

# Windows Serwer 2008 R2

Moduł x. Certyfikaty

# Instalacja roli „Usługi certyfikatów w usłudze AD”

Maszyna Widok Urządzenia Pomoc

Menedżer serwera

Plik Akcja Widok Pomoc

Menedżer serwera **Kreator dodawania ról**

**Wybieranie ról serwera**

Zanim rozpocznesz

**Role serwera**

- Usługi AD CS
  - Usługi ról
  - Typ instalacji
  - Typ urzędu certyfikacji
  - Klucz prywatny
    - Kryptografia
    - Nazwa urzędu certyfikacji
    - Okres ważności
  - Baza danych certyfikatów
- Potwierdzenie
- Postęp
- Wyniki

Wybierz jedną lub więcej ról do zainstalowania na tym serwerze.

Role:

- Active Directory Federation Services
- Hyper-V
- Serwer aplikacji
- Serwer DHCP (zainstalowano)
- Serwer DNS (zainstalowano)
- Serwer faksów
- Serwer sieci Web (IIS) (zainstalowano)
- Usługi certyfikatów w usłudze Active Directory**
- Usługi domenowe w usłudze Active Directory (zainstalowano)
- Usługi drukowania i zarządzania dokumentami
- Usługi LDS w usłudze Active Directory
- Usługi plików (zainstalowano)
- Usługi pulpitu zdalnego
- Usługi wdrażania systemu Windows
- Usługi zarządzania prawami dostępu w usłudze Active Directory
- Usługi zasad i dostępu sieciowego
- Windows Server Update Services

Opis:

[Usługi certyfikatów w usłudze Active Directory \(AD CS, Active Directory Certificate Services\)](#) służą do tworzenia urzędów certyfikacji i powiązanych usług ról, które pozwalają wystawiać certyfikaty używane w różnych aplikacjach i zarządzać nimi.


[Więcej informacji o rolach serwera](#)

< Wstecz Dalej > Zainstaluj Anuluj

Podczas używania kreatora odświeżanie jest wyłączone

# Instalacja roli „Usługi certyfikatów w usłudze AD”

Kreator dodawania ról



## Wprowadzenie do Usług certyfikatów w usłudze Active Directory

Zanim rozpoczniesz

Role serwera

**Usługi AD CS**

- Usługi ról
- Typ instalacji
- Typ urzędu certyfikacji
- Klucz prywatny
  - Kryptografia
  - Nazwa urzędu certyfikacji
  - Okres ważności
- Baza danych certyfikatów

Potwierdzenie


Postęp

Wyniki

### Usługi certyfikatów w usłudze Active Directory (AD CS)

Usługi certyfikatów w usłudze Active Directory (AD CS) udostępniają infrastrukturę certyfikatów umożliwiającą realizowanie scenariuszy z zastosowaniem zabezpieczonych sieci bezprzewodowych, wirtualnych sieci prywatnych, protokołu IPSec, ochrony dostępu do sieci (NAP), systemu szyfrowania plików (EFS) oraz logowania przy użyciu karty inteligentnej.

#### Do zapamiętania

 Nie można zmienić ustawień nazwy i domeny tego komputera po zainstalowaniu urzędu certyfikacji. Jeśli chcesz zmienić nazwę komputera, przyłączyć go do domeny lub podwyższyć poziom tego serwera do kontrolera domeny, wykonaj te zmiany przed zainstalowaniem urzędu certyfikacji. Aby uzyskać więcej informacji, zobacz artykuł o nadawaniu nazw urządzeniom certyfikacji.

#### Informacje dodatkowe

- [Omówienie Usług certyfikatów w usłudze Active Directory](#)
- [Zarządzanie urządzeniem certyfikacji](#)
- [Nadawanie nazw urządzeniom certyfikacji](#)

< Wstecz   **Dalej >**   Zainstaluj   Anuluj

# Instalacja roli „Usługi certyfikatów w usłudze AD”

**Kreator dodawania ról**

**Wybieranie usług ról**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

**Usługi ról**

Typ instalacji

Typ urzędu certyfikacji

Klucz prywatny

Kryptografia

Nazwa urzędu certyfikacji

Okres ważności

Baza danych certyfikatów

Serwer sieci Web (IIS)

Usługi ról

Potwierdzenie

Postęp

Wyniki

Wybierz usługi ról do zainstalowania dla roli Usługi certyfikatów w usłudze Active Directory:

Usługi ról:

- Urząd certyfikacji**
- Rejestracja w sieci Web dla urzędu certyfikacji
- Usługa sieci Web uzyskiwania informacji na temat rejestracji
- Usługa sieci Web uzyskiwania informacji na temat zasad rejestracji

Opis:


[Urząd certyfikacji \(CA, Certification Authority\)](#) służy do wystawiania certyfikatów i zarządzania nimi. Wiele połączonych urzędów certyfikacji może tworzyć infrastrukturę kluczy publicznych.

[Więcej informacji o usługach ról](#)

< Wstecz    Dalej >    Zainstaluj    Anuluj

# Instalacja roli „Usługi certyfikatów w usłudze AD”

Kreator dodawania ról

 **Określanie typu instalacji**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

Usługi ról

**Typ instalacji**

Typ urzędu certyfikacji

Klucz prywatny

Kryptografia

Nazwa urzędu certyfikacji

Okres ważności

Baza danych certyfikatów

Serwer sieci Web (IIS)

Usługi ról

Potwierdzenie

Postęp

Wyniki

Urzędy certyfikacji mogą korzystać z danych w usłudze Active Directory w celu uproszczenia wystawiania certyfikatów i zarządzania nimi. Określ, jaki urząd certyfikacji chcesz zainstalować: przedsiębiorstwa czy autonomiczny.

**Przedsiębiorstwo**  
Wybierz tę opcję, jeśli ten urząd certyfikacji należy do domeny i może używać usługi katalogowej w celu wystawiania certyfikatów i zarządzania nimi.

**Autonomiczny**  
Wybierz tę opcję, jeśli ten urząd certyfikacji nie używa danych usługi katalogowej w celu wystawiania certyfikatów i zarządzania nimi. Autonomiczny urząd certyfikacji może należeć do domeny.

[Więcej informacji o różnicach między konfiguracją w przedsiębiorstwie i konfiguracją autonomiczną](#)

< Wstecz   Dalej >   Zainstaluj   Anuluj

# Instalacja roli „Usługi certyfikatów w usłudze AD”

**Kreator dodawania ról**

**Określanie typu urzędu certyfikacji**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

Usługi ról

Typ instalacji

**Typ urzędu certyfikacji**

Klucz prywatny

Kryptografia

Nazwa urzędu certyfikacji

Okres ważności

Baza danych certyfikatów

Serwer sieci Web (IIS)

Usługi ról

Potwierdzenie

Postęp

Wyniki

Można skonfigurować kombinację głównego urzędu certyfikacji i urzędów podrzędnych, aby utworzyć hierarchiczną infrastrukturę kluczy publicznych (PKI). Główny urząd certyfikacji jest urzędem certyfikacji, który wystawia swój certyfikat z podpisem własnym. Podrzędny urząd certyfikacji otrzymuje swój certyfikat z innego urzędu certyfikacji. Określ, czy chcesz skonfigurować główny czy podrzędny urząd certyfikacji.

**Główny urząd certyfikacji**  
Wybierz tę opcję, jeśli instalujesz pierwszy lub jedyny urząd certyfikacji w infrastrukturze kluczy publicznych.

**Podrzędny urząd certyfikacji**  
Wybierz tę opcję, jeśli urząd certyfikacji ma uzyskiwać swój certyfikat z innego urzędu certyfikacji, który znajduje się wyżej w infrastrukturze kluczy publicznych.


[Więcej informacji o infrastrukturze kluczy publicznych \(PKI\)](#)

< Wstecz    **Dalej >**    Zainstaluj    Anuluj

- wybieramy **Główny Urząd Certyfikacji**

# Instalacja roli „Usługi certyfikatów w usłudze AD”

Kreator dodawania ról

 **Konfigurowanie klucza prywatnego**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

Usługi ról

Typ instalacji

Typ urzędu certyfikacji

**Klucz prywatny**

Kryptografia

Nazwa urzędu certyfikacji

Okres ważności

Baza danych certyfikatów

Serwer sieci Web (IIS)

Usługi ról

Potwierdzenie

Postęp

Wyniki

Aby generować i wystawiać certyfikaty dla klientów, urząd certyfikacji musi mieć klucz prywatny. Określ, czy chcesz utworzyć nowy klucz prywatny czy użyć istniejącego.

**Utwórz nowy klucz prywatny**  
Użyj tej opcji, jeśli nie masz klucza prywatnego lub chcesz utworzyć nowy klucz prywatny w celu zwiększenia zabezpieczeń. Zostanie wyświetlony monit o wybranie dostawcy usług kryptograficznych i określenie długości klucza prywatnego. Aby można było wystawiać certyfikaty, należy też wybrać algorytm wyznaczania wartości skrótu.

**Użyj istniejącego klucza prywatnego**  
Użyj tej opcji, aby po ponownym zainstalowaniu urzędu certyfikacji zachować ciągłość z uprzednio wystawionymi certyfikatami.

**Wybierz certyfikat i użyj skojarzonego z nim klucza prywatnego**  
Wybierz tę opcję, jeśli masz istniejący certyfikat na tym komputerze lub chcesz zaimportować certyfikat i używać skojarzonego z nim klucza prywatnego.

**Wybierz istniejący klucz prywatny na tym komputerze**  
Wybierz tę opcję, jeśli chcesz zachować klucze prywatne z poprzedniej instalacji lub chcesz użyć klucza prywatnego z alternatywnego źródła.


