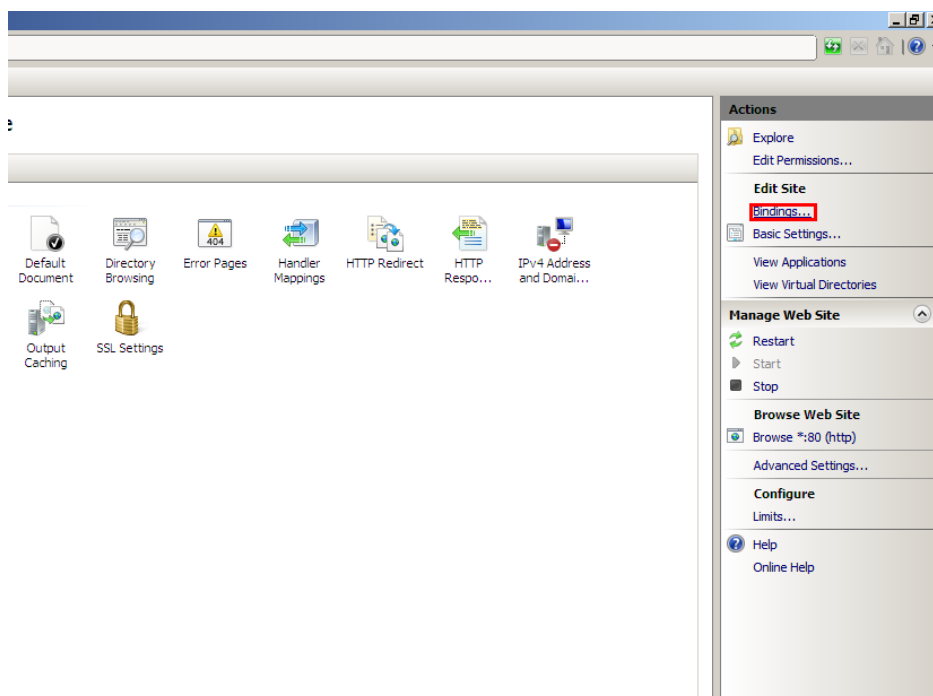
Zapisz certyfikat w postaci tekstowej \*.pem

Następnie proszę uruchomić Menedżera serwera IIS, kliknąć na węzeł z nazwą konfigurowanego serwera i dwukrotnie kliknąć na ikonę „Certyfikaty serwera”:

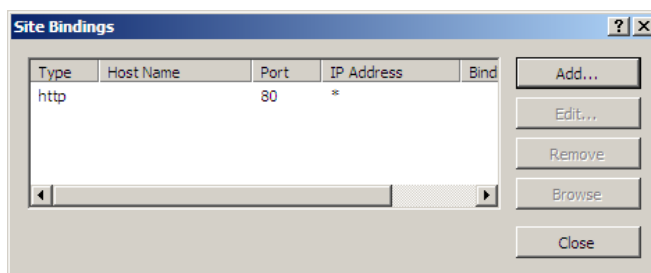


Następnie należy kliknąć prawym przyciskiem myszy w otwartym oknie i z menu kontekstowego wybrać pozycję kończenia rozpoczętego żądania (ang. „Complete Certificate Request”). W oknie dialogowym należy wskazać plik z certyfikatem zapisanym na dysku.

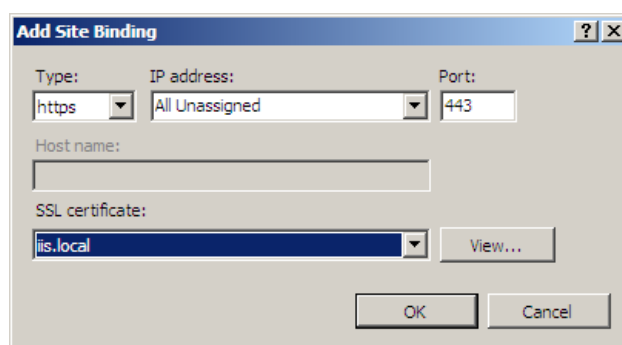
Kolejnym elementem do ustawienia są porty, na których ma nasłuchiwać serwer WWW. Wybieramy stronę WWW do konfiguracji i z menu po prawej stronie okna pozycję „Bindings”:



Po kliknięciu na ten odnośnik pojawi się następujące okno:



Następnie należy kliknąć przycisk „Add...” i w oknie pokazanym na kolejnym rysunku ustawić parametry protokołu SSL.



