

UNIZETO



POWSZECHNE
CENTRUM CERTYFIKACJI



instrukcja użytkownika

Microsoft Internet Explorer 6.0 PL

Wykorzystanie certyfikatów niekwalifikowanych
w oprogramowaniu Microsoft Internet Explorer 6.0 PL

wersja 1.0

Spis treści

1. WSTĘP	3
2. WYKORZYSTANIE CERTYFIKATÓW SERWERÓW WWW.....	3
3. WYKORZYSTANIE CERTYFIKATÓW UŻYTKOWNIKÓW DO UWIERZYTELNIANIA.....	17
3.1. INSTALACJA WŁASNEGO CERTYFIKATU Z PLIKU *.PFX	18
3.2. UWIERZYTELNIANIE UŻYTKOWNIKA	24
3.3. WYKONYWANIE KOPII BEZPIECZEŃSTWA WŁASNEGO CERTYFIKATU	26
4. USUWANIE CERTYFIKATÓW	32

1. Wstęp

Microsoft Internet Explorer to przeglądarka internetowa dostarczana wraz z systemem operacyjnym Microsoft Windows. Przeglądarka jest bardzo mocno zintegrowana z systemem operacyjnym i wykorzystuje szereg mechanizmów systemowych. Dotyczy to również mechanizmu obsługi certyfikatów. Dlatego należy wiedzieć, że wiele funkcji przeglądarki opisanych w niniejszej instrukcji wynika po prostu z cech systemu operacyjnego, a nie Internet Explorera. Ponieważ funkcje te są jednak integralną częścią przeglądarki i bez nich jej działanie nie byłoby możliwe, zostały opisane jako funkcje Microsoft Internet Explorera.

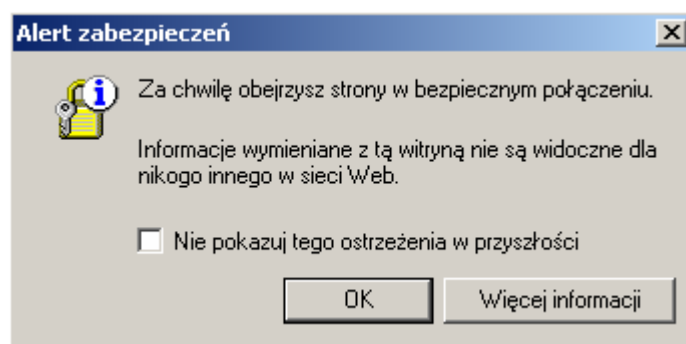
2. Wykorzystanie certyfikatów serwerów WWW

Powszechne wykorzystanie Internetu oraz stron WWW do wymiany danych osobowych, danych kart kredytowych (płatności on-line) oraz przeprowadzania transakcji naraża dane na szereg zagrożeń. Zagrożenia te polegają przede wszystkim na próbach przechwycenia (podsluchania) przesyłanych danych oraz ich kradzieży poprzez podstawienie fałszywych stron WWW.

Zabezpieczenie danych wymienianych za pośrednictwem stron WWW możliwe jest dzięki wykorzystaniu certyfikatów przez serwery WWW. Strona internetowa przedstawiająca się certyfikatem gwarantuje internaucie:

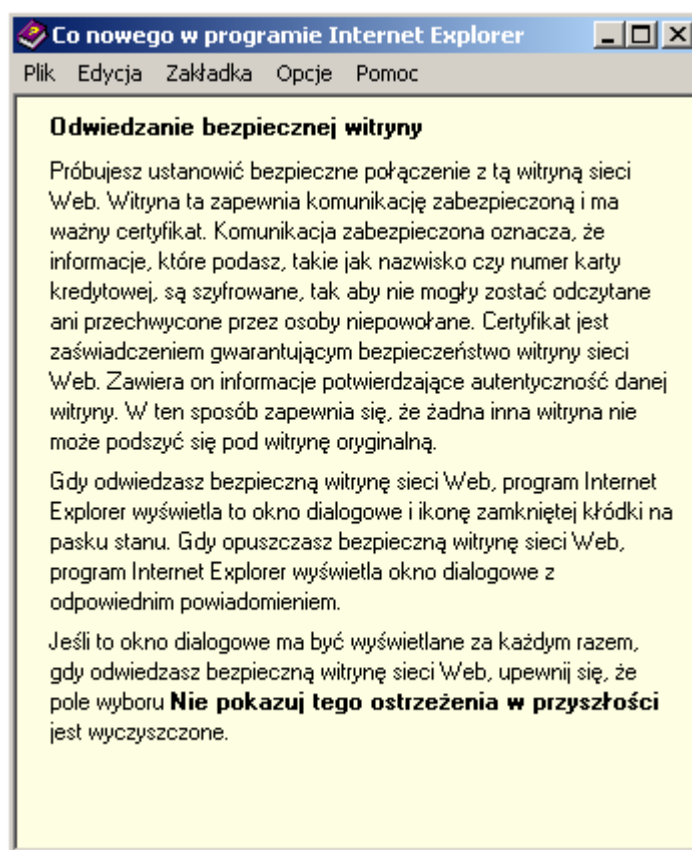
1. pewność, że strona, z którą się połączył, jest autentyczna, wiarygodna i nie została przez kogoś podstawiona. Ponieważ w certyfikacie, którym przedstawia się strona WWW, jest zapisany jej adres, a wiarygodność właściciela strony potwierdził wystawca certyfikatu, możemy być pewni jej autentyczności. Każda próba przedstawienia strony WWW o innym adresie niż zapisany w certyfikacie spowoduje wywołanie stosownego komunikatu ostrzegającego użytkownika o tym fakcie.
2. szyfrowane połączenie pomiędzy jego przeglądarką internetową a serwerem WWW (stroną WWW). Szyfrowanie możliwe jest przy wykorzystaniu protokołu **SSL (Secure Sockets Layer)**. Dzięki temu wszelkie dane przekazywane przez przeglądarkę i stronę WWW są bezpieczne nawet wtedy, gdy zostaną przechwycone w czasie transmisji. Ma to szczególne znaczenie w przypadku wypełniania na stronach WWW formularzy z danymi osobowymi lub danymi kart kredytowych podczas robienia zakupów w Internecie.

Przeglądarka Microsoft Internet Explorer nawiązując połączenie szyfrowane z serwerem WWW wyświetli poniższy komunikat (przy założeniu, że użytkownik korzysta z domyślnych ustawień zabezpieczeń w w/w przeglądarce):



Ustawienia zabezpieczeń można wyświetlić wybierając z menu pozycję **Narzędzia**, a następnie **Opcje internetowe**. W nowo otwartym oknie „Opcje internetowe” należy wybrać zakładkę **Zaawansowane**, w której przewijamy listę, aż ukaże się kategoria **Zabezpieczenia**.

Bezpieczne połączenie zostanie nawiązane, jeżeli użytkownik kliknie w powyższym oknie przycisk **OK**. Jeżeli wybrany zostanie przycisk **Więcej informacji**, ukaże się okno informujące o cechach bezpiecznego połączenia ze stroną WWW, które może zostać nawiązane.

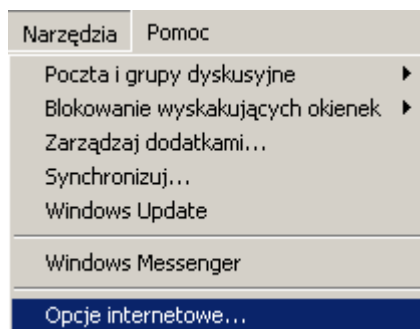


Powyższe okno zamykamy klikając znak **X**, znajdujący się w prawym górnym rogu okna, bądź wybierając z menu pozycję **Plik**, a potem **Zakończ**.

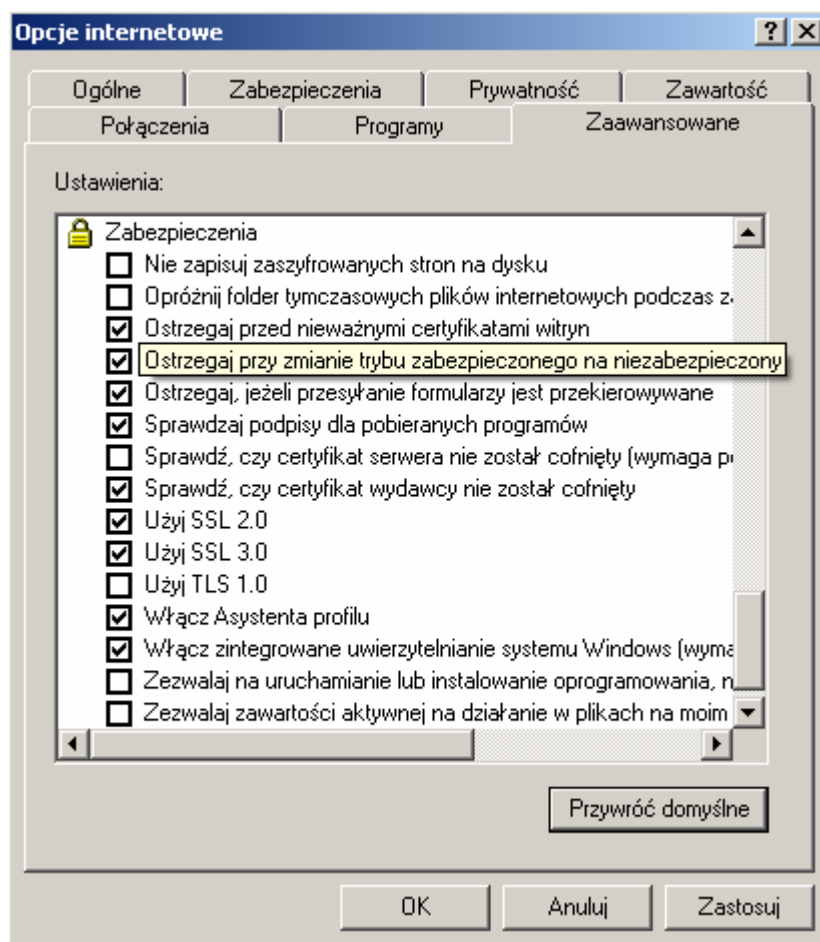
Jeżeli zaznaczymy opcję **Nie pokazuj tego ostrzeżenia w przyszłości**, komunikat o bezpiecznym połączeniu nie będzie więcej wyświetlany.

UWAGA! Zaznaczenie opcji **Nie pokazuj tego ostrzeżenia w przyszłości** w chwili nawiązywania bezpiecznego połączenia spowoduje również wyłączenie komunikatu o zakończeniu bezpiecznego połączenia z serwerem.

Jeżeli wybrano opcję **Nie pokazuj tego ostrzeżenia w przyszłości**, aby przywrócić poprzednie ustawienia, należy w menu przeglądarki Microsoft Internet Explorer wybrać pozycję **Narzędzia**, a potem **Opcje internetowe**.

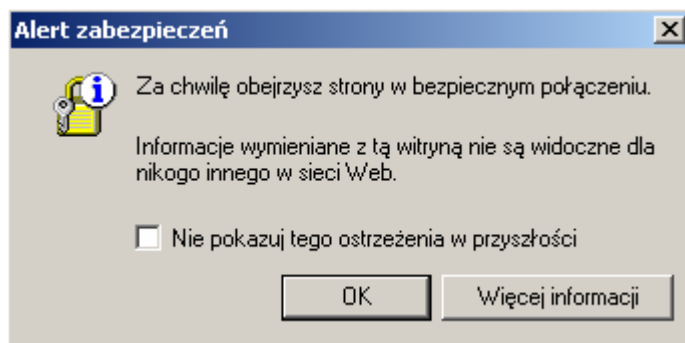


W nowo otwartym oknie „Opcje internetowe” wybieramy zakładkę **Zaawansowane**, w której zaznaczamy opcję **Ostrzegaj przy zmianie trybu zabezpieczonego na niezabezpieczony**.




Aby program zapamiętał wprowadzone zmiany, klikamy przycisk **OK**.