[Więcej informacji o kluczach publicznych i prywatnych](#)

< Wstecz   Dalej >   Zainstaluj   Anuluj

- Tworzymy nowy klucz prywatny

# Instalacja roli „Usługi certyfikatów w usłudze AD”

**Kreator dodawania ról**

 **Konfigurowanie kryptografii dla urzędu certyfikacji**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

Usługi ról

Typ instalacji

Typ urzędu certyfikacji

Klucz prywatny

**Kryptografia**

Nazwa urzędu certyfikacji

Okres ważności

Baza danych certyfikatów

Serwer sieci Web (IIS)

Usługi ról

Potwierdzenie

Postęp

Wyniki

Aby utworzyć nowy klucz prywatny, należy najpierw wybrać [dostawcę usługi kryptograficznej](#), [algorytm wyznaczania wartości skrótu](#) oraz długość klucza, zależnie od przeznaczenia wystawianego certyfikatu. Wybranie większej długości klucza poprawia zabezpieczenia, ale wydłuża czas operacji podpisywania.

Wybierz dostawcę usług kryptograficznych (CSP):  
RSA#Microsoft Software Key Storage Provider

Długość klucza (w znakach):  
2048

Wybierz algorytm wyznaczania wartości skrótu na potrzeby podpisywania certyfikatów wystawianych przez ten urząd certyfikacji:

SHA1  
MD5  
MD4  
MD2

Zezwalaj na działania administratora przy uzyskiwaniu dostępu do klucza prywatnego przez urząd certyfikacji

[Wiecej informacji o opcjach kryptograficznych urzędu certyfikacji](#)


< Wstecz   Dalej >   Zainstaluj   Anuluj

- wybieramy dostawcę **RSA#Microsoft Software Key**



# Instalacja roli „Usługi certyfikatów w usłudze AD”

Kreator dodawania ról

 **Konfigurowanie nazwy urzędu certyfikacji**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

Usługi ról

Typ instalacji

Typ urzędu certyfikacji

Klucz prywatny

Kryptografia

**Nazwa urzędu certyfikacji**

Okres ważności

Baza danych certyfikatów

Serwer sieci Web (IIS)

Usługi ról

Potwierdzenie

Postęp

Wyniki

Wpisz nazwę pospolitą identyfikującą ten urząd certyfikacji. Ta nazwa jest dodawana do wszystkich certyfikatów wystawianych przez ten urząd certyfikacji. Wartości sufiksu nazwy wyróżniającej są generowane automatycznie, ale można je modyfikować.

Nazwa pospolita tego urzędu certyfikacji:

Sufiks nazwy wyróżniającej:

Podgląd nazwy wyróżniającej:

[Więcej informacji o konfigurowaniu nazwy urzędu certyfikacji](#)

< Wstecz   Dalej >   Zainstaluj   Anuluj

- Nazwę urzędu ustawiamy na **server216-CA**

# Instalacja roli „Usługi certyfikatów w usłudze AD”

**Kreator dodawania ról**

**Ustawianie okresu ważności**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

Usługi ról

Typ instalacji

Typ urzędu certyfikacji

Klucz prywatny

Kryptografia

Nazwa urzędu certyfikacji

**Okres ważności**

Baza danych certyfikatów

Serwer sieci Web (IIS)

Usługi ról

Potwierdzenie

Postęp

Wyniki

Dla tego urzędu certyfikacji zostanie wystawiony certyfikat, aby zabezpieczyć komunikację z innymi urządzeniami certyfikacji oraz z klientami żądającymi certyfikatów. Okres ważności certyfikatu urzędu certyfikacji może być zależny od wielu czynników, takich jak przeznaczenie urzędu certyfikacji i jego zabezpieczenia.

Wybierz okres ważności certyfikatu generowanego dla tego urzędu certyfikacji:

10 Lata

Data wygaśnięcia urzędu certyfikacji: 2022-01-08 10:20

Pamiętaj, że urząd certyfikacji będzie wystawiać ważne certyfikaty tylko do swojej daty wygaśnięcia.

[Więcej informacji o ustawianiu okresu ważności certyfikatu](#)

< Wstecz    Dalej >    Zainstaluj    Anuluj

- Ustawiamy ważność certyfikatu na **10 lat**.

# Instalacja roli „Usługi certyfikatów w usłudze AD”

**Kreator dodawania ról**

**Konfigurowanie bazy danych certyfikatów**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

Usługi ról

Typ instalacji

Typ urzędu certyfikacji

Klucz prywatny

Kryptografia

Nazwa urzędu certyfikacji

Okres ważności

**Baza danych certyfikatów**

Serwer sieci Web (IIS)

Usługi ról

Potwierdzenie

Postęp

Wyniki

Baza danych certyfikatów rejestruje wszystkie żądania certyfikatów oraz wystawione, odwołane i wygasłe certyfikaty. Dziennik bazy danych umożliwia monitorowanie działań związanych z zarządzaniem urzędem certyfikacji.

Lokalizacja bazy danych certyfikatów:  
C:\Windows\system32\CertLog Przejrzyj...

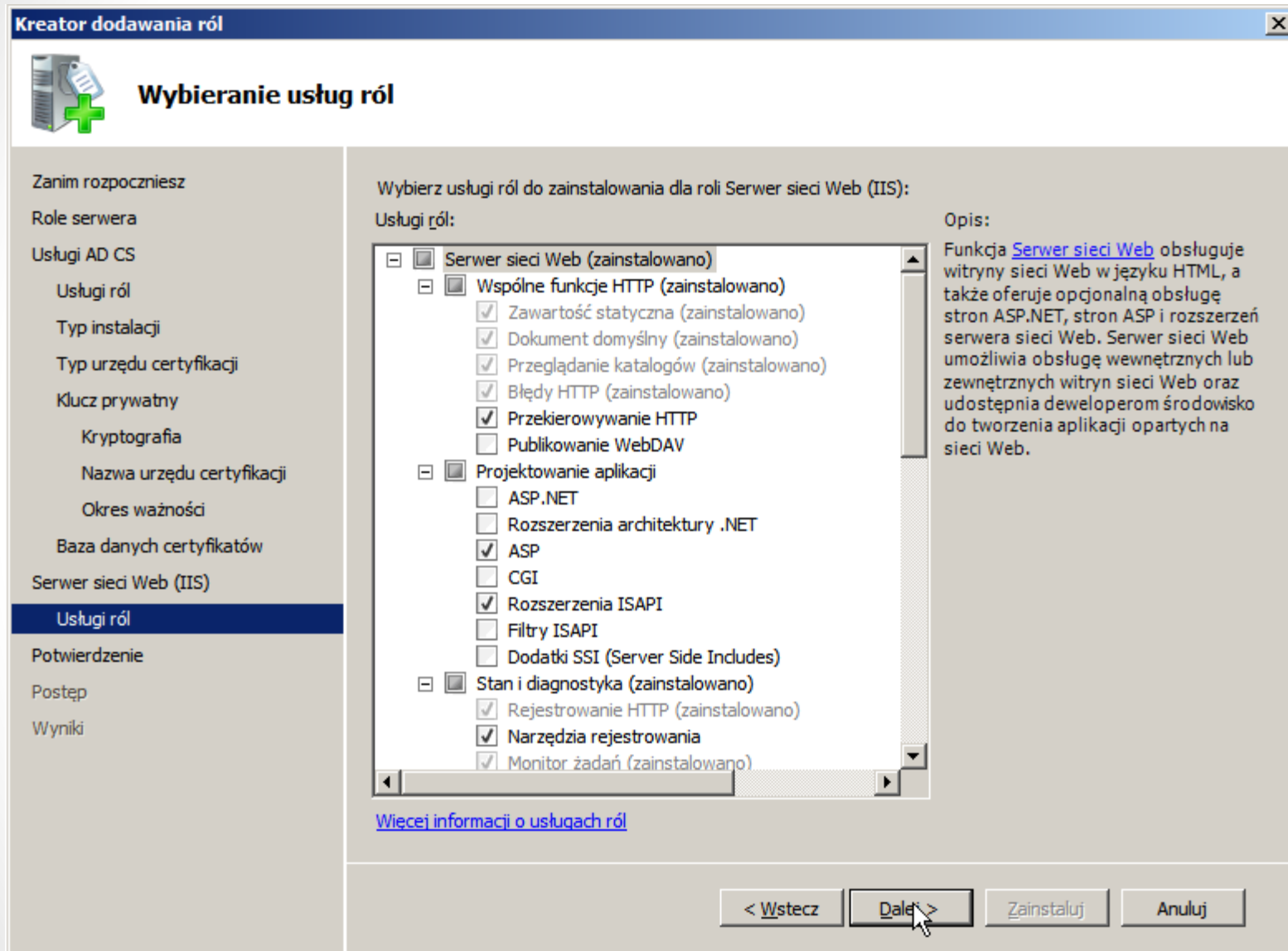
Użyj istniejącej bazy danych certyfikatów z poprzedniej instalacji w tej lokalizacji

Lokalizacja dziennika bazy danych certyfikatów:  
C:\Windows\system32\CertLog Przejrzyj...

< Wstecz Dalej > Zainstaluj Anuluj

- Ścieżki dostępu do bazy danych jednostki certyfikującej oraz logów.

# Instalacja roli „Usługi certyfikatów w usłudze AD”



- Komponenty serwera IIS instalowane wraz z IIS

# Instalacja roli „Usługi certyfikatów w usłudze AD”

**Kreator dodawania ról**

**Potwierdzenie opcji instalacji**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

Usługi ról

Typ instalacji

Typ urzędu certyfikacji

Klucz prywatny

Kryptografia

Nazwa urzędu certyfikacji

Okres ważności

Baza danych certyfikatów

Serwer sieci Web (IIS)

Usługi ról

**Potwierdzenie**

Postęp

Wyniki

Aby zainstalować następujące role, usługi ról lub funkcje, kliknij przycisk Zainstaluj.

⚠ Komunikaty ostrzegawcze: 1, informacyjne: 2

ℹ Po ukończeniu instalacji może być wymagane ponowne uruchomienie tego serwera.

⌵ **Usługi certyfikatów w usłudze Active Directory**

**Urząd certyfikacji**

⚠ Ustawienia nazwy i domeny tego komputera nie mogą zostać zmienione po zainstalowaniu urzędu certyfikacji.