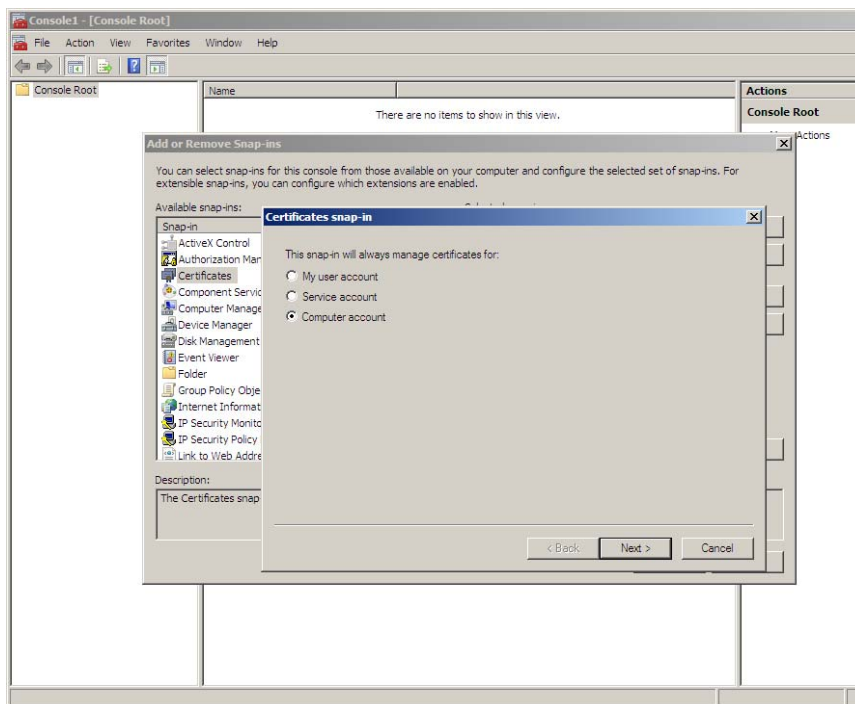
Pierwszym elementem do zmiany jest typ protokołu. Należy ustawić tę wartość na https. Drugim ważnym elementem jest klucz prywatny i pasujący do niego certyfikat, który będzie zabezpieczał witrynę. Z rozwijalnego menu w dolnej części okna należy wybrać uprzednio zainstalowany certyfikat. Na koniec proszę wcisnąć przycisk OK.