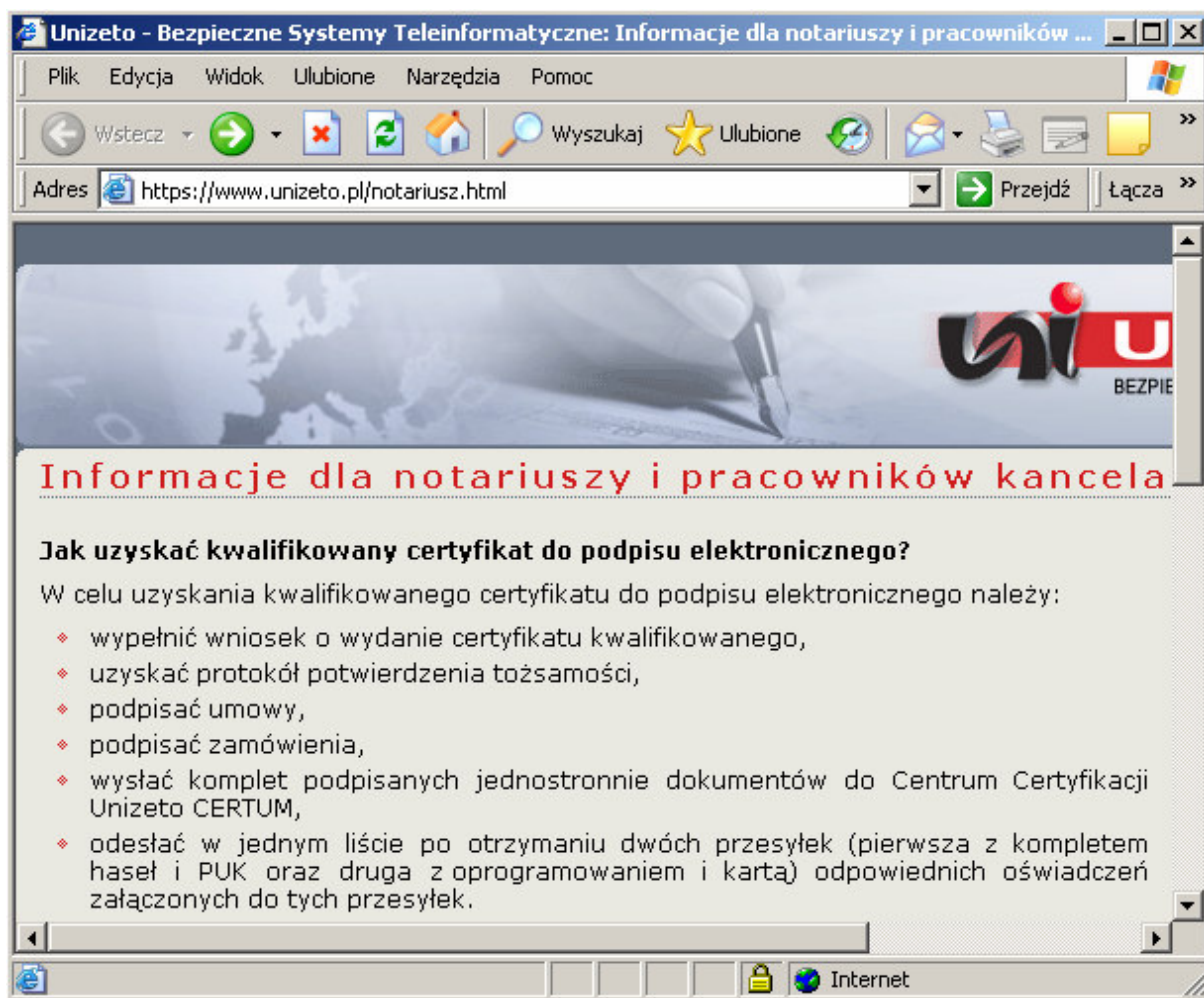
Jeżeli w oknie informującym o próbie nawiązania bezpiecznego połączenia klikniemy **OK**, nastąpi zamknięcie tego okna.



Następnie przeglądarka Internet Explorer nawiąże bezpieczne (szyfrowane) połączenie z serwerem WWW.

Nawiązanie połączenia szyfrowanego sygnalizuje użytkownikowi ikona kłódki  widoczna w prawej części paska stanu okna przeglądarki.

Drugą oznaką nawiązania szyfrowanego połączenia pomiędzy przeglądarką a serwerem WWW jest zmiana adresu widocznego w pasku adresu. Standardowy wpis **http** rozpoczynający każdy adres strony zmieni się na **https** (od skrótu **H**yper**T**ext **T**ransfer **P**rotocol **S**ecure).



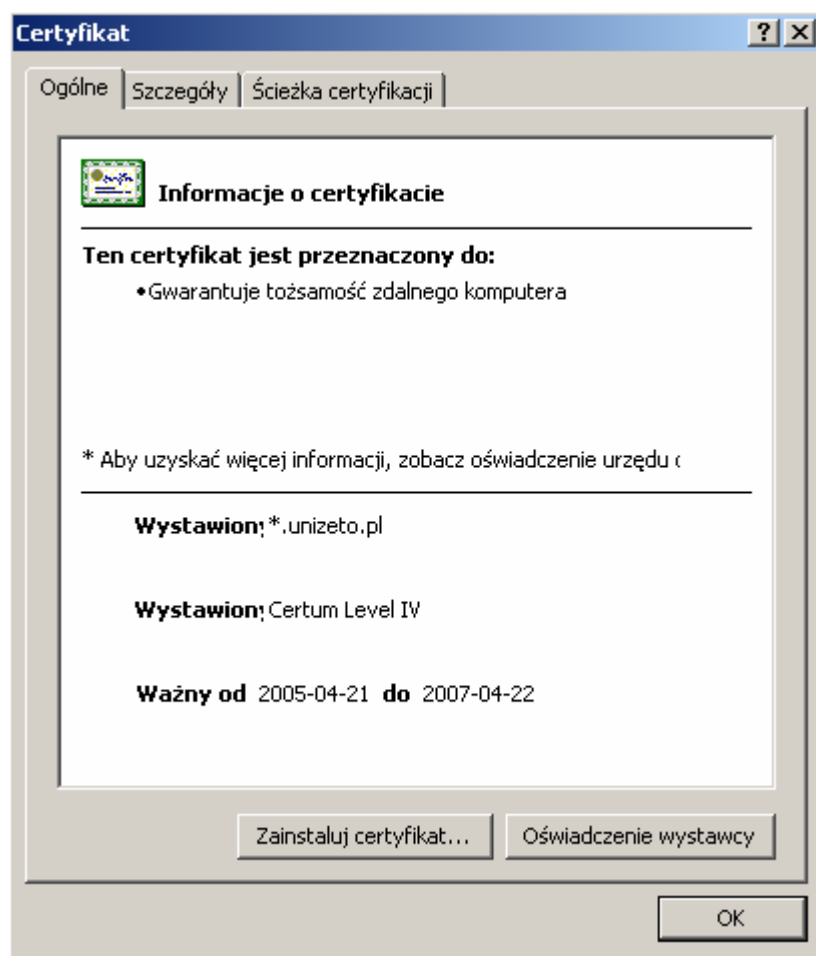
W przeciwieństwie do połączenia ze stronami WWW, których adres rozpoczyna się od **https**, połączenie ze stroną o adresie rozpoczynającym się od **http** (od skrótu **H**yper**T**ext **T**ransfer **P**rotocol) nie jest szyfrowane.

W chwili przesunięcia kursora myszy na ikonę kłódki widocznej w pasku stanu okna przeglądarki ukaże się komunikat o użyciu protokołu **SSL** (ang. **S**ecure **S**ockets **L**ayer), który zapewnia poufność i integralność przesyłanych danych oraz umożliwia przeprowadzanie uwierzytelnienia dzięki wykorzystaniu certyfikatów.



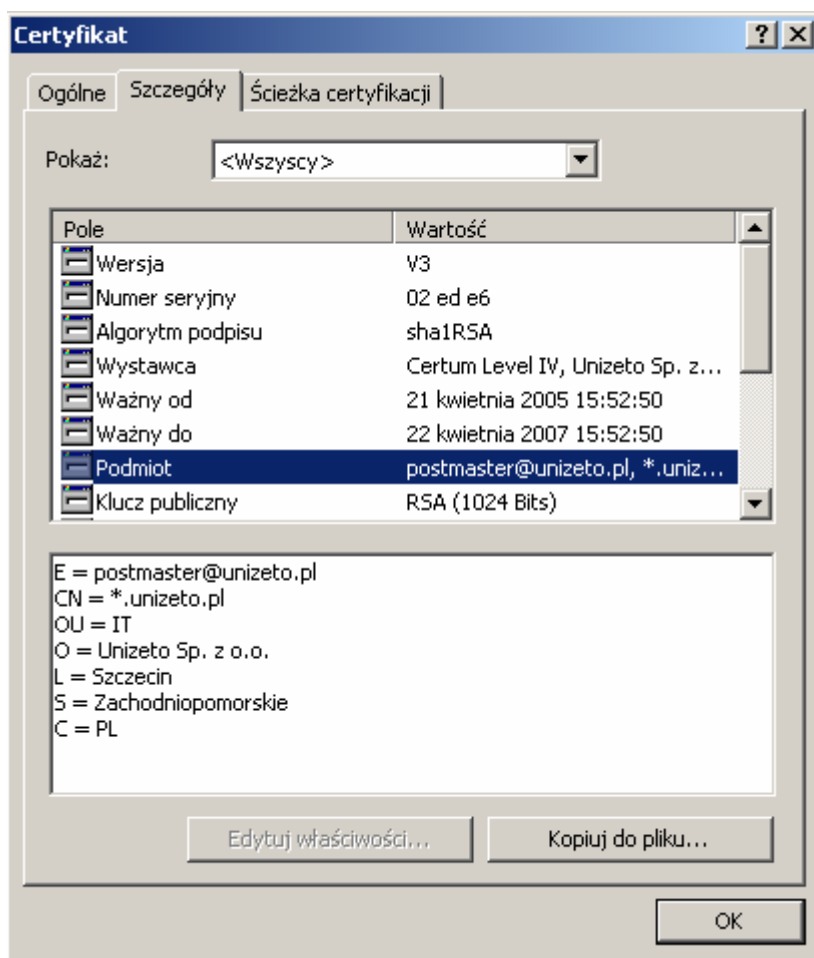
Jeżeli użytkownik kliknie dwukrotnie ikonę kłódki , ukaże się okno „Certyfikat” z informacjami o certyfikacie, który zabezpiecza przeglądany stronę WWW.

W zakładce **Ogólne** wyświetlone zostaną informacje dotyczące przeznaczenia certyfikatu, nazwy domeny, dla której został wystawiony, nazwy wystawcy certyfikatu oraz jego okresu ważności.



W oknie „Certyfikat” można zapoznać się z bardziej szczegółowymi informacjami dotyczącymi certyfikatu. W tym celu należy wybrać zakładkę **Szczegóły**.

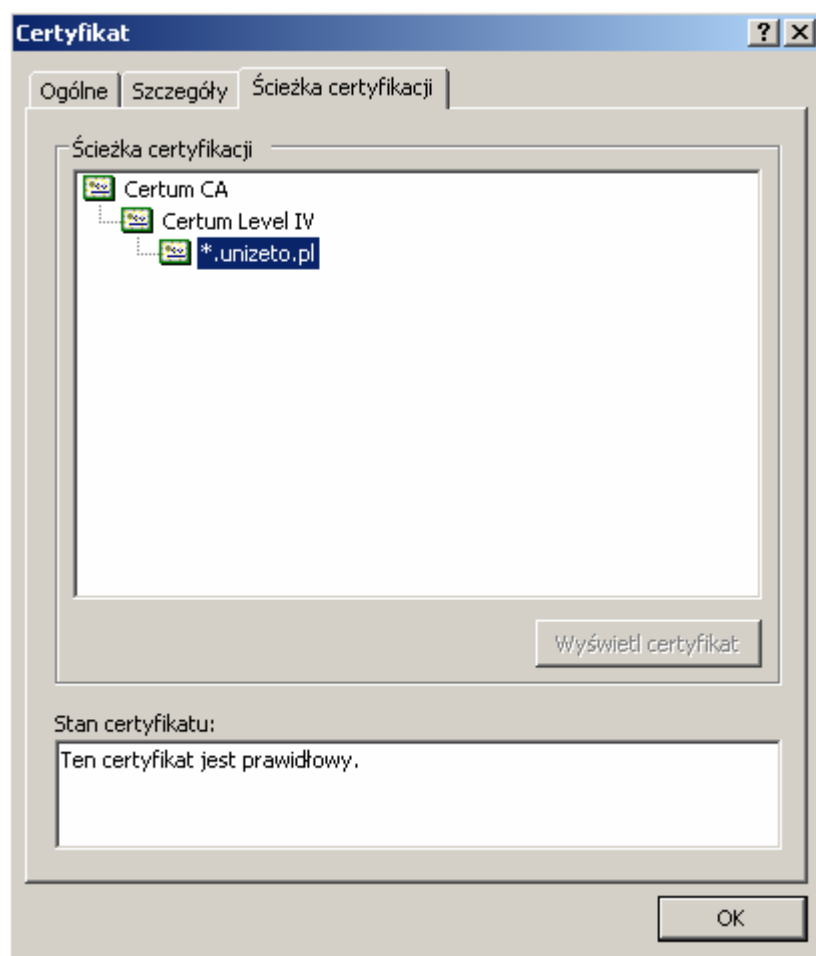
Zaznaczenie na liście wybranej pozycji spowoduje wyświetlenie szczegółowych informacji na jej temat w dolnej części okna.



W zakładce **Ścieżka certyfikacji** użytkownik może zapoznać się ze ścieżką certyfikacji certyfikatu serwera WWW.

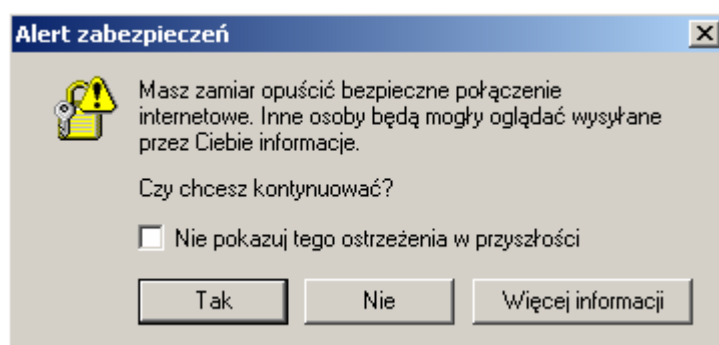
Ścieżka certyfikacji jest to drzewiasta struktura obrazująca hierarchiczne powiązanie między certyfikatem zabezpieczającym daną stronę WWW a certyfikatami centrum certyfikacji. Na najwyższym poziomie w ścieżce certyfikacji zawsze znajduje się certyfikat centrum certyfikacji (w tym przypadku Certum CA), tzw. root. Na najniższym poziomie umieszczony jest certyfikat zabezpieczający przeglądaną stronę (np. *.unizeto.pl). Pomiedzy certyfikatem serwera WWW, a certyfikatem centrum certyfikacji może znajdować się szereg innych certyfikatów pośrednich urzędów certyfikacji. Na rysunku poniżej przedstawiono sytuację, gdy w ścieżce certyfikacji znajduje się tylko jeden taki certyfikat (Certum Level IV).

Każdy certyfikat w ścieżce powinien posiadać wpis **Ten certyfikat jest prawidłowy** w polu **Stan certyfikatu**. Jeżeli jest inaczej, oznacza to, że centrum certyfikacji, które wystawiło certyfikat dla oglądanej właśnie strony WWW, nie jest zaufane, a strona może być niebezpieczna lub podstawiona.