Typ urzędu certyfikacji : Główny urząd certyfikacji przedsiębiorstwa

Dostawca usług kryptograficznych : RSA#Microsoft Software Key Storage Provider

Algorytm wyznaczania wartości skrótu : SHA 1

Długość klucza : 2048

Zezwalaj na interakcję z dostawcą usług kryptograficznych : Włączone

Okres ważności certyfikatu : 2022-01-08 10:20

Nazwa wyróżniająca : CN=server216-CA,DC=server216,DC=local

Lokalizacja bazy danych certyfikatów : C:\Windows\system32\CertLog

Lokalizacja dziennika bazy danych certyfikatów : C:\Windows\system32\CertLog


[Wydrukuj, zapisz lub wyślij pocztą e-mail te informacje](#)

< Wstecz Dalej > Zainstaluj Anuluj

- Okno podsumowujące kreatora instalacji roli AD CS

# Instalacja roli „Usługi certyfikatów w usłudze AD”

Kreator dodawania ról

 **Wyniki instalacji**

Zanim rozpoczniesz

Role serwera

Usługi AD CS

Usługi ról

Typ instalacji

Typ urzędu certyfikacji

Klucz prywatny

Kryptografia

Nazwa urzędu certyfikacji

Okres ważności

Baza danych certyfikatów

Serwer sieci Web (IIS)


Usługi ról



Potwierdzenie

Postęp



**Wyniki**

Następujące role, usługi ról lub funkcje zostały pomyślnie zainstalowane:

 1 komunikat ostrzegawczy

 **Usługi certyfikatów w usłudze Active Directory**  **Instalacja powiodła się**

Następujące usługi ról zostały zainstalowane:  
**Urząd certyfikacji**

 **Serwer sieci Web (IIS)**  **Instalacja powiodła się**

Następujące usługi ról zostały zainstalowane:  
**Serwer sieci Web**  
Wspólne funkcje HTTP  
Przekierowywanie HTTP  
Projektowanie aplikacji  
ASP  
Rozszerzenia ISAPI  
Stan i diagnostyka  
Narzędzia rejestrowania  
Śledzenie  
**Narzędzia do zarządzania**  
Zgodność z narzędziami zarządzania usługami IIS w wersji 6  
Zgodność z metabazą usług IIS 6

[Wydrukuj, zapisz lub wyślij pocztą e-mail raport o instalacji](#)

< Wstecz    Dalej >    Zamknij    Anuluj

Wygenerujemy na serwerze IIS certyfikat dla witryny ***szyfrowana.server216.local***, który umożliwi zestawianie pomiędzy naszą witryną ***szyfrowana***, a użytkownikami szyfrowanego połączenia protokołem SSL.

## ZARZĄDZANIE INFRASTRUKTURĄ KLUCZA PUBLICZNEGO (PKI)

# Zarządzanie urzędem certyfikacyjnym

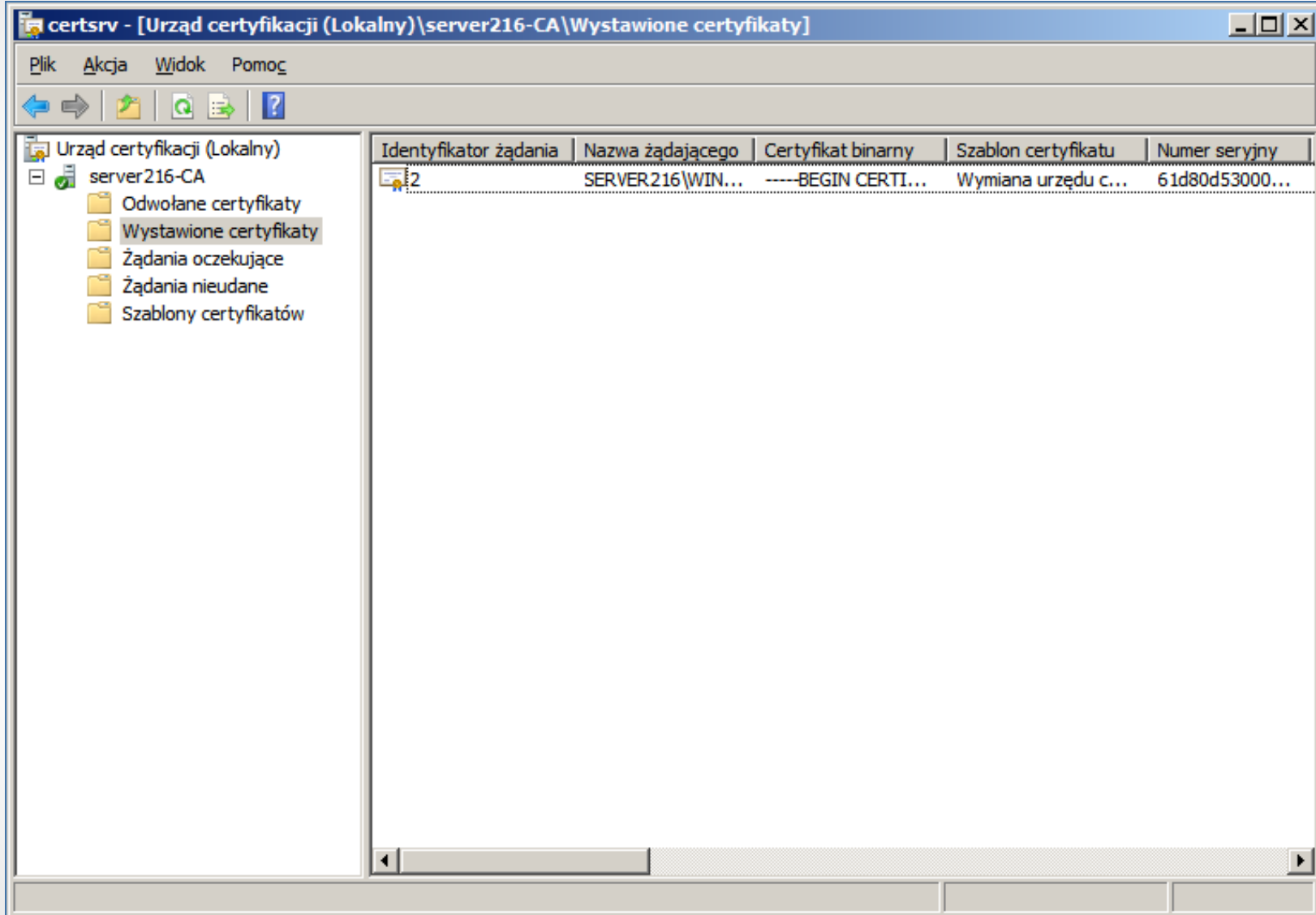
The screenshot shows the Windows Server 2008 R2 Start menu. The 'Narzędzia administracyjne' (Administrative Tools) folder is expanded, and the 'certification authority' service is selected. A tooltip is visible over the selected item, providing a description of the service.

**certification authority**  
Pozwala zarządzać usługami certyfikatów w usłudze Active Directory, które służą do wystawiania certyfikatów używanych przez programy szyfrujące w oparciu o technikę klucza publicznego.