**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 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.

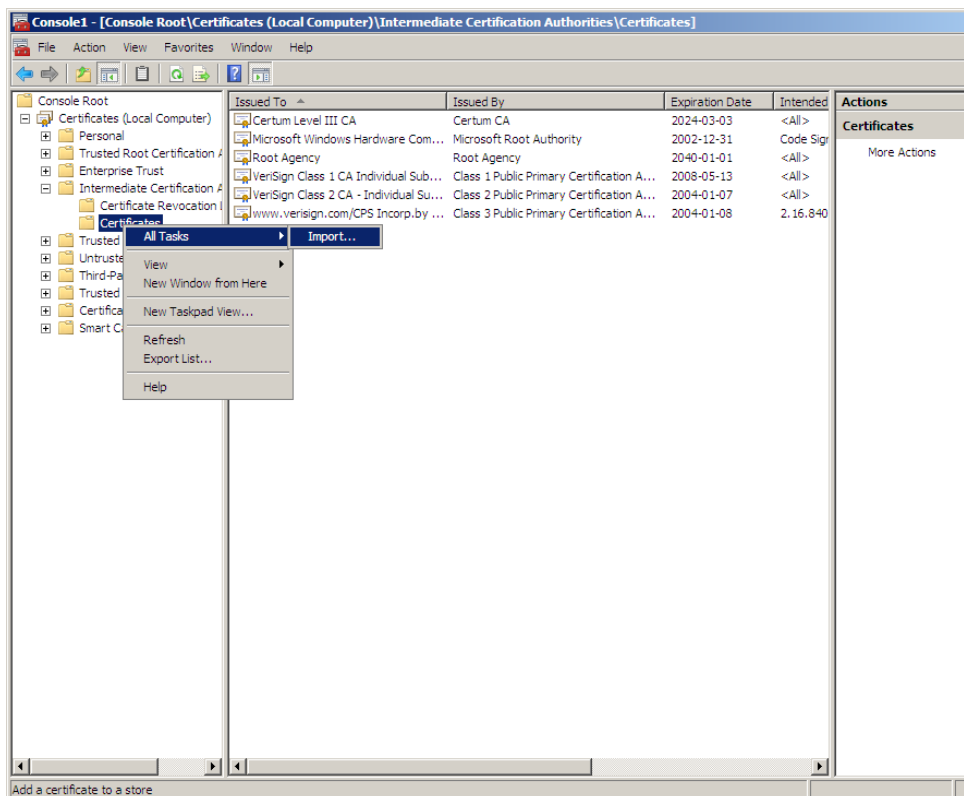
Proszę wcisnąć kombinację klawiszy [WinKey + R] wpisać polecenie mmc.exe. Zostanie uruchomiony edytor przystawek MMC. Z menu „Plik” należy wybrać pozycję „Dodaj/Usuń przystawkę”. W nowym oknie trzeba kliknąć przycisk „Dodaj” a następnie wskazać przystawkę „Certyfikaty” i wcisnąć przycisk „Dodaj”.

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”.

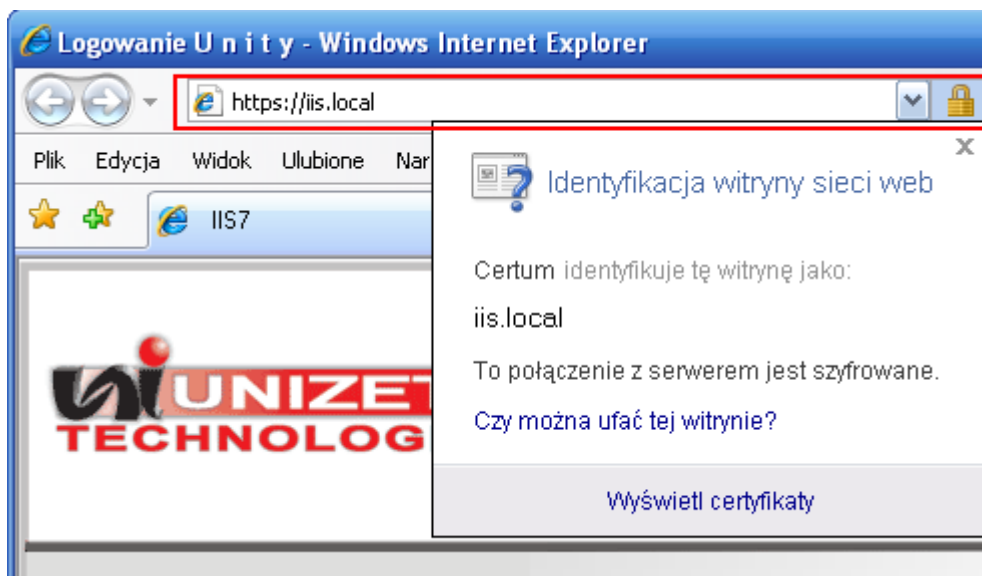
W lewym panelu nowo otwartego okna proszę rozwinąć gałąź „Certyfikaty urzędów pośrednich”. Proszę kliknąć prawym przyciskiem myszy na folder „Certyfikaty” i z menu kontekstowego wybrać pozycję „Wszystkie zadania” a następnie „Importuj...”.