Żeby zamknąć okno, należy wybrać przycisk **OK**.

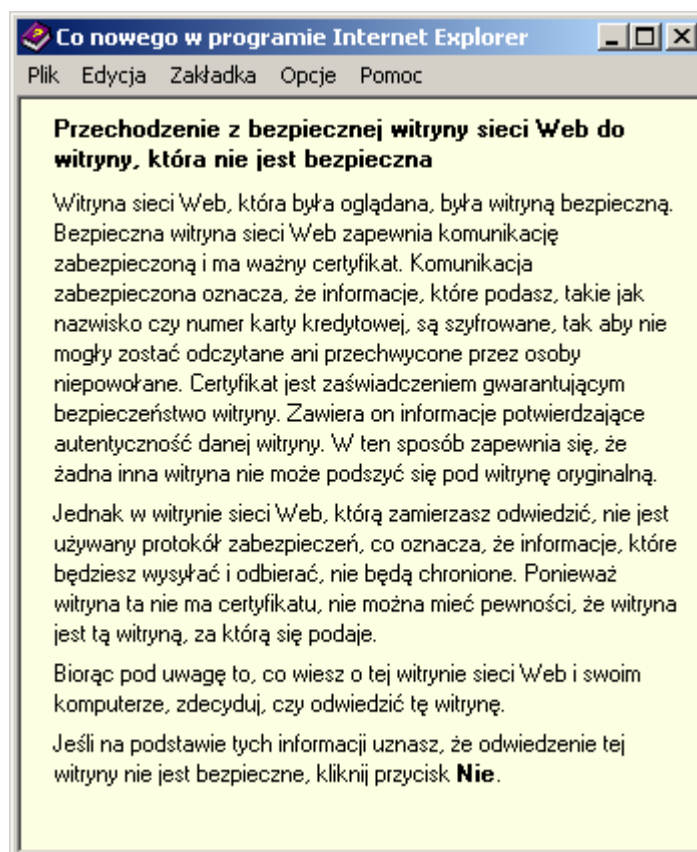
W przypadku przejścia ze strony WWW zabezpieczonej certyfikatem i wymuszającej szyfrowane połączenie na stronę, która certyfikatu nie posiada, ukaże się poniższy komunikat:



UWAGA! Zaznaczenie opcji **Nie pokazuj tego ostrzeżenia w przyszłości** w chwili zamykania bezpiecznego połączenia spowoduje również wyłączenie komunikatu o nawiązywaniu bezpiecznego połączenia.

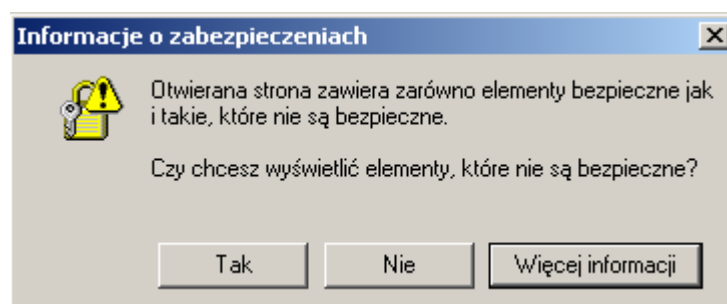
Aby kontynuować przeglądanie stron, należy wybrać przycisk **Tak**. Trzeba jednak wziąć pod uwagę, że bezpieczne połączenie zostanie zakończone i dalsza wymiana danych będzie przebiegać w niezasyfrowanym połączeniu.

Jeżeli zostanie wybrany przycisk **Nie**, Internet Explorer zablokuje zmianę strony na niezabezpieczoną certyfikatem. Jeżeli wybrany zostanie przycisk **Więcej informacji**, ukaże się poniższe okno:




Okno zamykamy klikając znak **✕** znajdujący się w prawym górnym rogu okna bądź wybierając z górnego menu **Plik**, a potem **Zakończ**.

Jeżeli zabezpieczona certyfikatem strona WWW zawiera elementy, których lokalizacji nie można bezpośrednio powiązać z adresem serwera (lub nazwą domeny umieszczoną w certyfikacie), bądź też zawiera elementy pobierane z innego serwera (np. banery reklamowe), przeglądarka nawiązując połączenie z taką stroną wyświetli komunikat:

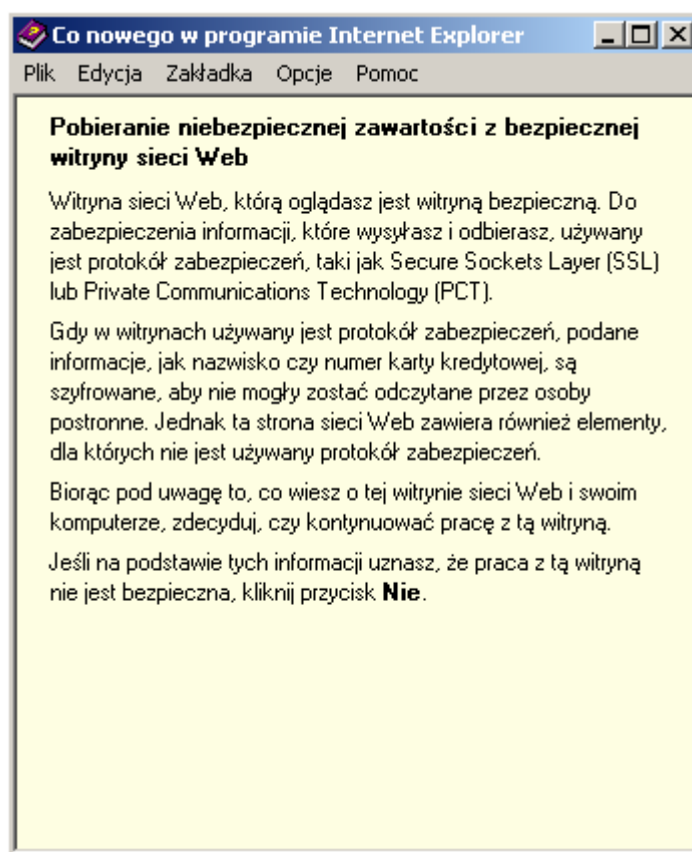



Wybór przycisku **Tak** spowoduje, że przeglądarka nie wyświetli dla nowo otwartej strony ikony kłódki w pasku stanu przeglądarki, ale nawiązane połączenie będzie szyfrowane, a adres strony będzie rozpoczynał się od wpisu **https**.

Na stronach, z którymi nawiązano szyfrowane połączenie (adres rozpoczynający się od **https**), oraz dla których nie jest wyświetlana ikona kłódki, również możliwe jest wyświetlenie certyfikatu. Żeby to zrobić należy kliknąć w puste miejsce, w którym na pasku stanu powinna widnieć kłódka.

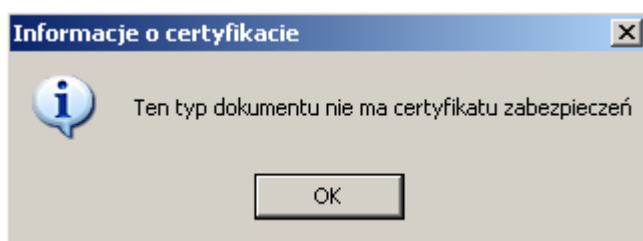
Jeżeli użytkownik wybierze przycisk **Nie**, nowo wyświetlona strona będzie zawierała jedynie elementy, do przesłania których zostało użyte połączenie szyfrowane. Inne elementy nie zostaną wyświetlone. Wyświetlona strona będzie oznaczona ikoną kłódki  w pasku stanu przeglądarki, a adres strony będzie rozpoczynał się od wpisu **https**.

Wybór przycisku **Więcej informacji** spowoduje wyświetlenie okna z informacjami o połączeniu, które możemy nawiązać z nową stroną. Informacja dotyczy głównie tego, że strona WWW zawiera również elementy, dla których nie są używane protokoły zabezpieczeń.



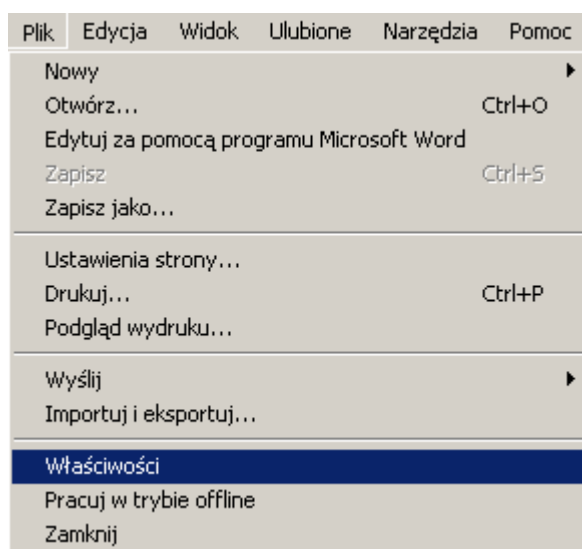
Okno zamykamy klikając znak  znajdujący się w prawym górnym rogu okna bądź wybierając z górnego menu **Plik**, a potem **Zakończ**.

Jeżeli przeglądana strona nie jest zabezpieczona certyfikatem, a użytkownik kliknie dwukrotnie w miejsce na pasku stanu przeglądarki, w którym powinien widnieć znak kłódki, ukaże się poniższy komunikat:

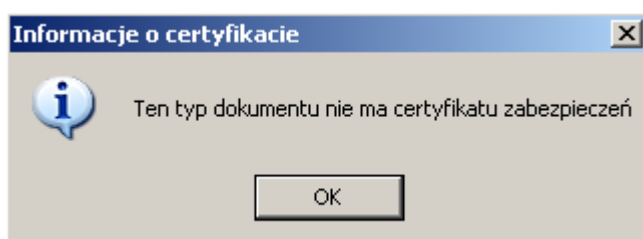


Będzie to potwierdzenie informacji, że serwer WWW nie ma certyfikatu i przeglądarka nie może nawiązać bezpiecznego połączenia z umieszczonymi na nim stronami WWW.

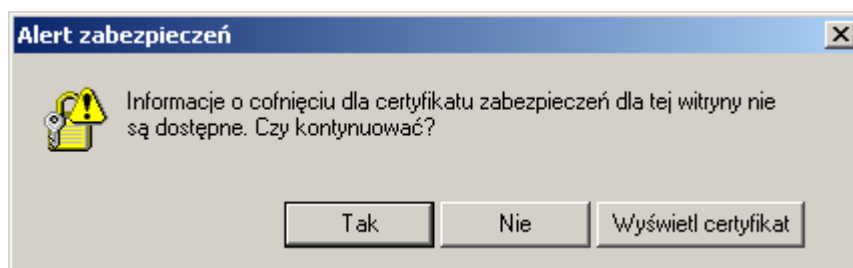
Identyczny komunikat możemy uzyskać wybierając z górnego menu przeglądarki Microsoft Internet Explorer **Plik**, a następnie **Właściwości**.



Ukaże się okno „Właściwości”, w którym należy kliknąć przycisk **Certyfikaty**. Wyświetlony zostanie identyczny komunikat:



Użytkownik może spotkać się z sytuacją, gdy przeglądarka Microsoft Internet Explorer łącząc się ze stroną internetową zabezpieczoną certyfikatem wyświetli komunikat następującej treści:

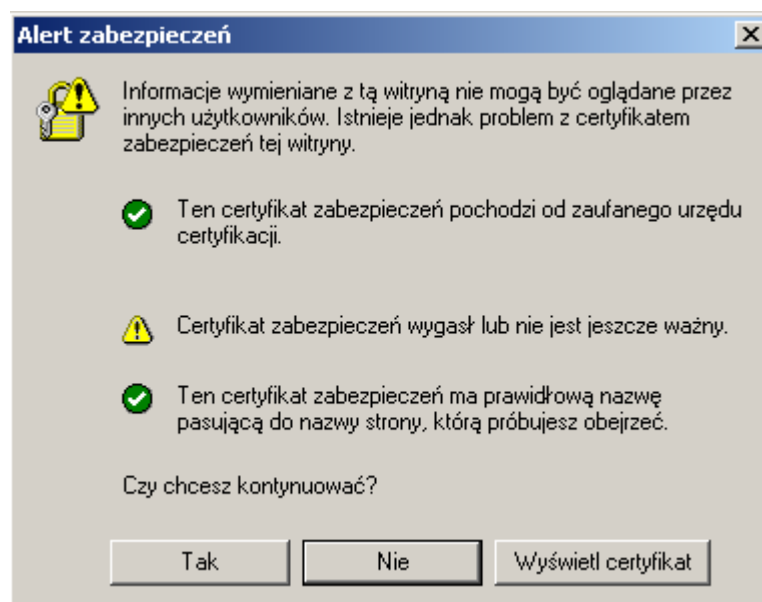


Ważność certyfikatu zabezpieczającego stronę jest sprawdzana przy każdej próbie połączenia się przeglądarki z serwerem, na którym umieszczono zabezpieczoną stronę WWW, pod warunkiem, że w ustawieniach przeglądarki została włączona funkcja **Sprawdź, czy certyfikat serwera nie został cofnięty** (opis aktywowania funkcji w dalszej części instrukcji). Internet Explorer próbuje połączyć się z serwerami wystawcy certyfikatu i sprawdza, czy certyfikat nie został unieważniony. Jeżeli próba połączenia z serwerami wystawcy certyfikatu nie powiedzie się, pojawi się powyższy komunikat. Oznaczać on będzie, że Internet Explorer nie mógł zweryfikować ważności certyfikatu przedstawionego przez serwer WWW, na którym znajduje się oglądana strona internetowa.

Wybór przycisku **Tak** spowoduje nawiązanie szyfrowanego połączenia ze stroną zabezpieczoną certyfikatem, należy jednak wziąć pod uwagę, że certyfikat może być już nieważny.