- Uruchamiamy przystawkę **Certification Authority**

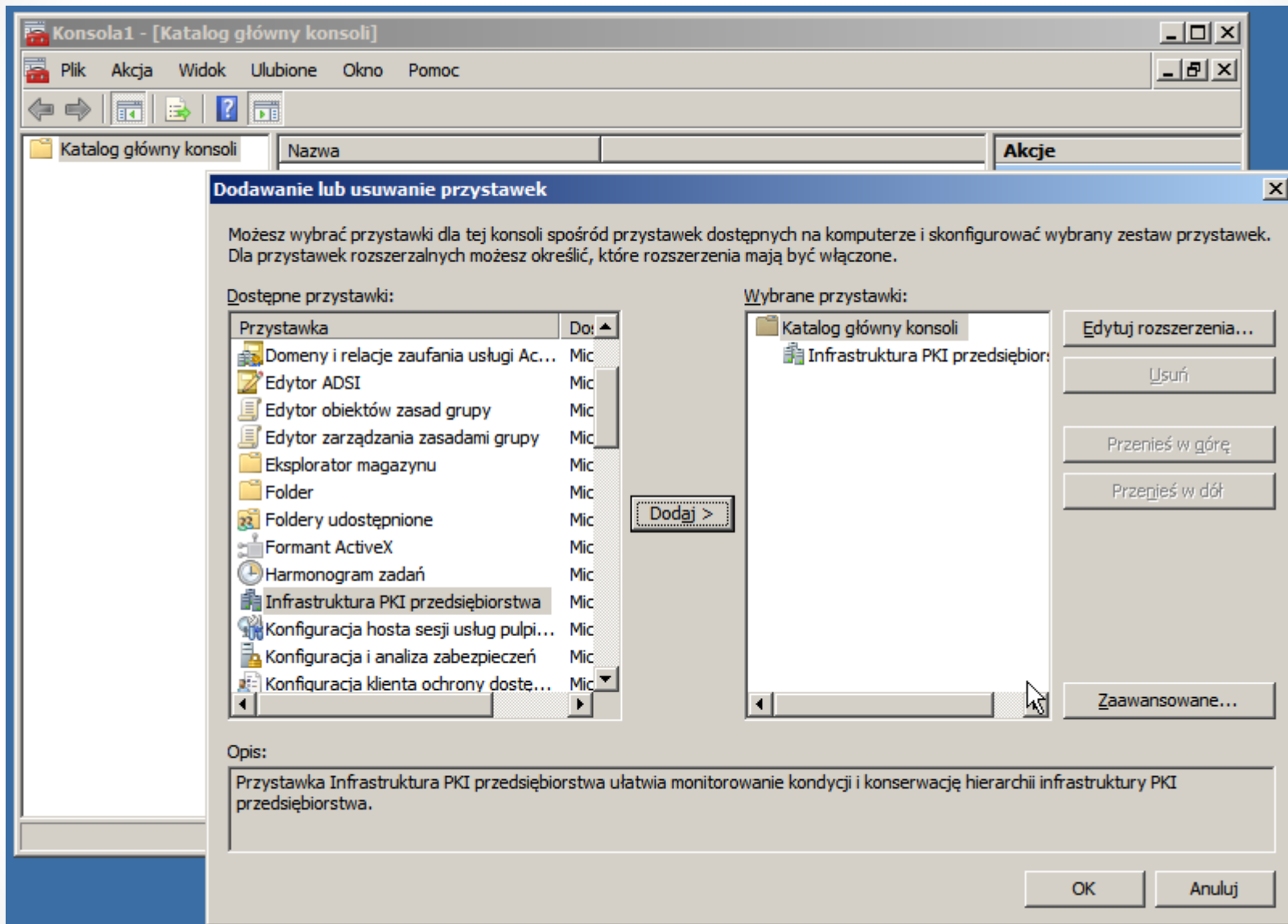


# Konsola do zarządzania jednostką certyfikującą



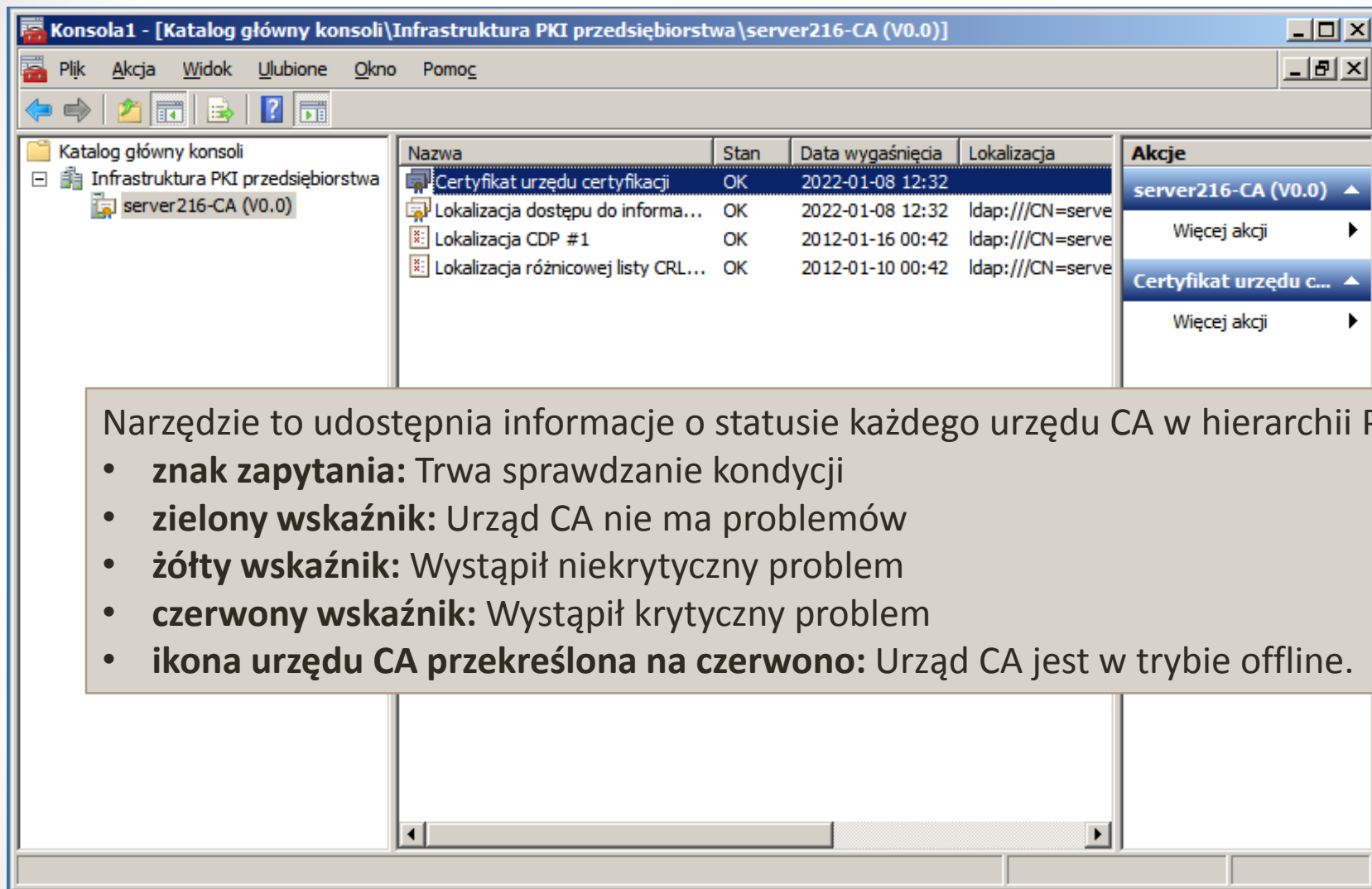
- Jednostka aktywowana - z zainstalowanym certyfikatem

# Przystawka Enterprise PKI



- Dodajemy „Infrastruktura PKI przedsiębiorstwa”

# Przystawka Enterprise PKI



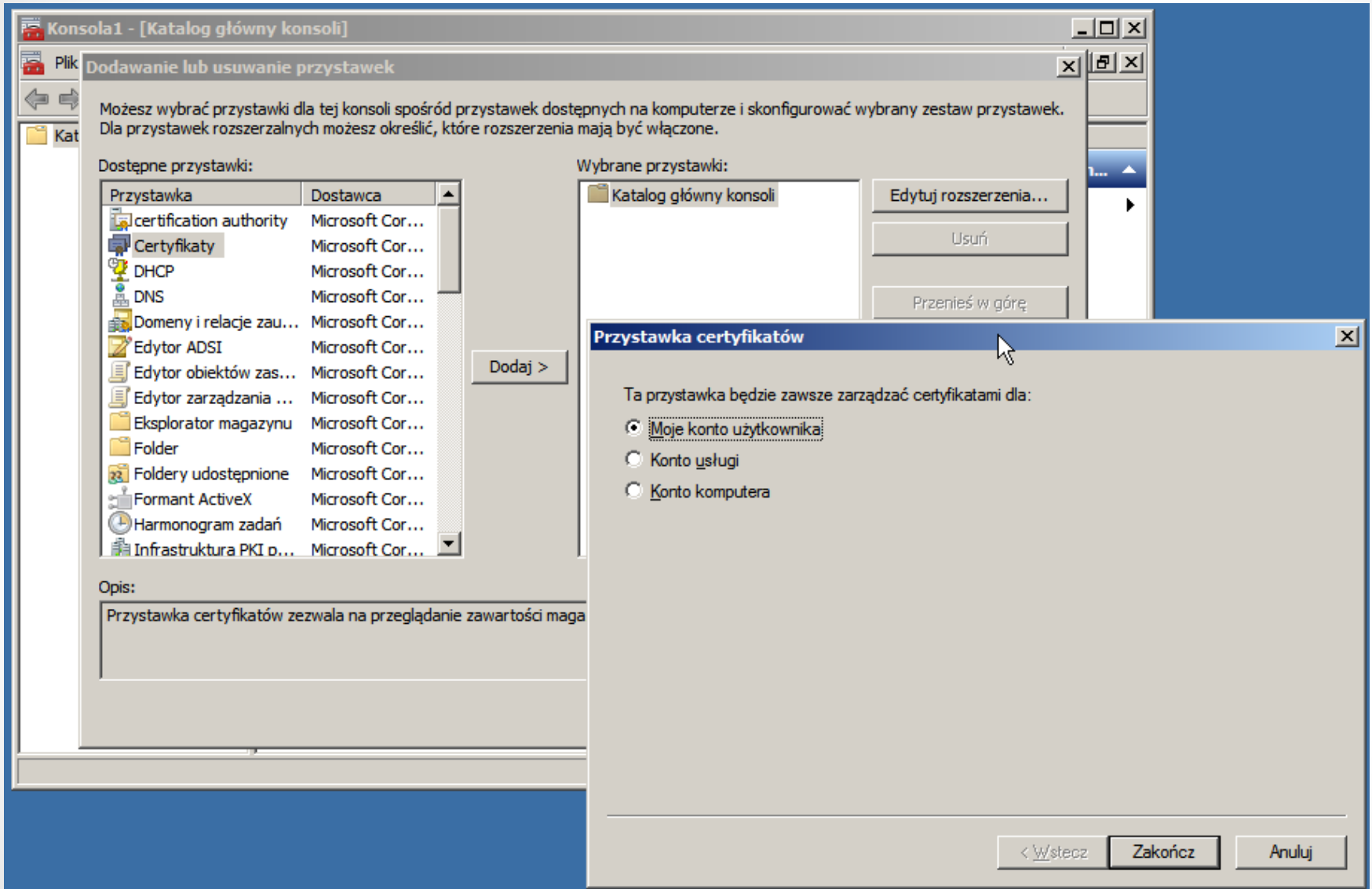
The screenshot shows the 'Konsola1' interface for the 'Infrastruktura PKI przedsiębiorstwa' (Enterprise PKI Infrastructure). The main window displays a table of certificates and their status. The table has columns for 'Nazwa' (Name), 'Stan' (Status), 'Data wygaśnięcia' (Expiration Date), and 'Lokalizacja' (Location). The first row, 'Certyfikat urzędu certyfikacji' (Certificate Authority Certificate), is highlighted in blue and has a status of 'OK'. The other rows are 'Lokalizacja dostępu do informa...', 'Lokalizacja CDP #1', and 'Lokalizacja różnicowej listy CRL...', all with 'OK' status. To the right of the table is an 'Akcje' (Actions) menu with options for 'server216-CA (V0.0)' and 'Certyfikat urzędu c...'. A text box is overlaid on the screenshot, providing information about the status indicators.

Narzędzie to udostępnia informacje o statusie każdego urzędu CA w hierarchii PKI:

- **znak zapytania:** Trwa sprawdzanie kondycji
- **zielony wskaźnik:** Urząd CA nie ma problemów
- **żółty wskaźnik:** Wystąpił niekrytyczny problem
- **czerwony wskaźnik:** Wystąpił krytyczny problem
- **ikona urzędu CA przekreślona na czerwono:** Urząd CA jest w trybie offline.