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 Certum Level II CA, Certum Level III CA, oraz Certum Level IV CA.

Instalacja certyfikatu została ukończona. Aby sprawdzić, czy instalacja jest poprawna należy wejść na zabezpieczoną stronę WWW. Jeśli przy pasku adresu pojawi się ikona z kłódką oznacza to, że połączenie jest szyfrowane a przeglądarka poprawnie zweryfikowała wystawcę certyfikatu:



#### 4. Uwierzytelnianie klientów na podstawie certyfikatów klucza publicznego.

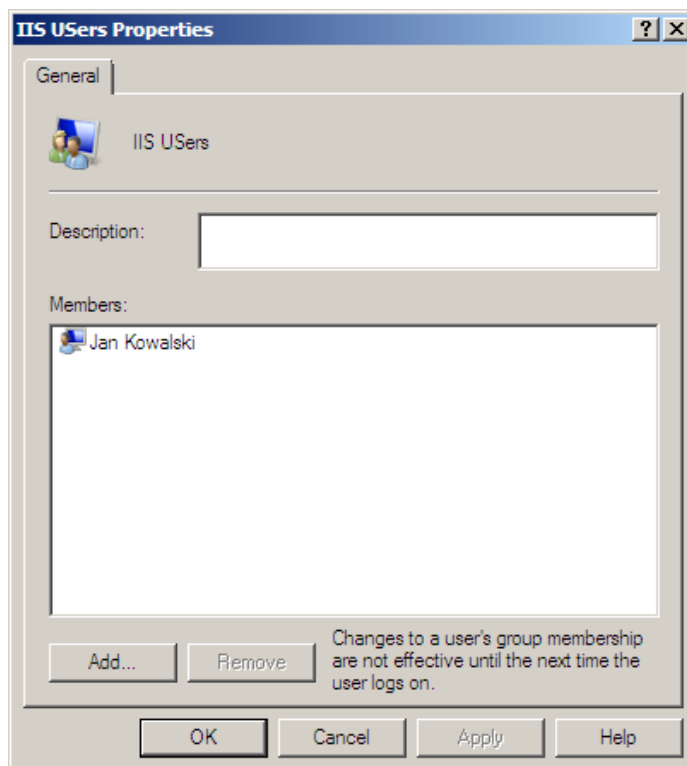
Wraz z wprowadzeniem wersji 3 protokołu SSL możliwe stało się uwierzytelnianie dwustronne. W standardowej konfiguracji serwera SSL możliwe jest tylko uwierzytelnianie serwera na podstawie jego certyfikatu. Konfiguracja uwierzytelniania dwustronnego umożliwia kontrolowanie dostępu do serwera z użyciem silnej kryptografii. Użytkownicy nie uwierzytelniają się za pomocą nazwy użytkownika i hasła, lecz za pomocą podpisu cyfrowego. Klucz prywatny i certyfikat mogą być przechowywane w magazynie określonej przeglądarki, toteż dostęp do witryny jest ściśle ograniczony. Do uwierzytelniania dwustronnego potrzeba zarówno certyfikatu serwera jak i certyfikatów klienta. Mogą to być na przykład kombinacja Certum Enterprise ID i Certum Professional ID.

Aby skonfigurować uwierzytelnianie należy postępować zgodnie z następującymi krokami.