Wybranie przycisku **Nie** spowoduje, że Internet Explorer zablokuje otwarcie strony, dla której nie można było zweryfikować ważności certyfikatu.

Jeżeli za pomocą przeglądarki połączymy się z serwerem WWW, którego certyfikat wygaś (skończył się jego okres ważności), Internet Explorer wyświetli poniższy komunikat:



Jeżeli użytkownik nie chce dalej przeglądać stron ze względu na brak zabezpieczeń (nieważny certyfikat), powinien wybrać przycisk **Nie**. Spowoduje to, że dalsze przeglądanie stron WWW, które są opatrzone certyfikatem tego serwera, nie będzie możliwe.


Użytkownik może dalej przeglądać strony jeśli wybierze przycisk **Tak**. Spowoduje to nawiązanie szyfrowanego połączenia między przeglądarką a serwerem, jednak należy brać pod uwagę, że certyfikat serwera jest nieważny, a przeglądane strony - niewiarygodne. Mogą one zawierać niebezpieczny kod (np. wirusa), przekierowywać dane do osób trzecich lub zawierać nieprawdziwe informacje.

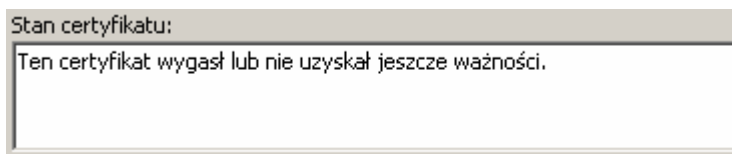
Jeżeli wybrany zostanie przycisk **Wyświetl certyfikat**, ukaże się okno „Certyfikat”, gdzie w zakładce **Ogólne** będzie wyświetlona poniższa informacja.

**Informacje o certyfikacie**

Ten certyfikat wygaś lub nie uzyskał jeszcze ważności.

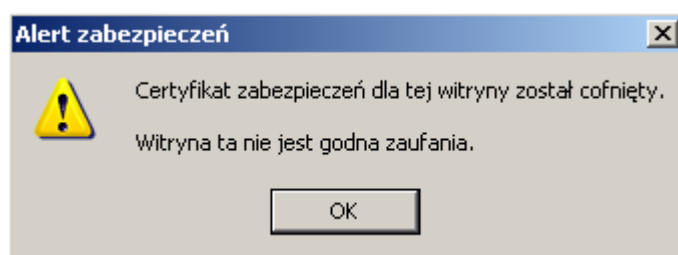
Wybrawszy zakładkę **Szczegóły** okna „Certyfikat” możemy zapoznać się z okresem ważności certyfikatu i upewnić się, że certyfikat wygaś. Pola związane z okresem ważności to **Ważny od** oraz **Ważny do**.

W zakładce **Ścieżka certyfikacji** z lewej strony certyfikatu, który wygaś, ukaże się znak . Jeżeli zaznaczymy certyfikat, który wygaś, w polu **Stan certyfikatu** znajdującym się w dolnej części zakładki, będzie widniał wpis **Ten certyfikat wygaś lub nie uzyskał jeszcze ważności**.




Okno „Certyfikaty” zamykamy przyciskiem **OK**.

Jeżeli za pomocą przeglądarki połączymy się z serwerem WWW, którego certyfikat został unieważniony, a w ustawieniach przeglądarki włączona jest opcja **Sprawdź, czy certyfikat serwera nie został cofnięty**, oprócz komunikatu o nawiązywaniu bezpiecznego połączenia ukaże się poniższy komunikat:

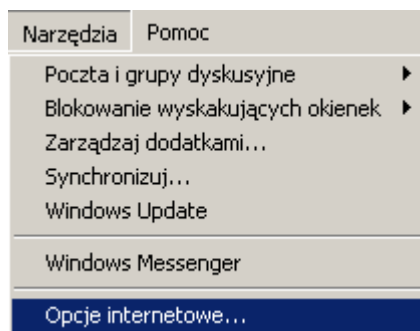


Kliknięcie przycisku **OK** spowoduje zamknięcie okna z komunikatem, a strona internetowa, której certyfikat unieważniono, nie zostanie wyświetlona.

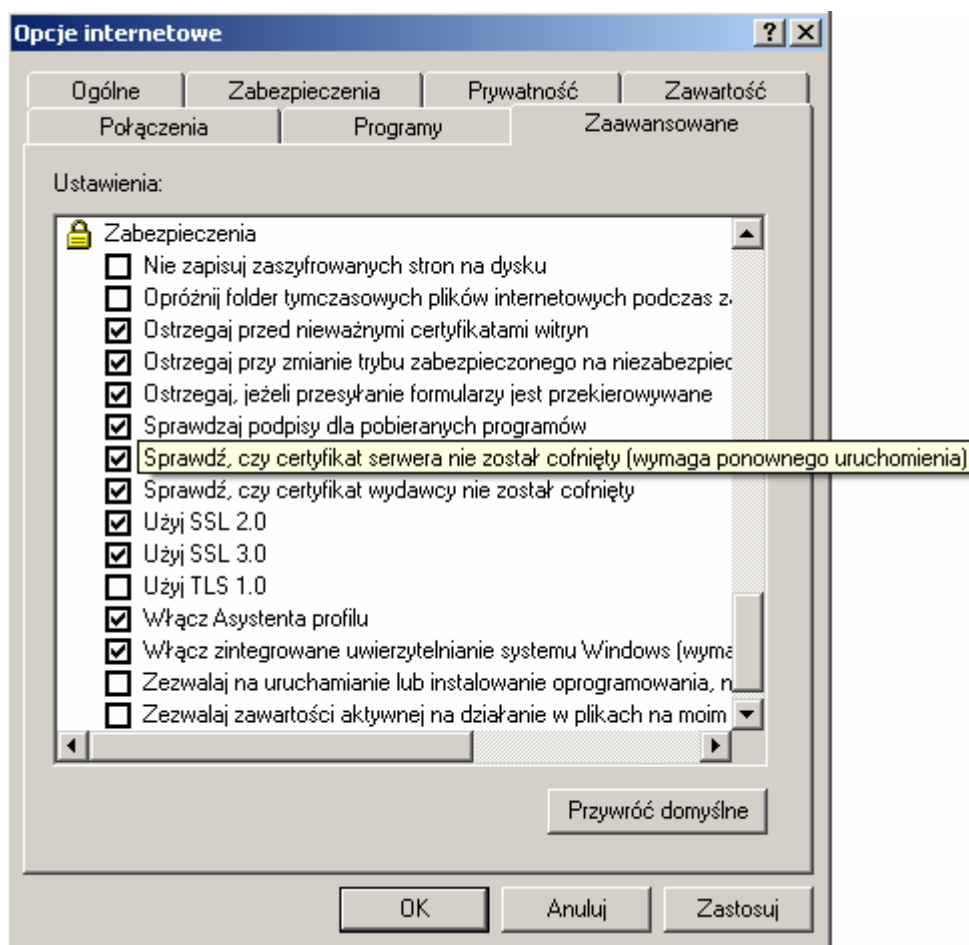
Jeżeli w przeglądarce nie włączono opcji **Sprawdź, czy certyfikat serwera nie został cofnięty**, podczas łączenia się z serwerem WWW, którego certyfikat jest unieważniony, nie pojawi się żadne ostrzeżenie, a przeglądarka pokaże żadaną stronę WWW. Podwójne kliknięcie ikony kłódki  w pasku stanu okna przeglądarki ukaże informacje o certyfikacie serwera WWW, ale nie będzie w niej informacji o jego unieważnieniu.

UWAGA! W domyślnych ustawieniach przeglądarki internetowej Microsoft Internet Explorer opcja **Sprawdź, czy certyfikat serwera nie został cofnięty** jest wyłączona. Żeby zapewnić wysoki poziom bezpieczeństwa użytkownik powinien zaznaczyć w/w opcję postępując według poniższych zaleceń.

Żeby włączyć opcję **Sprawdź, czy certyfikat serwera nie został cofnięty**, należy z menu przeglądarki Microsoft Internet Explorer wybrać **Narzędzia**, a potem **Opcje internetowe**.

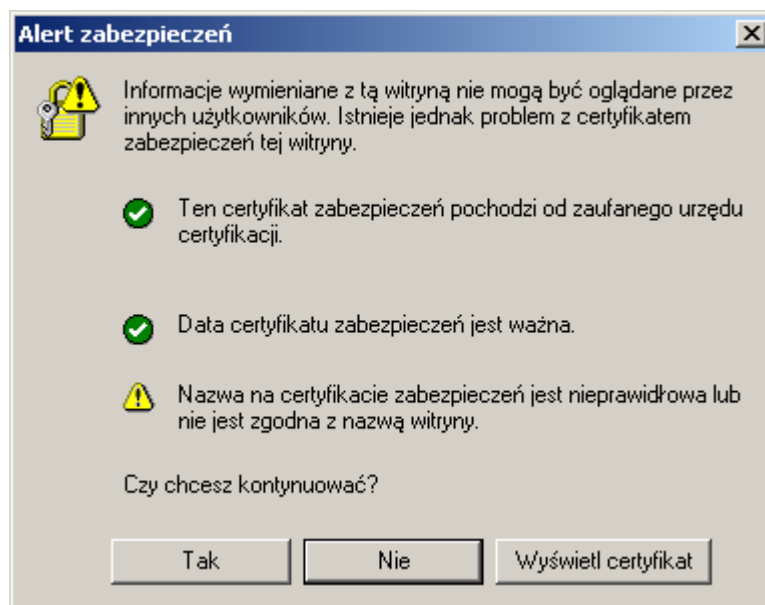


W nowo otwartym oknie „Opcje internetowe” wybieramy zakładkę **Zaawansowane**, w której zaznaczamy opcję **Sprawdź, czy certyfikat serwera nie został cofnięty**.



Wprowadzone zmiany zatwierdzamy przyciskiem **OK**, a potem zamykamy wszystkie otwarte okna przeglądarki.

Jeżeli przeglądarka nawiąże połączenie z serwerem WWW udostępniającym certyfikat, który został wystawiony dla innej domeny, ukazane zostanie poniższe okno.



Wybór przycisku **Tak** umożliwi wyświetlenie strony internetowej, która przedstawia taki certyfikat. Kliknięcie przycisku **Wyświetl certyfikat** ukaże okno „Certyfikat” ze szczegółowymi informacjami o otrzymanym certyfikacie serwera. Wybranie przycisku **Nie** spowoduje, że Microsoft Internet Explorer zablokuje otwarcie takiej strony internetowej.

3. Wykorzystanie certyfikatów użytkowników do uwierzytelniania

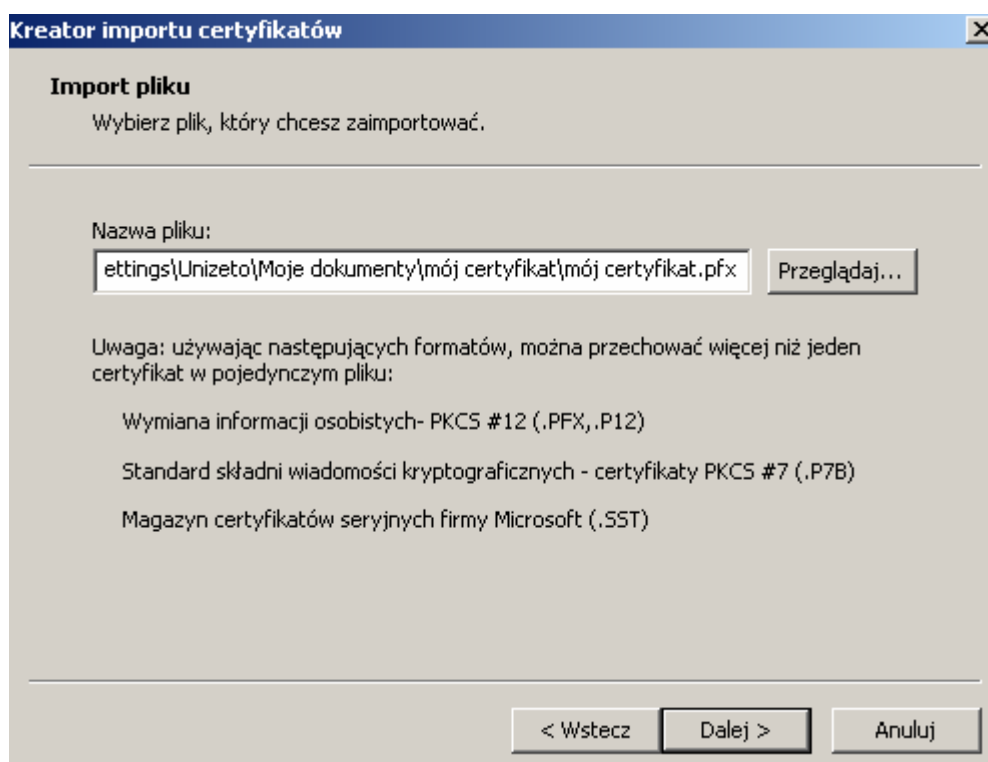
Poza opisaną w poprzednim rozdziale obsługą certyfikatów serwerowych, potwierdzających wiarygodność odwiedzanych stron WWW oraz umożliwiających szyfrowanie połączeń z tymi stronami, Internet Explorer pozwala na obsługę certyfikatów osobistych. Certyfikaty te, zawierające adres e-mail oraz dane określonej osoby, mogą być użyte za pomocą przeglądarki do uwierzytelniania użytkownika do określonych zasobów. Zasobami tymi mogą być zarówno internetowe strony WWW, strony WWW w sieci wewnętrznej dowolnej organizacji (firmy, urzędu, korporacji) lub aplikacje działające w technologii tzw. „cienkiego klienta”, czyli takie, które pracują na serwerze, a dostęp do nich odbywa się poprzez przeglądarkę internetową.