- Narzędzie **Infrastruktura PKI przedsiębiorstwa** pozwala na przeglądanie statusu wszystkich środowisk PKI w organizacji.

# Przystawka Certyfikaty



- W Uruchom wpisujemy **mmc**

# Przystawka Certyfikaty

The screenshot shows the Windows Certificate Manager console window titled "Konsola1 - [Katalog główny konsoli\Certyfikaty - bieżący użytkownik\Zaufane główne urzędy certyfikacji\Certyfikaty]". The left pane shows a tree view of the certificate store, with "Zaufane główne urzędy certyfikacji" expanded to show "Certyfikaty". The right pane displays a list of certificates issued to the current user, including "Class 3 Public Primary Certification...", "Copyright (c) 1997 Microsoft Corp.", "GTE CyberTrust Global Root", "Microsoft Authenticode(tm) Root...", "Microsoft Root Authority", "Microsoft Root Certificate Authority", "NO LIABILITY ACCEPTED, (c)97 V...", "server216-CA", "server216-CA", and "Thawte Timestamping CA".

The "Certyfikat" dialog box is open, showing the "Informacje o certyfikacie" tab. It contains the following information:

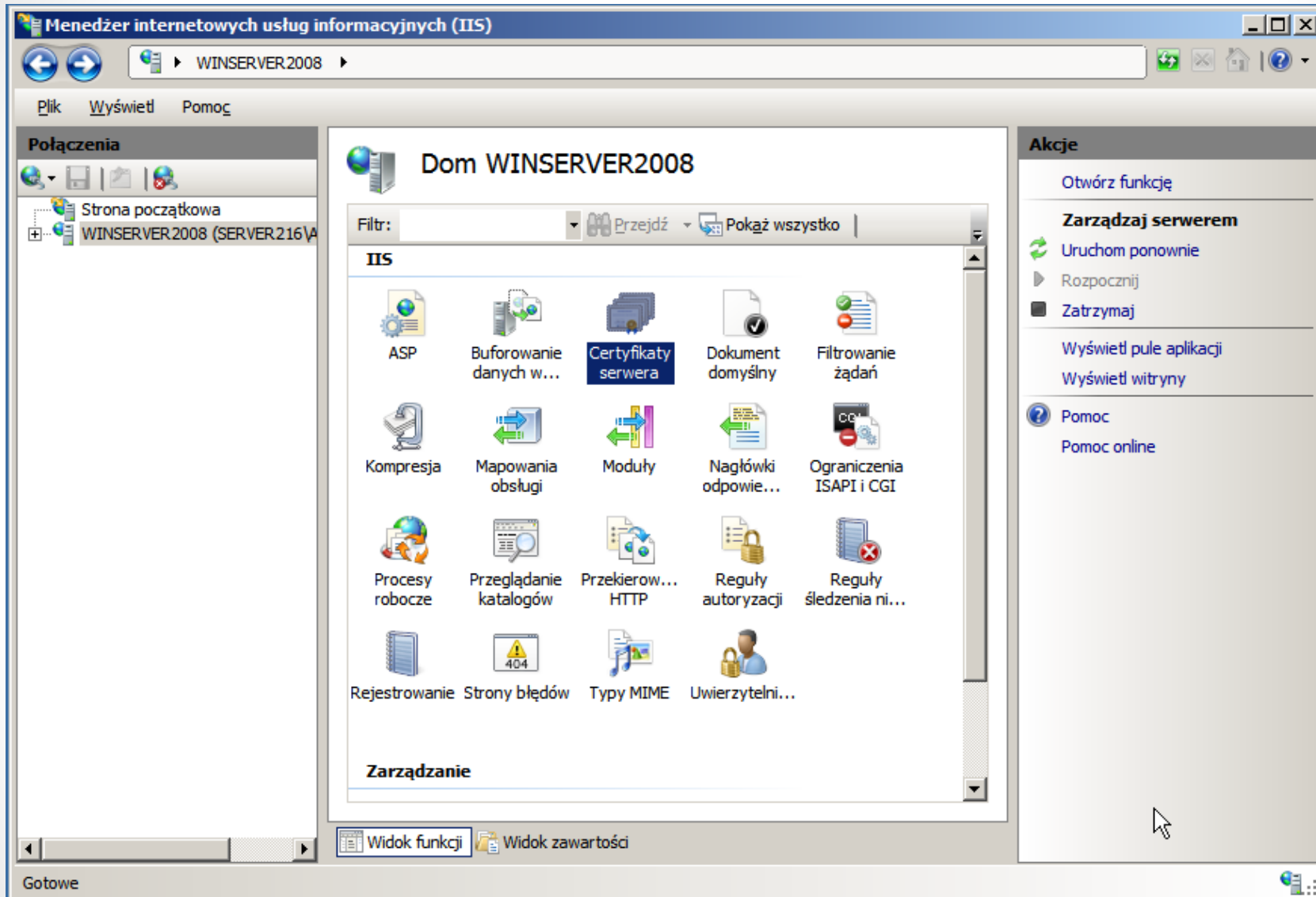
- Ten certyfikat jest przeznaczony do:**
  - Wszystkie zasady wydawania
  - Wszystkie zasady aplikacji
- Wystawiony dla:** server216-CA
- Wystawiony przez:** server216-CA
- Ważny od** 2012- 01- 08 **do** 2022- 01- 08

Buttons: "Oświadczenie wystawcy", "Dowiedz się więcej o [certyfikatach](#)", "OK".

Liczba certyfikatów w magazynie Zaufane główne urzędy certyfikacji jest równa 11.

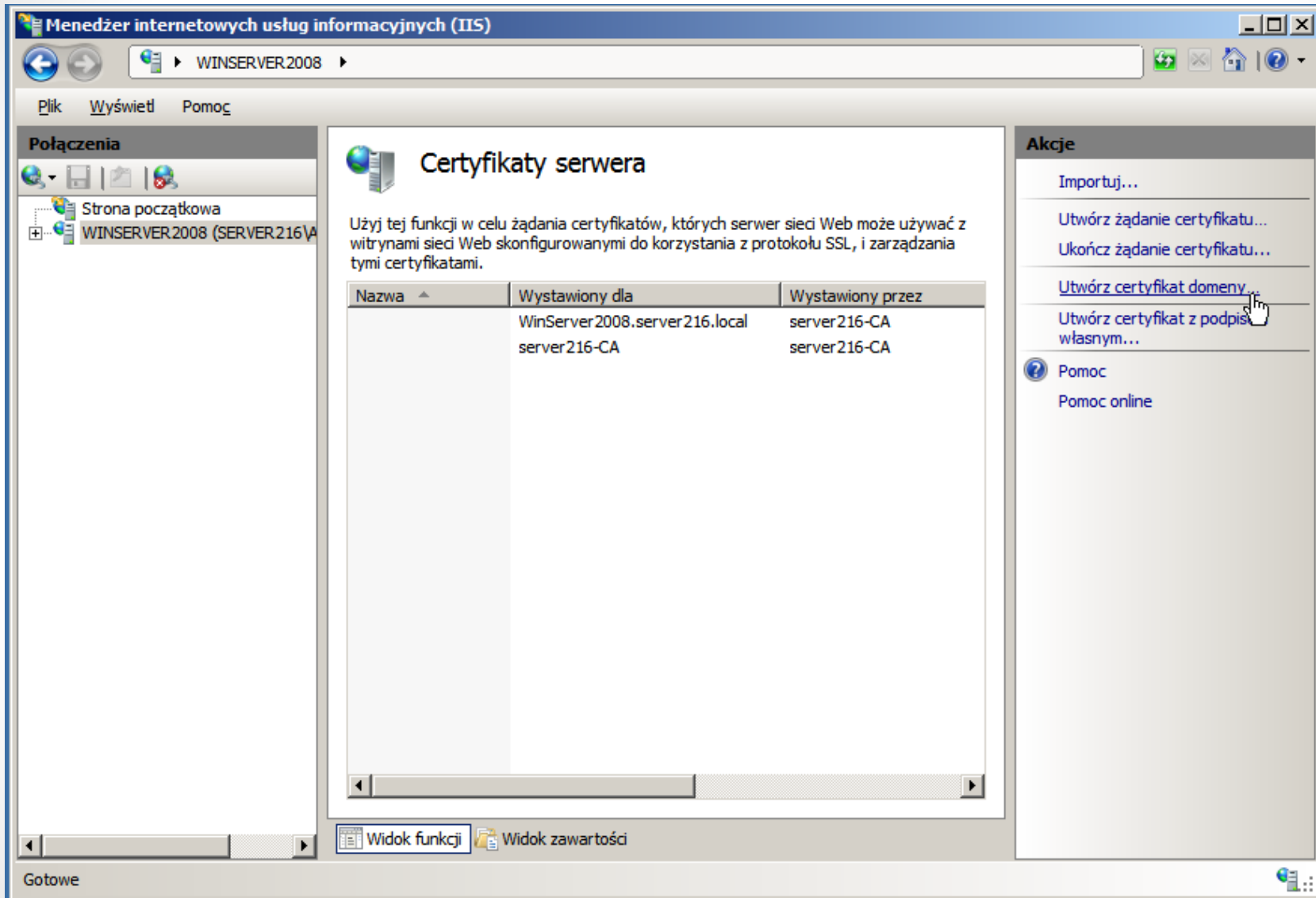
- Przeglądamy listę **Zaufanych głównych urzędów certyfikacji** dla użytkownika Administrator