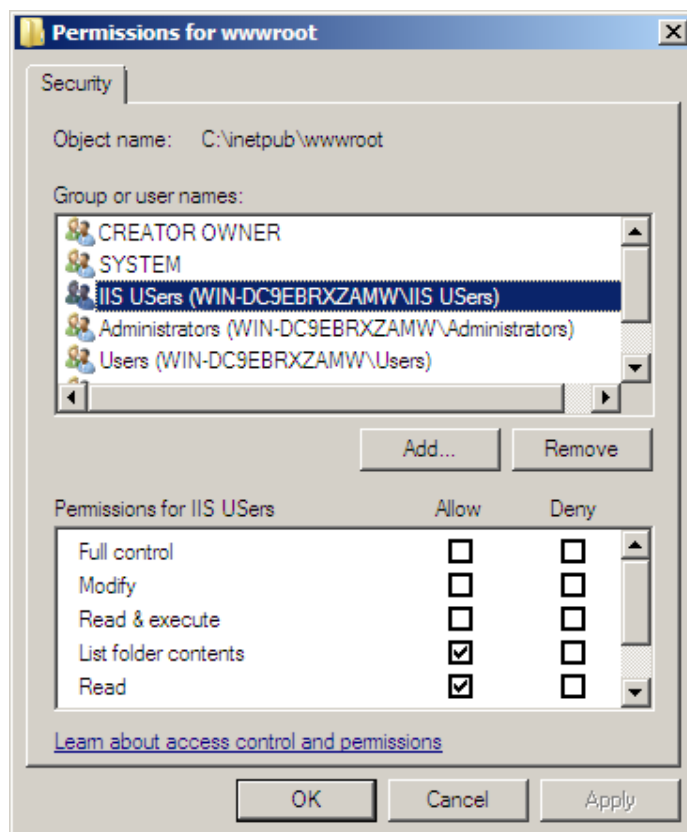
Pierwszym krokiem powinno być utworzenie kont użytkowników w systemie operacyjnym z zainstalowanym serwerem IIS.

W oknie „Uruchom” (Winkey + R) należy wpisać „compmgmt.msc” i w prawym panelu nowego okna przejść do węzła „Użytkownicy i grupy lokalne”. Proszę dodać grupę użytkowników korzystających z serwera WWW. Na potrzeby tego poradnika stworzono grupę „IIS Users”. Następnie proszę utworzyć i dodać żadaną ilość użytkowników i dodać ich do grupy „IIS Users”. Proszę nie zapomnieć o ustawieniu hasła tym użytkownikom.

**Uwaga!** Należy pamiętać o tym, że użytkownicy muszą mieć dokładnie takie same nazwy, jakie są wymienione w polu Common Name certyfikatu użytkowników!



Następnie należy ustawić odpowiednie uprawnienia do katalogu na serwerze, w którym przechowywana jest konfigurowana witryna WWW. Grupa „IIS Users” powinna mieć prawa do „Przeglądania zawartości folderu” i „Odczytu”. Przedstawiono to na obrazku poniżej.



W kolejnym kroku należy przygotować certyfikaty klienta na potrzeby serwera IIS. Konieczne będzie posiadanie certyfikatów klientów w postaci tekstowej. Jeśli wykorzystywane są certyfikaty CERTUM to można je uzyskać z naszego repozytorium. Proszę wejść na stronę [www.certum.pl](http://www.certum.pl) i z górnego paska wybrać „Obsługa certyfikatów” a następnie „Wyszukaj certyfikat”. Proszę wyszukać certyfikat niekwalifikowany o żądanej Nazwie powszechnej lub numerze seryjnym.