Zasoby te zazwyczaj dostępne są po uwierzytelnieniu się użytkownika. Najczęściej w tym celu stosowana jest metoda polegająca na podaniu loginu i hasła, jednak jest ona mało praktyczna i ma wiele wad (niski poziom bezpieczeństwa, łatwość utraty lub zapomnienia hasła itp.). Obecnie coraz powszechniejszą metodą uwierzytelnienia się jest użycie certyfikatu osobistego do identyfikacji użytkownika i przydzielenie mu na tej podstawie określonych uprawnień oraz dostępu do wybranych zasobów. Konieczne jest do tego posiadanie i zainstalowanie w przeglądarce własnego certyfikatu.

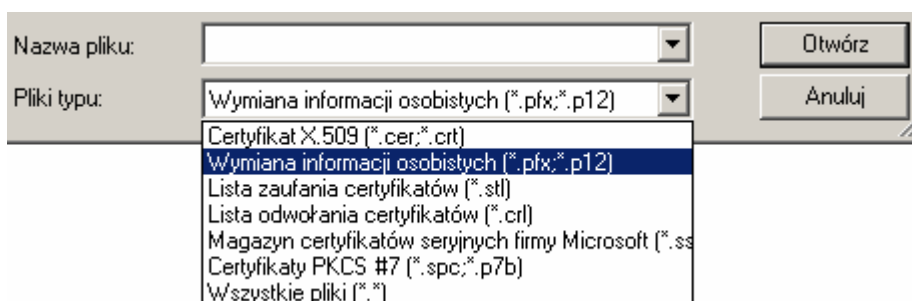
3.1. Instalacja własnego certyfikatu z pliku *.pfx

Pliki z rozszerzeniem *.pfx są plikami, które zawierają kopię bezpieczeństwa naszego certyfikatu osobistego. Jeżeli posiadamy plik z rozszerzeniem *.pfx zawierający klucz prywatny, klucz publiczny oraz certyfikat, możemy przystąpić do jego importu. Możemy to zrobić na trzy sposoby:

1. Lokalizujemy plik na dysku, klikamy nań dwa razy lewym przyciskiem myszy. Uruchomi się „Kreator importu certyfikatów”, w którym klikamy przycisk **Dalej**. Następnie wskazujemy lokalizację pliku, z którego będziemy pobierać certyfikat (program domyślnie tworzy ścieżkę do importowanego certyfikatu).



Naciskamy **Przełączaj**. Ukazuje się okno, w którym w polu **Pliki typu** wybieramy **Wymiana informacji osobistych (*.pfx;*.p12)**.



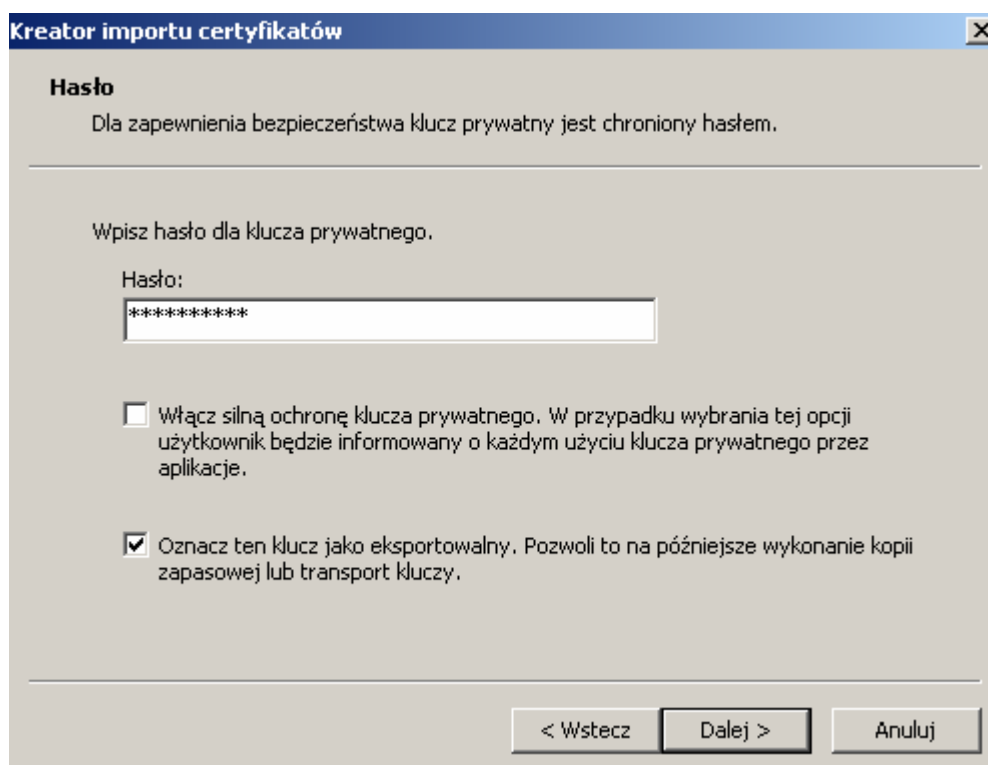
Lokalizujemy plik *.pfx z certyfikatem, a później zaznaczamy go i zatwierdzamy wybór przyciskiem **Otwórz**.

Klikamy **Dalej**, a potem podajemy hasło, którym zabezpieczony jest klucz prywatny. W tym samym oknie można zaznaczyć dwie dodatkowe opcje: **Włącz silną ochronę klucza prywatnego** oraz **Oznacz ten klucz jako eksportowalny**.

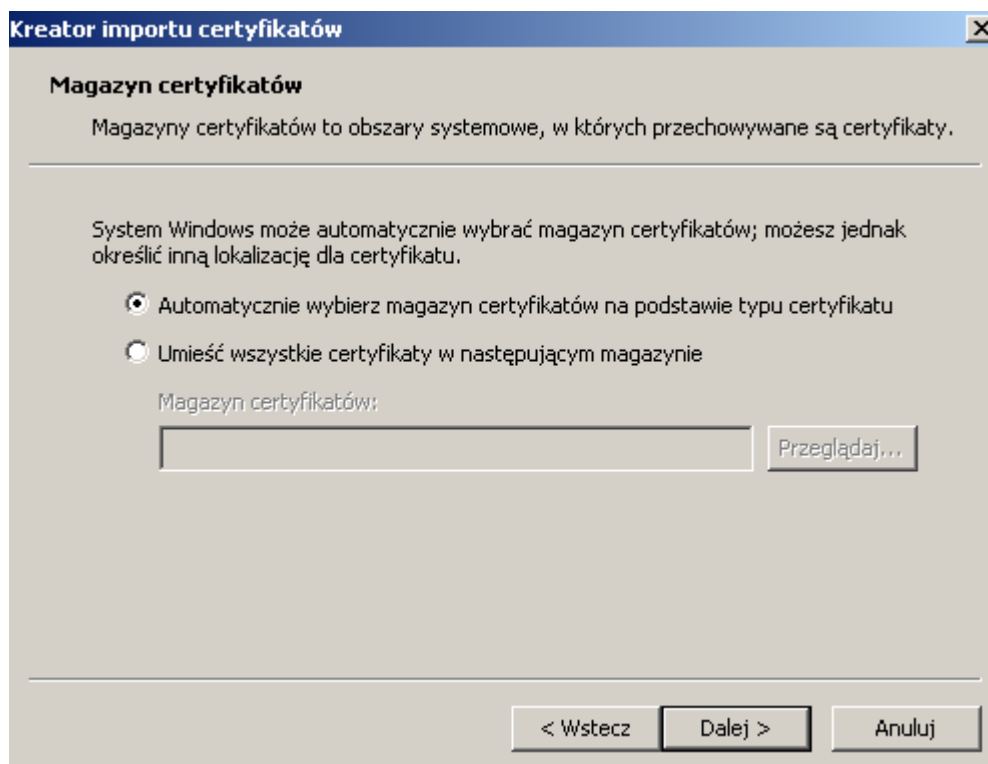
Zaznaczenie opcji **Włącz silną ochronę klucza prywatnego** spowoduje, że użytkownik będzie informowany o każdym użyciu klucza prywatnego przez aplikację.

Zaznaczenie opcji **Oznacz ten klucz jako eksportowalny** umożliwi użytkownikowi wykonanie w przyszłości kopii bezpieczeństwa kluczy, a następnie przeniesienie certyfikatu i kluczy na inną stację roboczą.

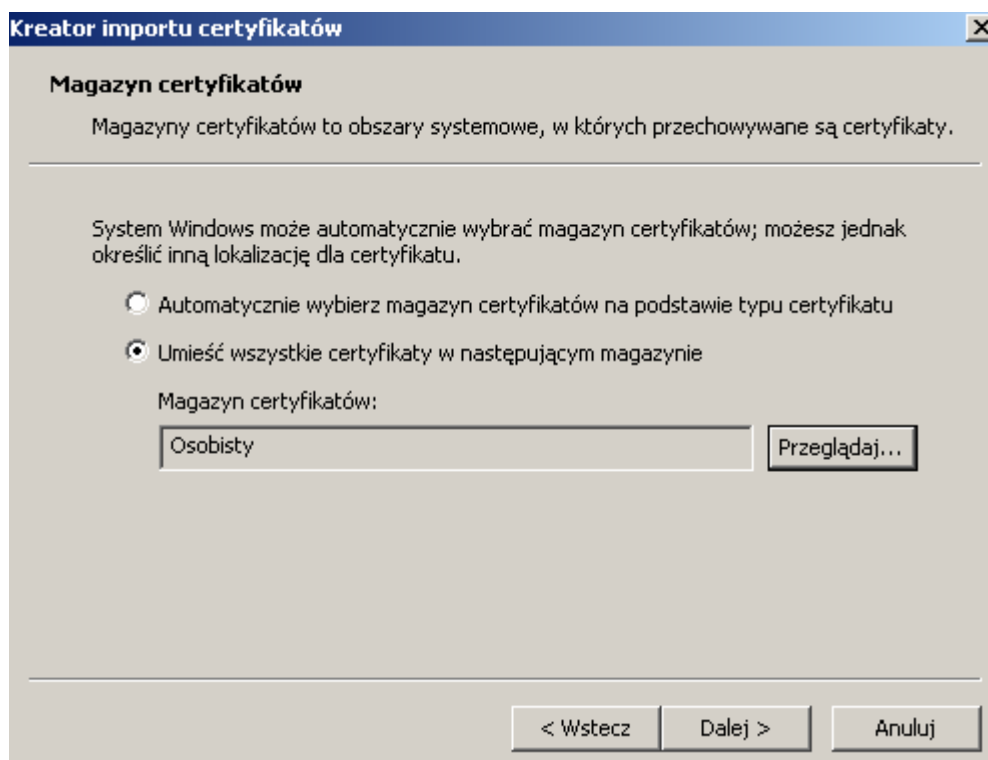
Naciskamy przycisk **Dalej**.



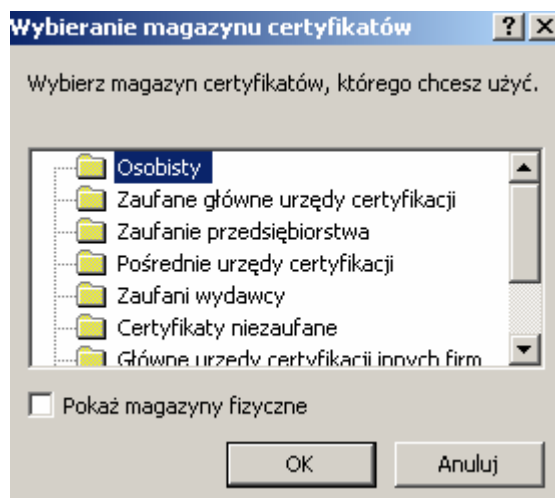
Potem zaznaczamy **Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu** i zatwierdzamy wybór przyciskiem **Dalej**.



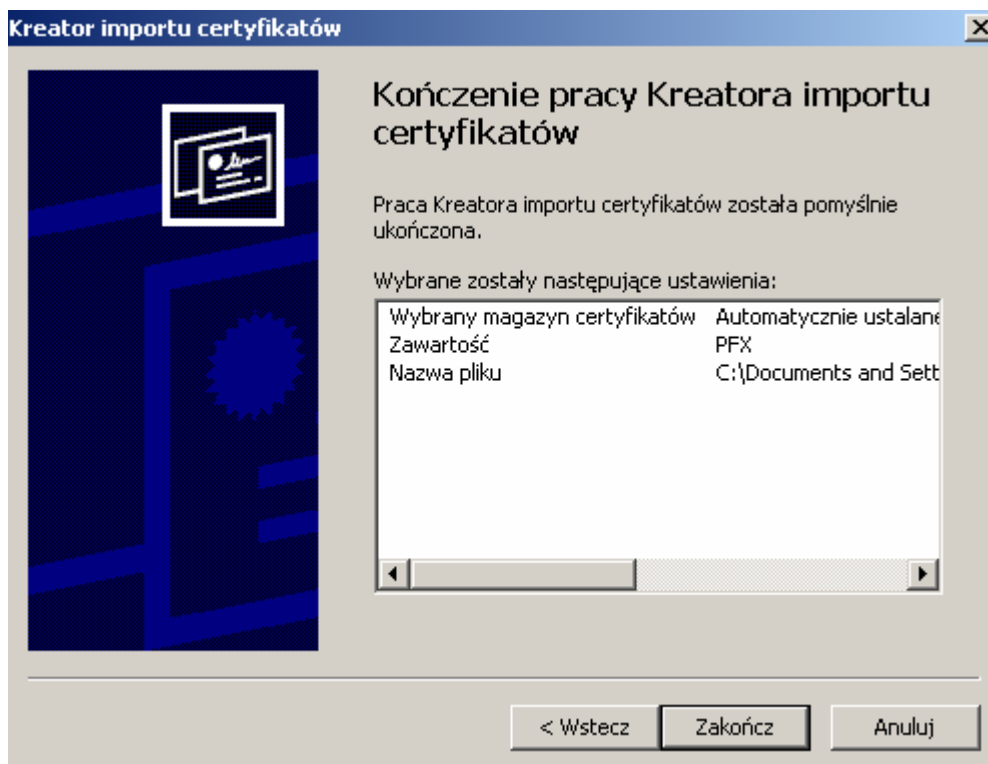
Można również wybrać samodzielnie magazyn, do którego zostanie przypisany importowany certyfikat. W tym celu należy zaznaczyć **Umieść wszystkie certyfikaty w następującym magazynie** i wybrać **Przełącznik**.