# Tworzenie nowego certyfikatu



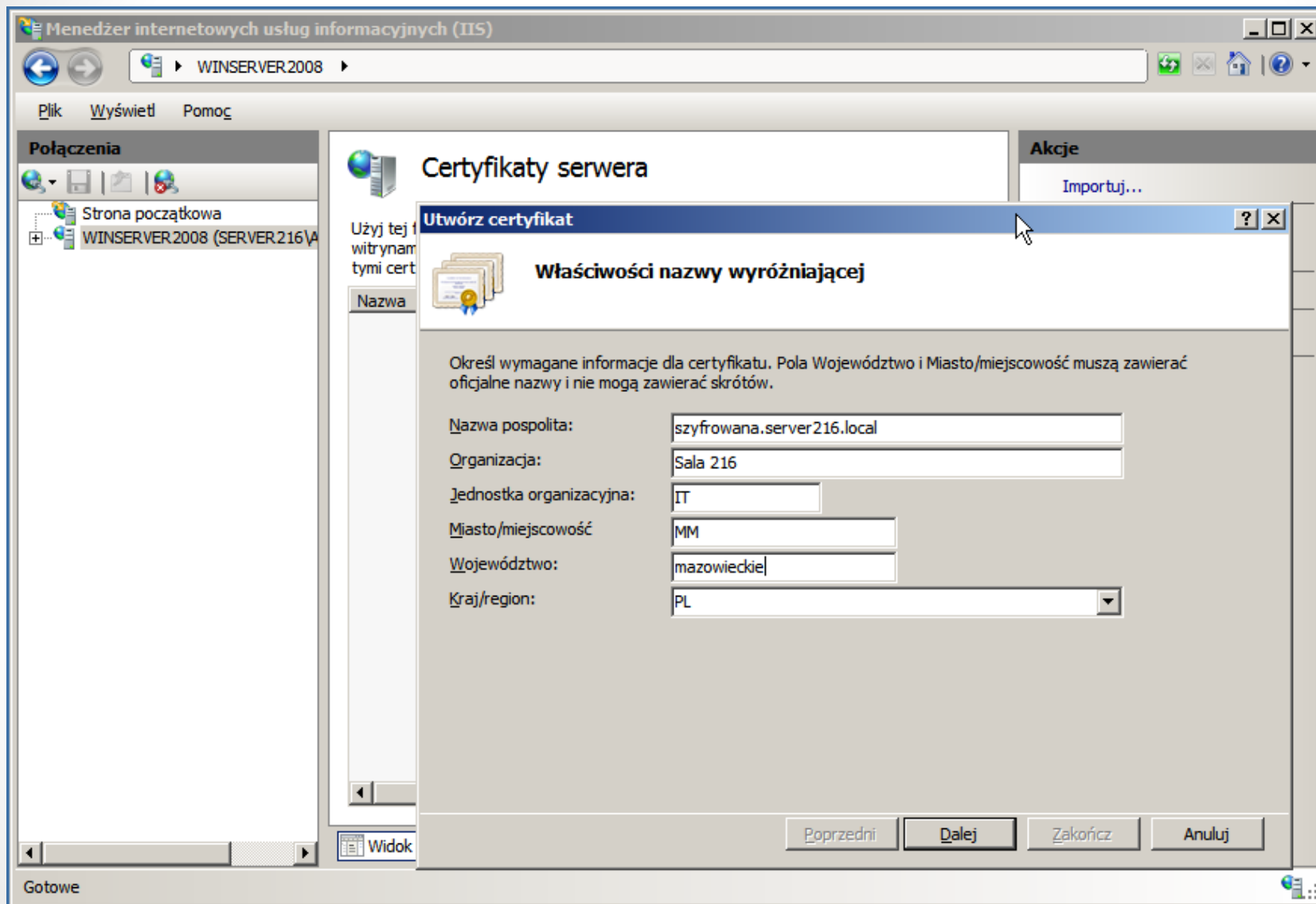
- Wybieramy: **Certyfikaty serwera**

# Tworzenie nowego certyfikatu



- Wybieramy: **Utwórz certyfikat domeny**

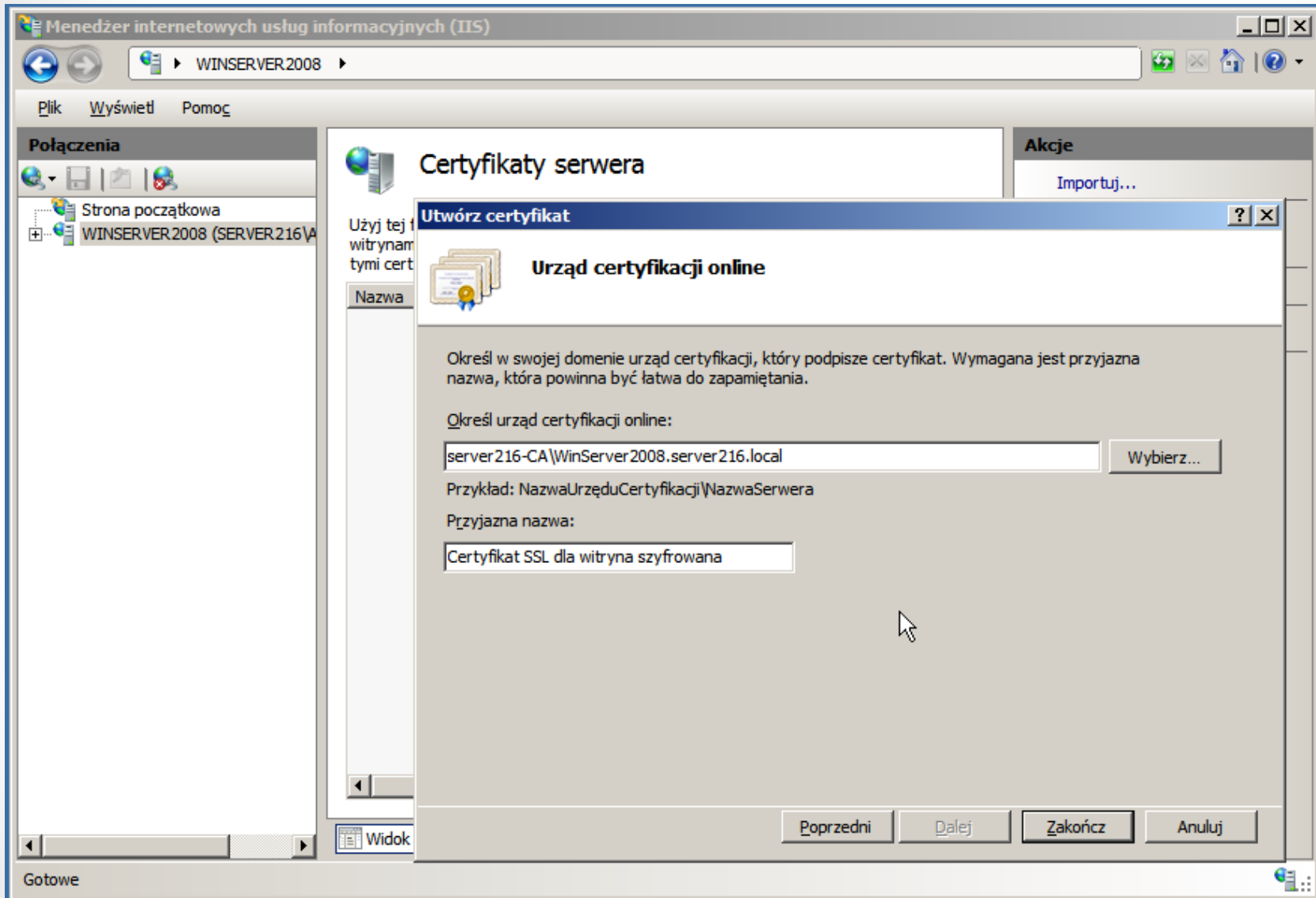
# Tworzenie nowego certyfikatu



- Wpisujemy dane

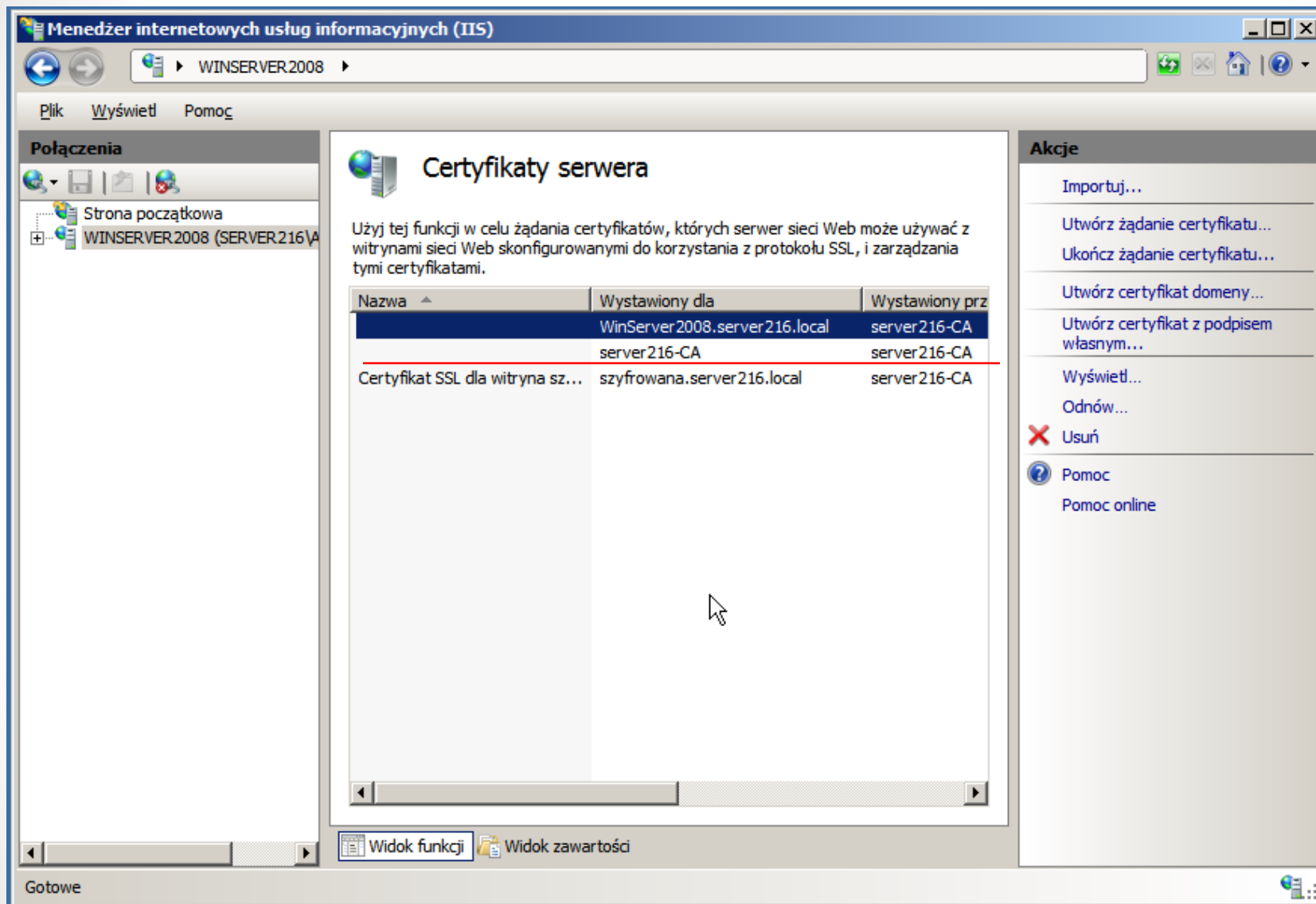


# Tworzenie nowego certyfikatu



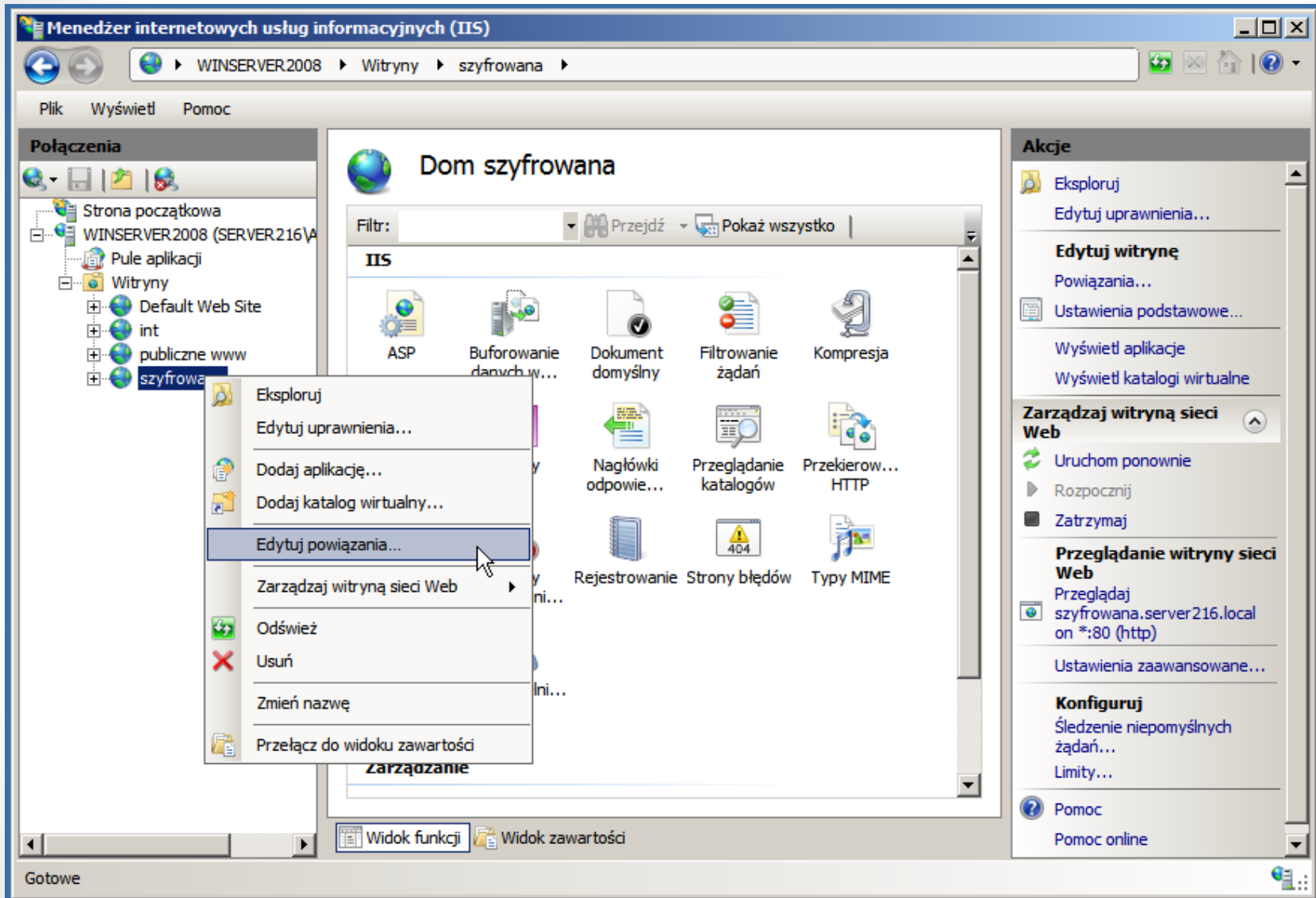
- Określamy urząd certyfikacji online

# Tworzenie nowego certyfikatu



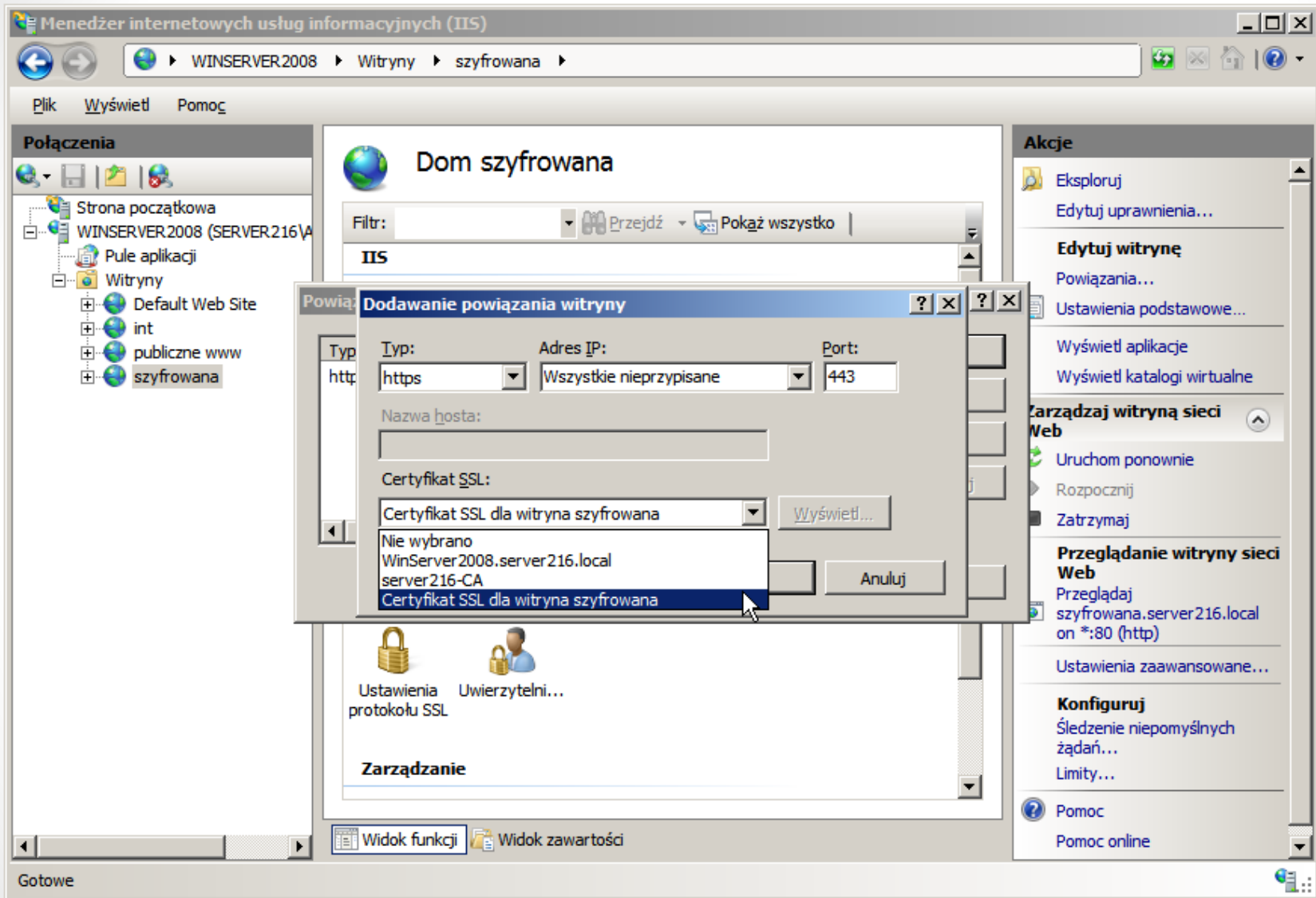
- Certyfikat został utworzony

# Konfigurujemy witrynę do korzystania z certyfikatu



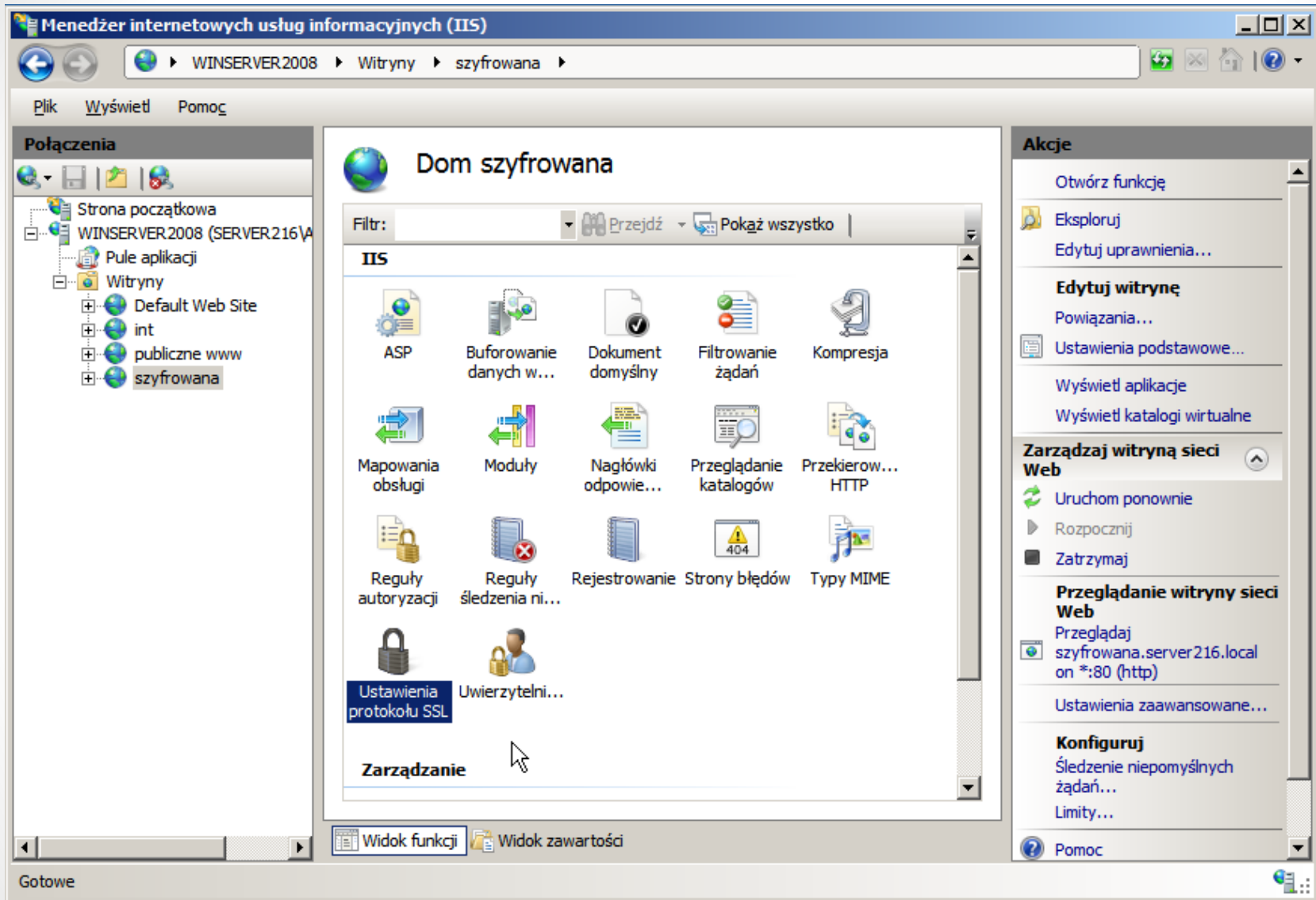
- Wybieramy naszą witrynę: **szyfrowana**

# Konfigurujemy witrynę do korzystania z certyfikatu



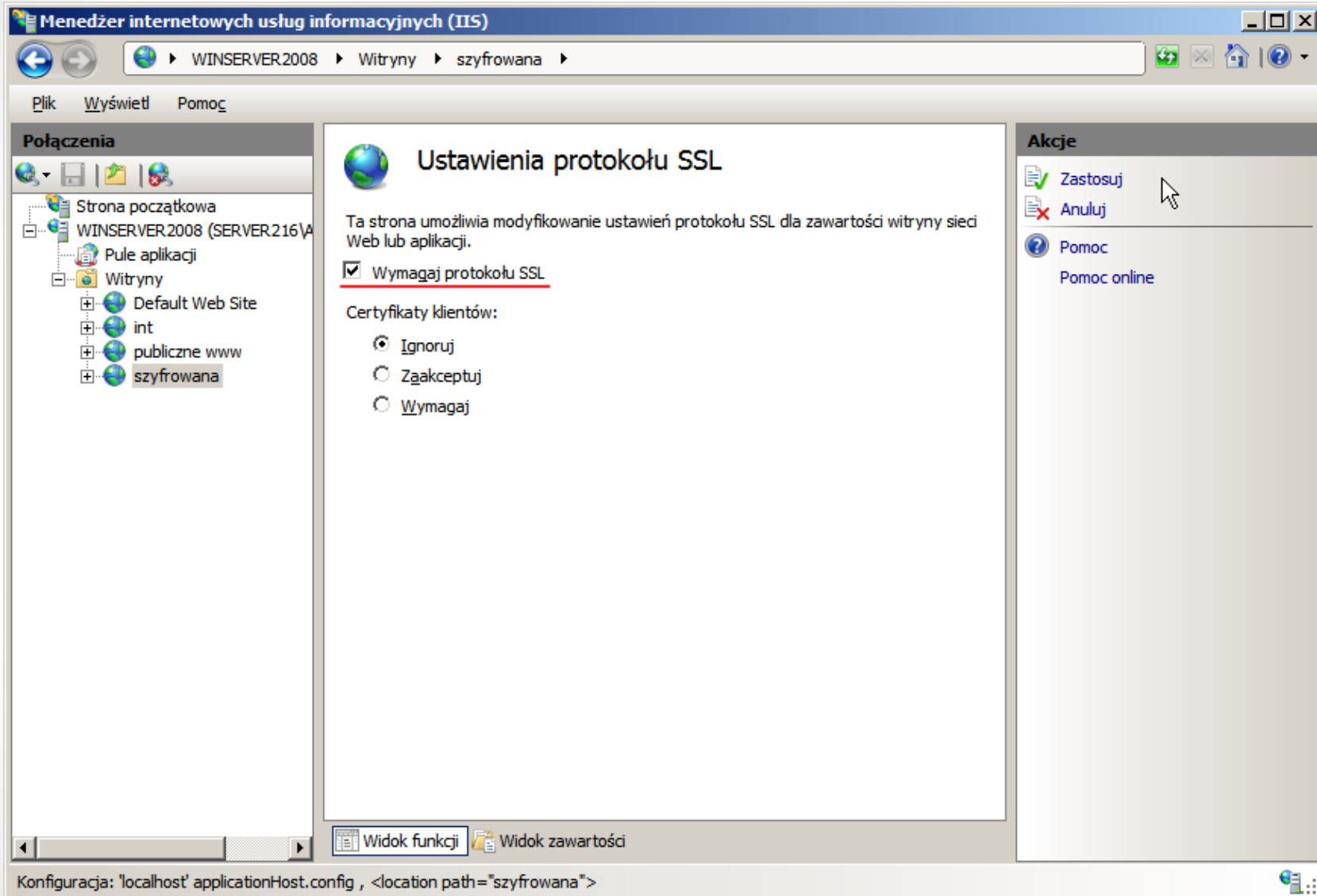
- Wybieramy utworzony przed chwilą certyfikat

# Konfigurujemy witrynę do korzystania z certyfikatu



- Konfigurujemy ustawienia protokołu SSL

# Konfigurujemy witrynę do korzystania z certyfikatu



- Konfigurujemy ustawienia protokołu SSL

# Testujemy

The screenshot shows a Windows Internet Explorer browser window. The title bar reads "Szczegółowe informacje o błędzie usług IIS 7.5 — 403.4 — Forbidden - Windows Internet Explorer". The address bar contains "http://szyfrowana.server216.local/". The main content area has a blue header with the text "Błąd serwera w aplikacji „SZYFROWANA”" and "Internet Information Services 7.5". Below this, a box titled "Podsumowanie błędu" contains the message: "Błąd HTTP 403.4 — Forbidden" and "Strona, do której próbujesz uzyskać dostęp, jest chroniona za pomocą protokołu SSL (Secure Sockets Layer)". A second box titled "Szczegółowe informacje o błędzie" provides technical details:

Moduł <b>IIS Web Core</b>	Żądany adres <b>http://szyfrowana.server216.local:80/</b>
Powiadomienie <b>BeginRequest</b>	URL
Obsługa <b>StaticFile</b>	Ścieżka <b>C:\inetpub\szyfrowana</b>
Kod błędu <b>0x80070005</b>	fizyczna
	Metoda <b>Jeszcze nie ustalono</b>
	logowania
	Użytkownik <b>Jeszcze nie ustalono</b>
	logowania

The status bar at the bottom shows "Gotowe", "Internet | Tryb chroniony: wyłączony", and "100%".

- Wpisaliśmy adres naszej strony bez **https**

# Testujemy

The screenshot shows a Windows Internet Explorer browser window with the address bar set to `https://szyfrowana.server216.local/`. The main content area displays a blue error banner with the text "Błąd serwera w aplikacji „SZYFROWANA”" and "Internet Information Services 7.5". Below this, a "Podsumowanie błędu" (Error Summary) section