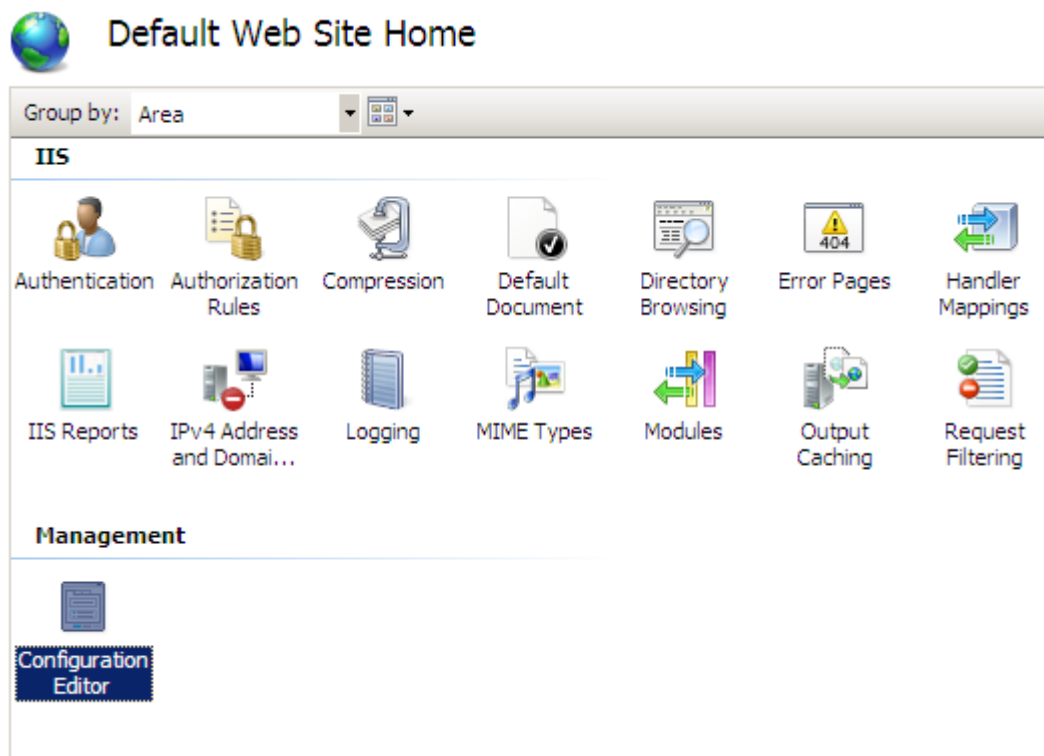
Po otwarciu pliku z certyfikatem w Notatniku lub innym edytorze tekstowym powinien ukazać się widok podobny do tego:

```
-----BEGIN CERTIFICATE-----
MIIEvTCCBCagAwIBAgIDBIFbMA0GCSqGSIb3DQEBBQUAMEQxCzAJBgNVBAYTA1BM
MRswGQYDVQQKEsJVbml6ZXRvIFNwLiB6IG8uby4xGDAWBgNVBAMTD0N1cnR1bSBM
ZXZ1bCBJVjAeFw0wOTAzMTAxMzE5MDFaFw0xMTAzMTE5MzE5MDFaMIHYMQswCQYD
VQQGEwJQTDEbMBkGA1UECBMSemFjaG9kbmlvcG9tb3Jza211MREwDwYDVQQHEWhT
emN6ZWNPbjEiMCAgA1UEChMZVW5pemV0byBUZWNobm9sb2dpZXMgUy5BLjE0MDIG
A1UECXMxRjQ0VSVFVNIkVud3N6ZWNObmUgQ2VudHJ1bSBkZXJ0eWZpa2FjamkgKFVD
KTEWMBQGA1UEAxMNSmFyb3NsYXcgTWlsYTenMCUGCSqGSIb3DQEJARYYamFyb3Ns
YXcubWlsYUB1bml6ZXRvLnBsMIGfMA0GCSqGSIb3DQEBQUAA4GNADCBiQKBggQDV
ZyhmN5kQY1x+Bk3vBKDoOzSYKpiFBOHkt1izIt1hLY/tVP0ByzKsFR//CtvCQHby
RhbkuTwLFUirNkqUPaAcwSeTMHiH3u3U3XwakpXDJQ0b55XK7w091ZVovxfyMGBw
ZDACz6uFa5eYdHFYwjxMrfZJm91Bfp637e/+hJE5mQIDAQABo4ICJjCCAiIwIwYD
VR0RBwwGoEYamFyb3NsYXcubWlsYUB1bml6ZXRvLnBsMAkGA1UdEwQCMAAwCwYD
VR0PBAQDAgTwMBEGCWCsGAGG+EIBAQQEAWIFoDAWBgNVHR8EKTAncMCWgI6Ahhhh9c
dHRwOi8vY3JsLmN1cnR1bS5wbC9jbGFzc2QuY3JsMF4GCCsGAQUFBwEBBFIwUDAh
BggrBgEFBQcwAYYVaHR0cDovL29jc3AuY2VydHVtLnBsMCAcGAQUFBzACChh9c
dHRwOi8vd3d3LmN1cnR1bS5wbC9jbGFzc2QuY3J0MIIBPAYDVR0gBIIBMzCCAS8w
ggErBgoqhGgBhvZ3AgIEMIIBGzAkBggrBgEFBQcCARYYaHR0cDovL3d3dy5jZXJ0
dW0ucGwvQ1BTMIHyBggrBgEFBQcCAjCB5TAgFh1Vbml6ZXRvIFR1Y2hub2xvZ211
cyBTLkEuMAMCAQEAgcBVc2FnZSBvZiB0aGlzIGN1cnR1bml6ZXRvIFR1Y2hub2xvZ211
dGx5IHN1YmplY3R1ZCB0byB0aGUgQ0VSVFVNIEN1cnR1bml6ZXRvIFR1Y2hub2xvZ211
Y2UgU3RhZGvtZW50ICChDUFMpIGluY29ycG9yYXR1ZCBieSBvZmVudWUyUgaGVy
ZWluIGFuZCBpb3NpdG9yeQphdCBodHRwczovL3d3dy5jZXJ0dW0ucGwvcmVwb3NpdG9yeS4wDQYJKoZIhvcNAQEFBQADgYEAZ63ueiinL/+WugVFSg+n
vRo2XNn6+SgJ+wcWYVJpnFPZ8WNfZydsdWltd1c0M1dBd7esy+Su2D1TKZbbhU7p
Bp8zxOnH7hXV1DuDhOPXlnpoab3tnh3QipNgJuEe1TfpKMwPUuXt2ETbnF9LsvbD
D1/txWwfp6yH4qoOvkz7LQc=
-----END CERTIFICATE-----
```