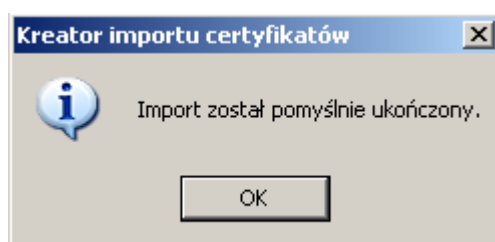
Następnie wybieramy magazyn **Osobisty** i potwierdzamy wybór przyciskiem **OK**.



Po kliknięciu **Dalej** ukaże się okno z wcześniej określonymi przez nas danymi związanymi z importem certyfikatu. Operację kończymy klikając **Zakończ**.

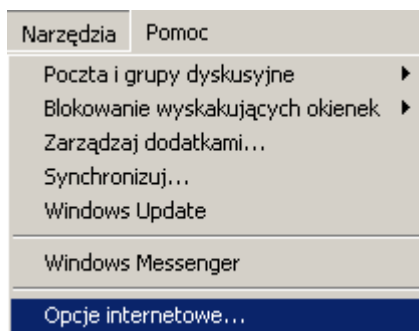


Poprawne zainstalowanie certyfikatu będzie potwierdzone następującym komunikatem:

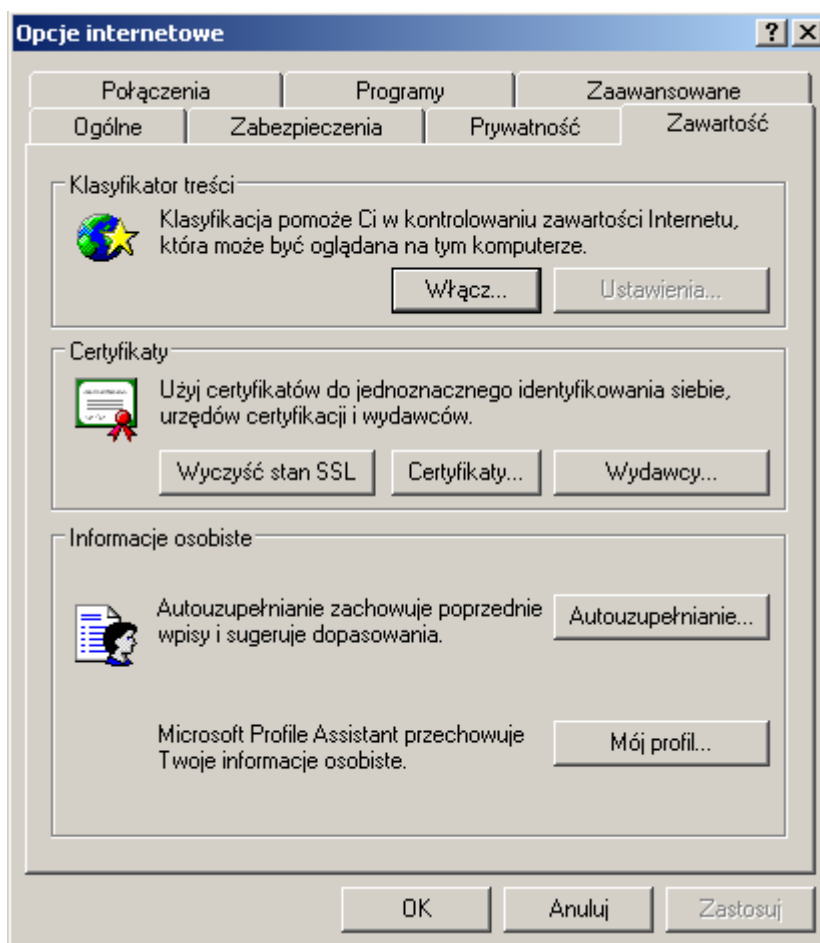


Certyfikat osobisty jest już zainstalowany w programie Microsoft Internet Explorer.

2. „Kreator importu certyfikatów” możemy także uruchomić wybierając z menu programu Microsoft Internet Explorer pozycję **Narzędzia**, a potem **Opcje internetowe**.



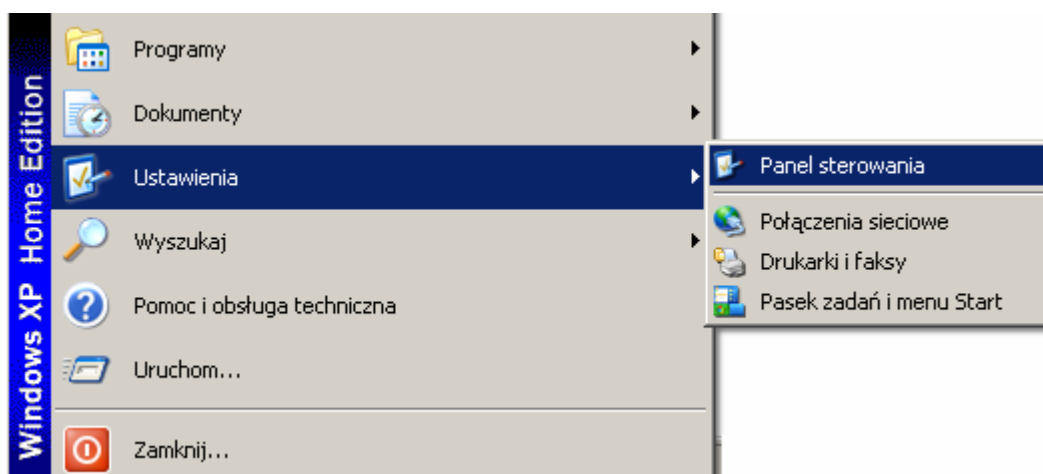
W oknie opcji internetowych wybieramy zakładkę **Zawartość**.



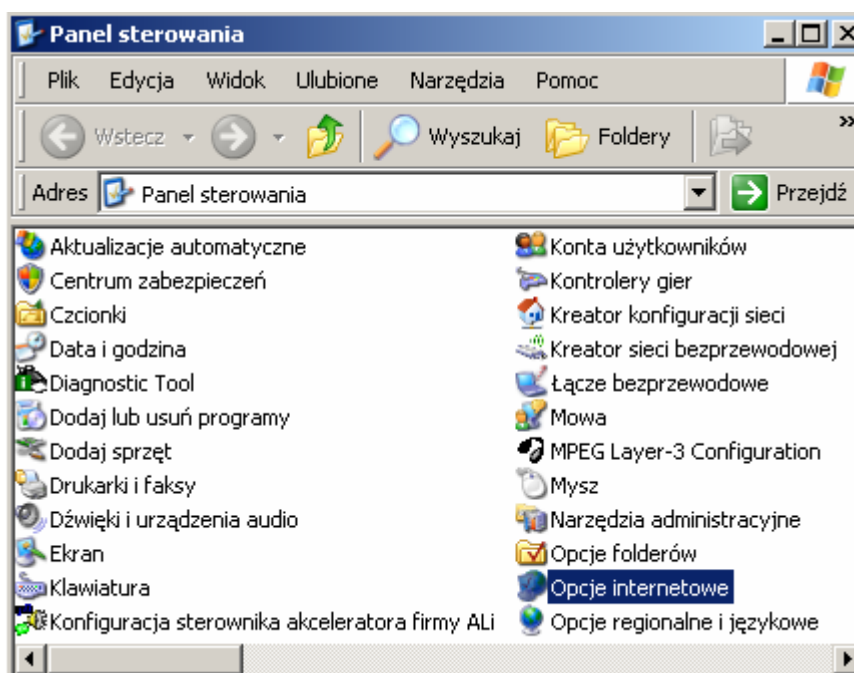
W części okna dotyczącej certyfikatów klikamy przycisk **Certyfikaty**. W nowo otwartym oknie „Certyfikaty” klikamy przycisk **Importuj**. Teraz postępujemy tak, jak w punkcie 1 od momentu pojawienia się „Kreatora importu certyfikatów”.

3. Trzecią metodą na zainstalowanie własnego certyfikatu z pliku *.pfx jest uruchomienie „Kreatora

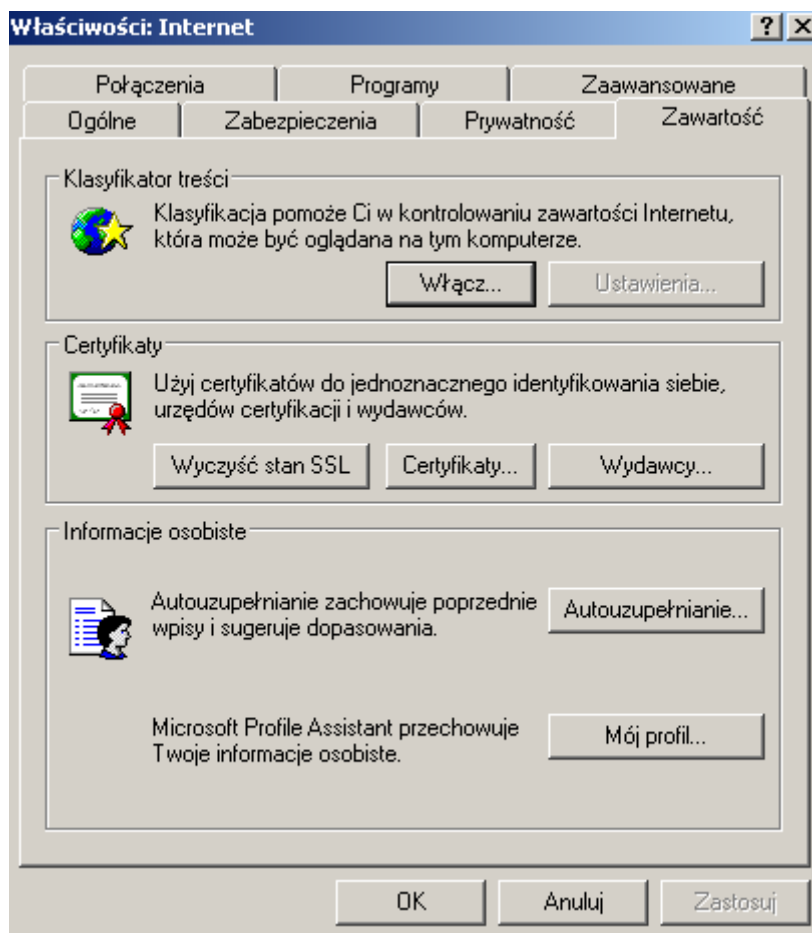
importu certyfikatów” z **Panelu Sterowania** w systemie operacyjnym Windows. Z menu **Start** wybieramy **Ustawienia**, a następnie **Panel sterowania**.



Ukaże się okno „Panel sterowania”.



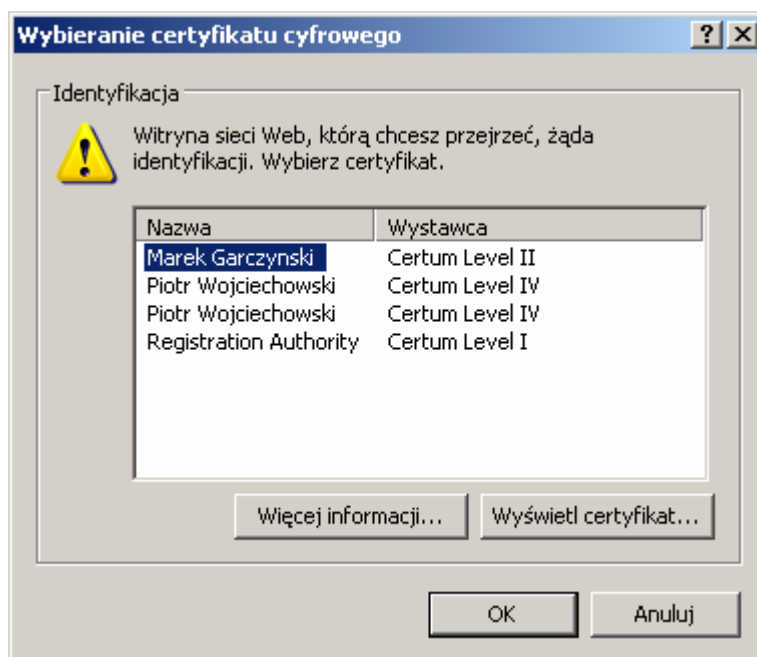
Wybieramy **Opcje internetowe**. W nowo otwartym oknie klikamy zakładkę **Zawartość**.