contains the text: "Błąd HTTP 403.4 – Forbidden" and "Strona, do której próbuje: protokołu SSL (Secure Sockets Layer)". A "Szczegółowe informacje o błędzie" (Detailed Error Information) section lists: "Moduł IIS Web Core", "Powiadomienie BeginRequest", "Obsługa StaticFile", and "Kod błędu 0x80070005".

Overlaid on the error page is a "Zabezpieczenia systemu Windows" (Windows Security) dialog box. It contains the message: "Serwer szyfrowana.server216.local w lokalizacji szyfrowana.server216.local wymaga nazwy użytkownika i hasła." Below the message are two input fields: the first contains the username "tygrysek" and the second contains a masked password ".....". There is a checkbox labeled "Zapamiętaj moje poświadczenia" (Remember my credentials) which is currently unchecked. At the bottom of the dialog are "OK" and "Anuluj" (Cancel) buttons.

At the bottom of the browser window, the status bar shows "Trwa ocena" (Evaluation in progress) on the left and "Internet | Tryb chroniony: wyłączony" (Internet | Protected Mode: off) on the right, along with a zoom level of 100%.

- Podajemy login i hasło



# Testujemy



- Działa;)

# linki

- <http://www.wss.pl/baza-wiedzy/korporacyjna-infrastruktura-kluca-publicznego---budowa-i-zarzadzanie-czesc-1,1909>