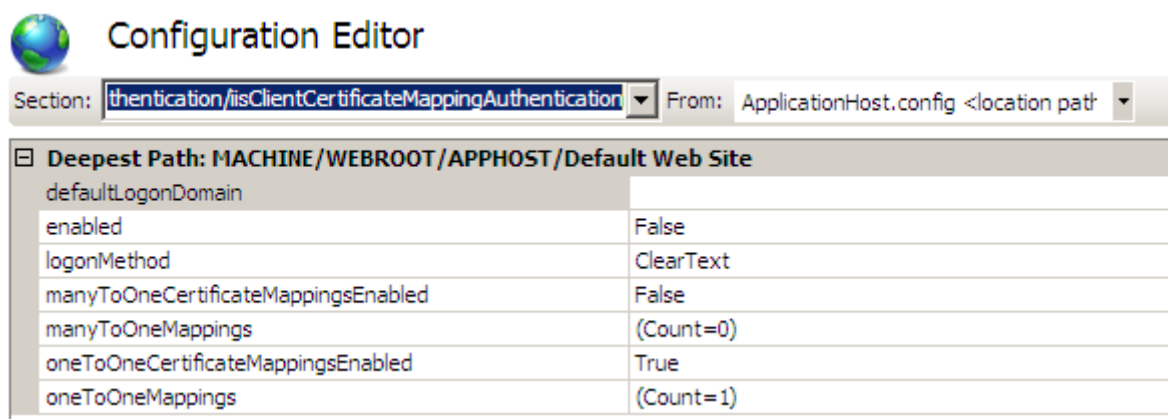
Należy usunąć znaczniki -----BEGIN CERTIFICATE----- oraz -----END CERTIFICATE----- . Następnie proszę usunąć wszystkie znaki nowej linii w tym pliku. Wszystkie litery, cyfry oraz znaki specjalne powinny znaleźć się w jednej linii. Czynności te należy powtórzyć dla wszystkich certyfikatów, jakimi mają się posługiwać klienci.

Kolejnym krokiem jest konfiguracja serwera IIS. Konieczne będzie zainstalowanie pakietu Administration Pack for IIS 7.0. Można go ściągnąć za darmo ze stron internetowych firmy Microsoft.