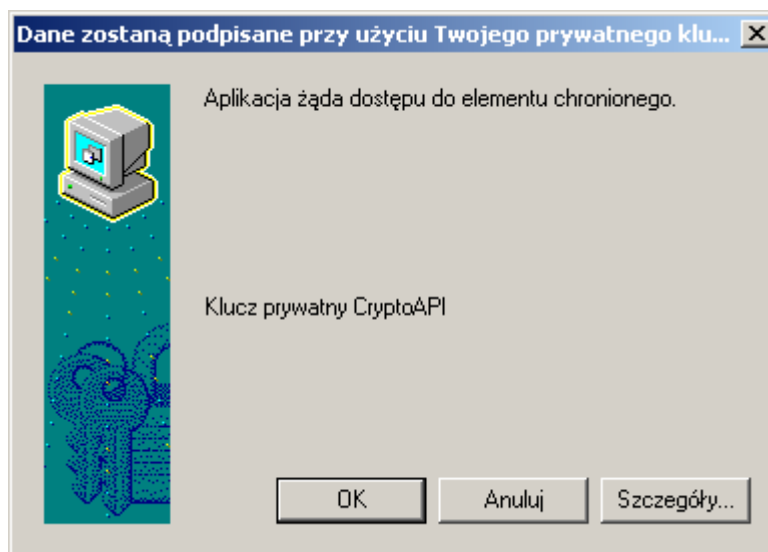
Klikamy przycisk **Certyfikaty**. Pojawi się okno „Certyfikaty”. Klikamy **Importuj**. Teraz postępujemy tak, jak w punkcie 1 od chwili pojawienia się „Kreatora importu certyfikatów”.

3.2. Uwierzytelnianie użytkownika

Certyfikaty niekwalifikowane, wydane przez CERTUM – Powszechne Centrum Certyfikacji można wykorzystać nie tylko do zabezpieczania serwerów WWW, ale również do uwierzytelniania użytkowników. Jeżeli serwer, z którym połączył się użytkownik, wymusza jego identyfikację za pomocą certyfikatu, ukaże się okno „Wybieranie certyfikatu cyfrowego”, w którym należy wskazać swój certyfikat osobisty. Potwierdzamy wybór klikając przycisk **OK**.

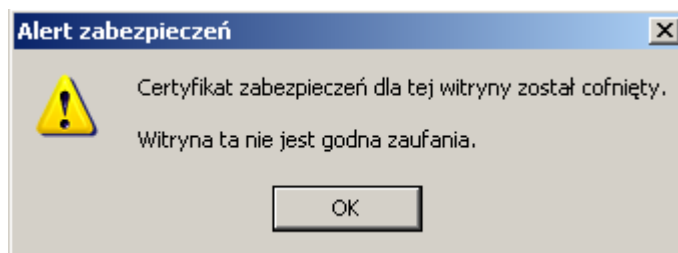


Kiedy pojawi się okno informujące o tym, że aplikacja żąda dostępu do elementu chronionego, wybieramy przycisk **OK**.



Kliknięcie przycisku **OK** spowoduje przesłanie do serwera certyfikatu użytkownika, a po jego weryfikacji przez serwer - uwierzytelnienie danej osoby.

Jeżeli certyfikat do uwierzytelniania, który przedstawimy serwerowi, będzie certyfikatem unieważnionym (wpisanym na listę certyfikatów unieważnionych CRL), wyświetlony zostanie poniższy komunikat.



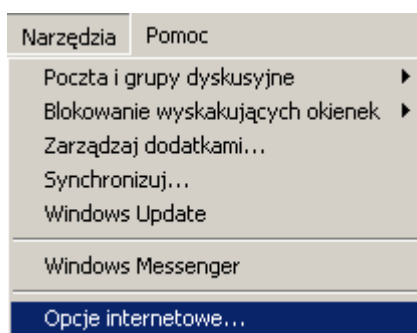
Oznacza on, że użytkownik nie został uwierzytelniony i nie ma dostępu do chronionych zasobów. Klikamy przycisk **OK**.

Jeśli certyfikat do uwierzytelniania, który przedstawimy serwerowi, będzie certyfikatem, który stracił ważność (wygasł), w oknie przeglądarki pojawi się informacja „Nie można wyświetlić strony”.

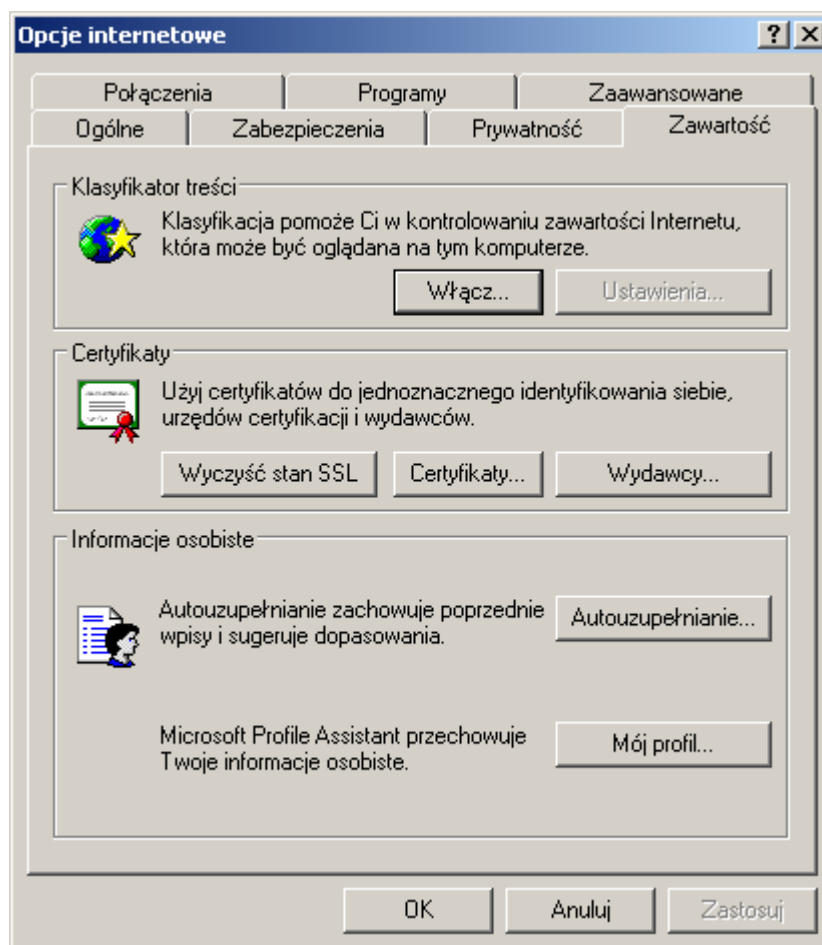


3.3. Wykonywanie kopii bezpieczeństwa własnego certyfikatu

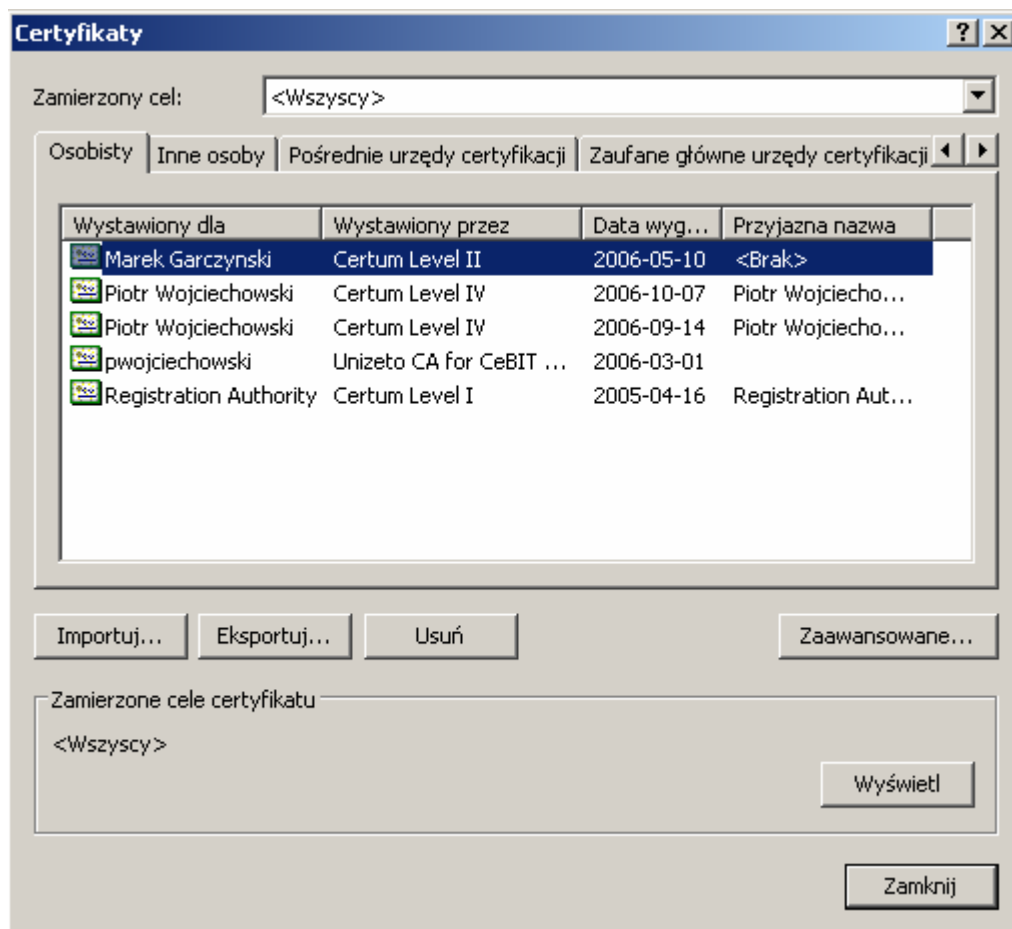
Aby wykonać kopie bezpieczeństwa własnego certyfikatu, należy z menu programu Microsoft Internet Explorer wybrać **Narzędzia**, a następnie **Opcje internetowe**.



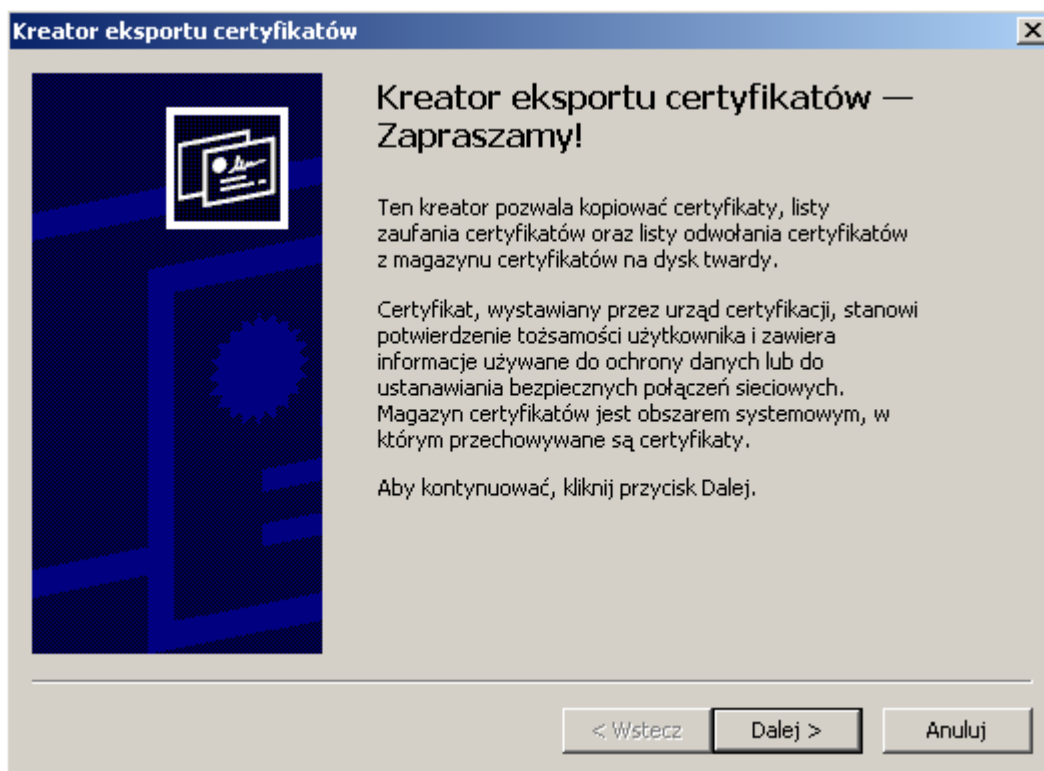
W nowo otwartym oknie „Opcje internetowe” wybieramy zakładkę **Zawartość**.



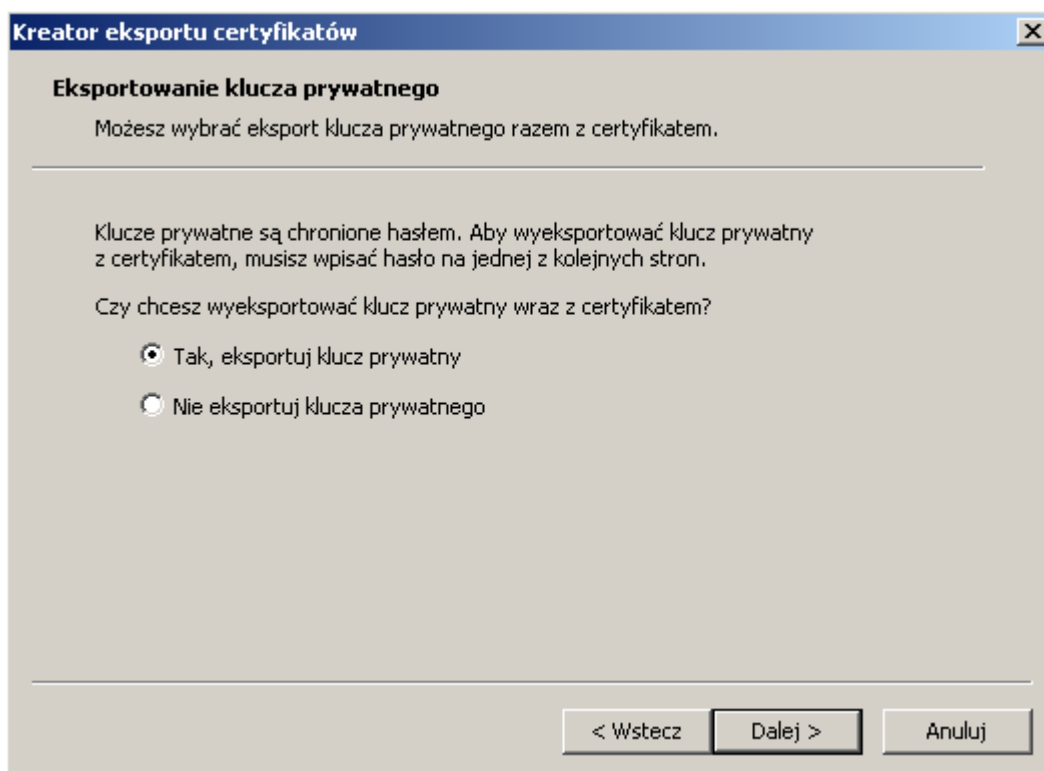
Klikamy przycisk **Certyfikaty**, a potem w zakładce **Osobisty** okna „Certyfikaty” zaznaczamy certyfikat, który będzie eksportowany i klikamy przycisk **Eksportuj**.