Po uruchomieniu Menedżera konfiguracji IIS proszę rozwinąć gałąź reprezentującą konfigurowaną witrynę. W prawym panelu proszę dwukrotnie kliknąć ikonę „Edytor konfiguracji”




Z rozwijalnego menu „Section” w Edytorze konfiguracji należy wybrać sekcję `system.webServer/security/authentication/iisClientCertificateMappingAuthentication`. Konieczne jest ustawienie parametrów tak, jak na przedstawionej grafice:



Najważniejsze jest tutaj pole `oneToOneMappings`. Jest to kolekcja użytkowników i certyfikatów, którym zezwoli się na logowanie na stronie WWW. Po wejściu do tego ustawienia pojawi się następujące okno:



Ostatnim krokiem jest włączenie sprawdzania certyfikatów przy wchodzeniu na stronę. Należy przejść do węzła odpowiadającego za konfigurację witryny i dwukrotnie kliknąć na ikonę ustawień protokołu SSL (ang. SSL Settings). Należy ustawić parametry tak, jak na rysunku.

 **SSL Settings**

This page lets you modify the SSL settings for the content of a Web site or application.

- Require SSL  
 Require 128-bit SSL

Client certificates:

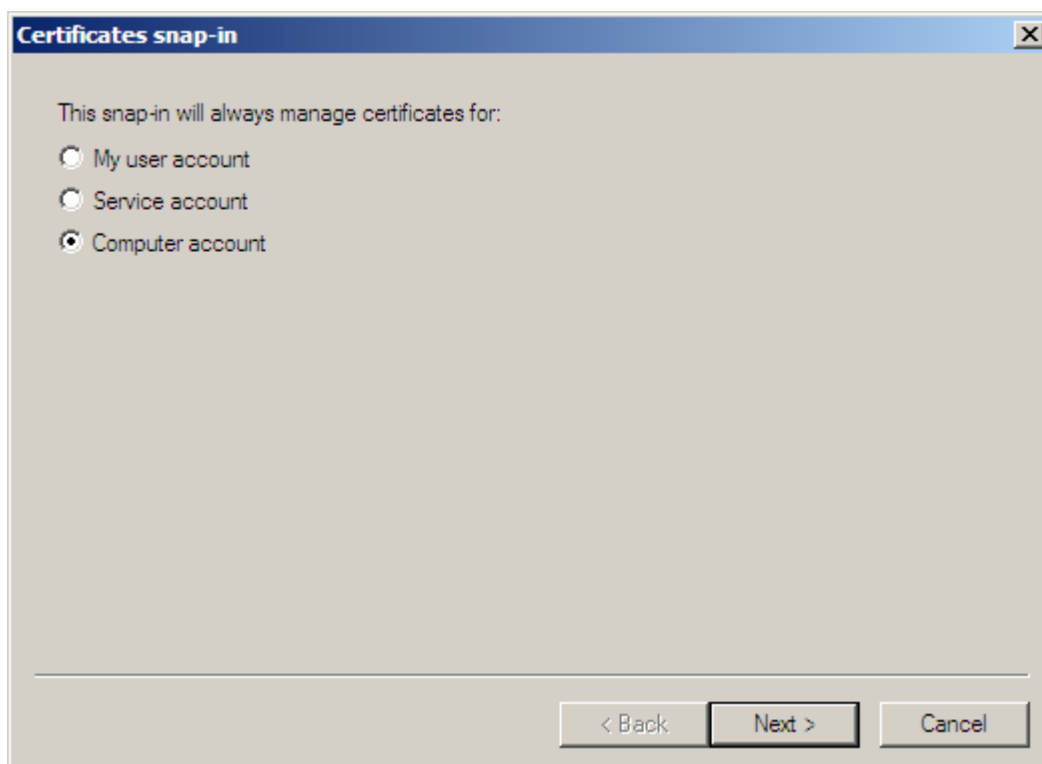
- Ignore  
 Accept  
 Require

Po ustawieniu tych właściwości konfiguracja serwera IIS zostanie ukończona.

## 5. Wykonywanie kopii zapasowej klucza prywatnego i certyfikatu

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.