Pojawi się „Kreator eksportu certyfikatów”, w którym klikamy przycisk **Dalej**.



Następnie należy wybrać, czy certyfikat ma być eksportowany z kluczem prywatnym.



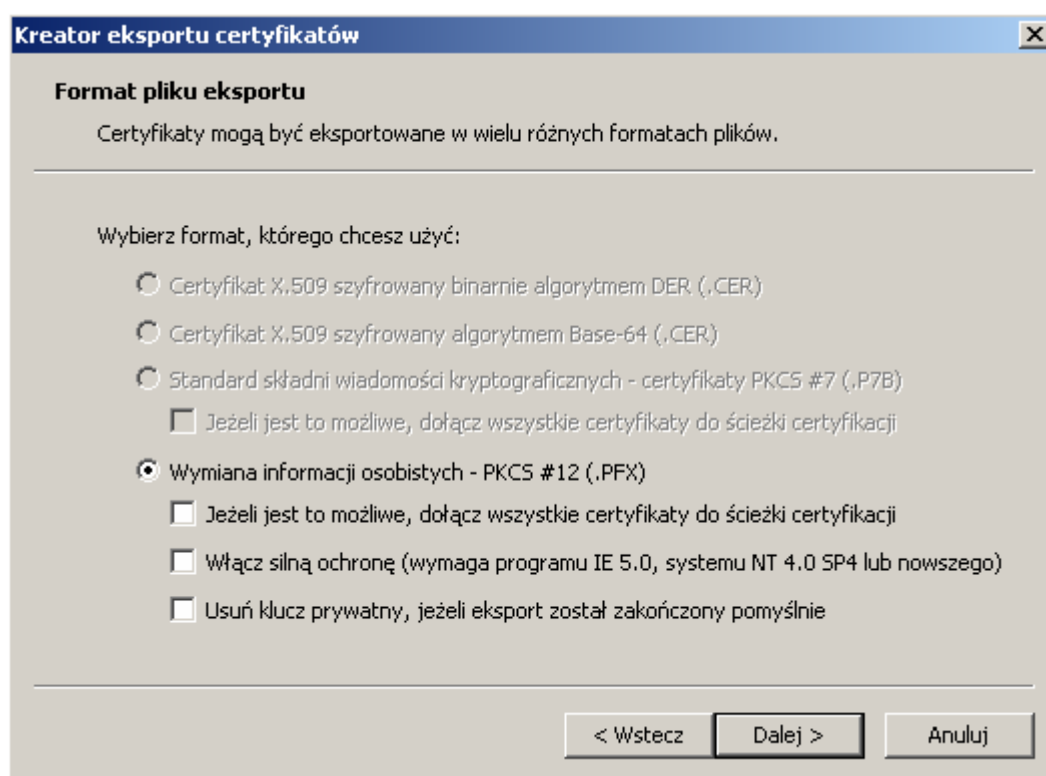
Zaznaczamy opcję **Tak, eksportuj klucz prywatny**, co spowoduje umieszczenie klucza prywatnego w pliku z certyfikatem. Dzięki temu w trakcie późniejszego importu certyfikatu z tego pliku Internet Explorer będzie rozpoznawał certyfikat jako certyfikat osobisty.

UWAGA! W przypadku zaznaczenia opcji **Nie eksportuj klucza prywatnego** utworzony zostanie plik z certyfikatem, którego nie będzie można zaimportować jako certyfikatu osobistego. Możliwy będzie tylko import tego certyfikatu jako certyfikatu innej osoby.

Po dokonaniu wyboru klikamy **Dalej**.

W kolejnym oknie należy zwrócić uwagę na opcję **Włącz silną ochronę**.

Zaznaczenie opcji **Włącz silną ochronę** może uniemożliwić import certyfikatu w przeglądarkach internetowych i programach pocztowych innych producentów niż Microsoft. Jeżeli zatem planujemy import certyfikatu z utworzonego pliku w programach innych producentów, nie należy zaznaczać opcji **Włącz silną ochronę**.



Potem wybieramy przycisk **Dalej**.

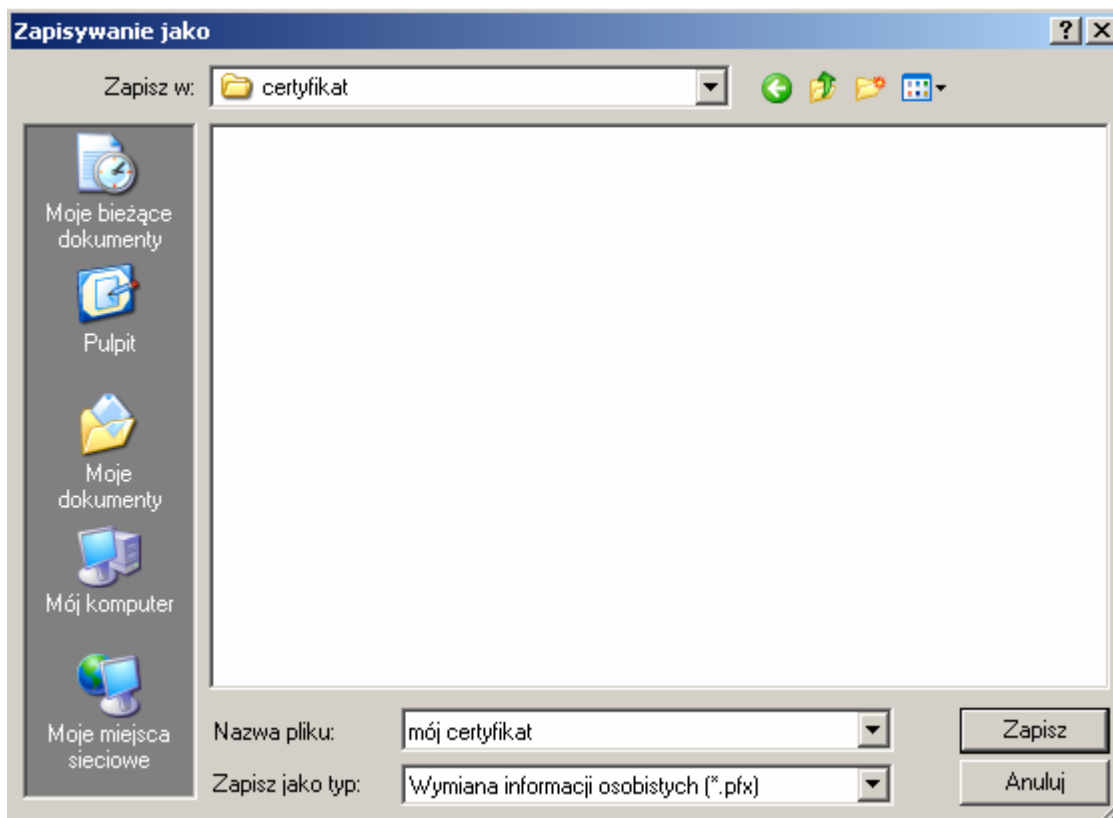
Wpisujemy hasło, które będzie zabezpieczało nasz klucz prywatny, a następnie potwierdzamy wpisując je ponownie w polu poniżej. Klikamy **Dalej**.

Wpisz i potwierdź hasło.

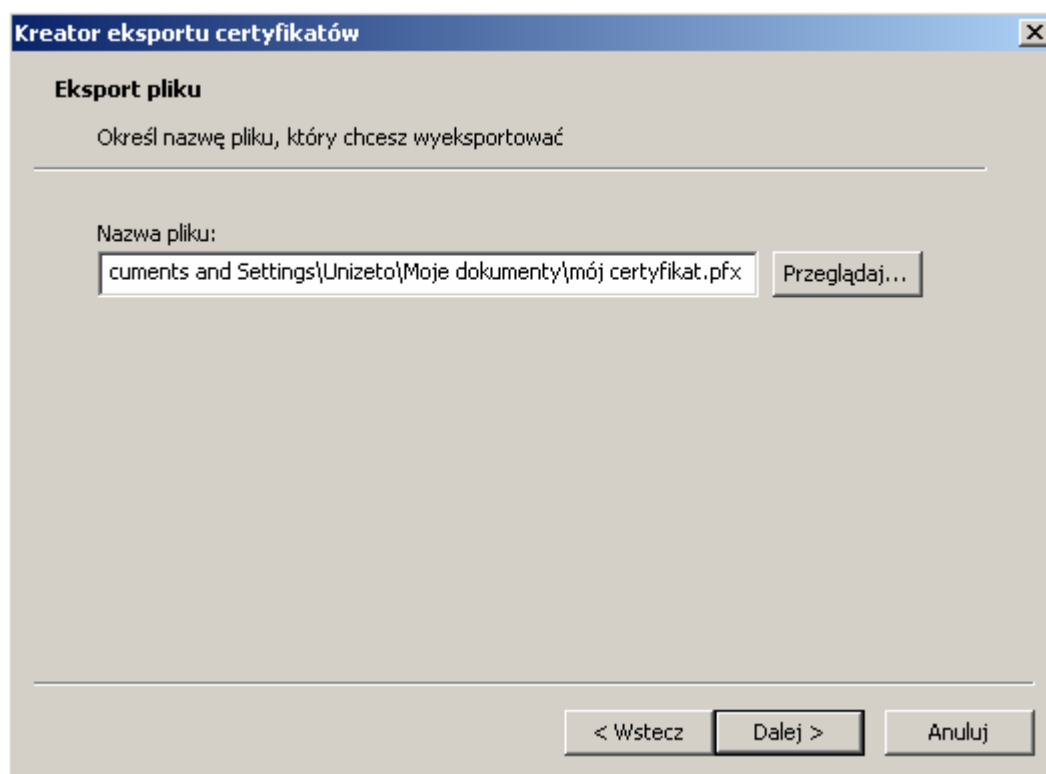
Hasło:

Potwierdź hasło:

„Kreator eksportu certyfikatów” poprosi o podanie nazwy pliku. Klikamy przycisk **Przeglądaj**. W nowo otwartym oknie wskazujemy lokalizację oraz wpisujemy nazwę pliku w polu **Nazwa pliku**. Wprowadzone dane zatwierdzamy przyciskiem **Zapisz**.



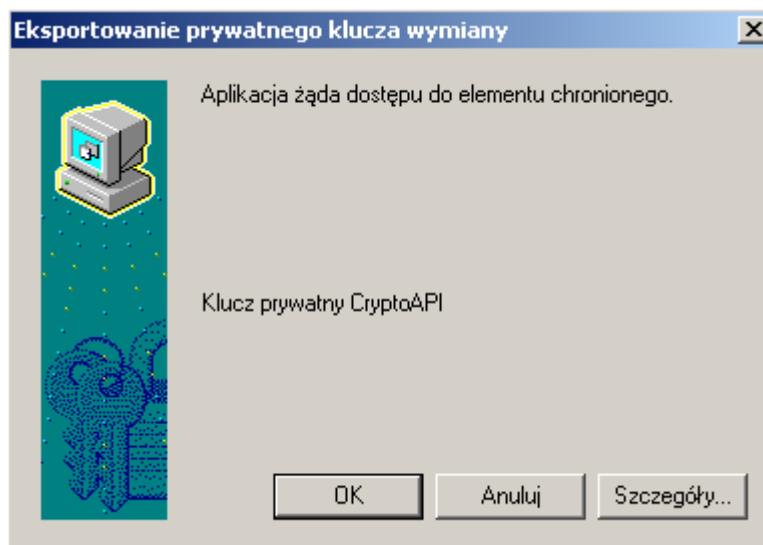
Po powrocie do głównego okna „Kreatora eksportu certyfikatów” klikamy **Dalej**.



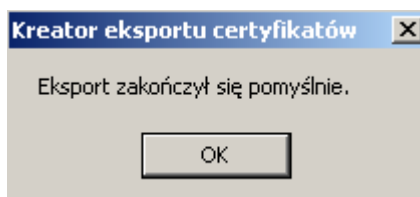
Kreator pokaże okno ze wszystkimi określonymi przez nas informacjami związanymi z eksportem.

Jeżeli informacje są prawidłowe, klikamy przycisk **Zakończ**.

Ukaże się okno informujące, że program żąda dostępu do elementu chronionego.



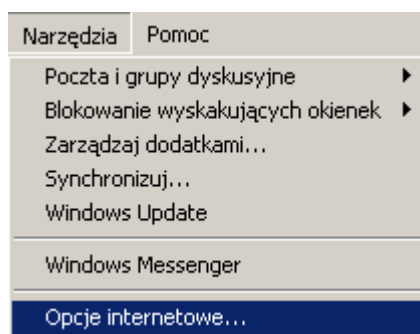
Klikamy **OK**. Zakończenie operacji eksportu będzie potwierdzone komunikatem „Eksport zakończył się pomyślnie”. Klikamy **OK**.



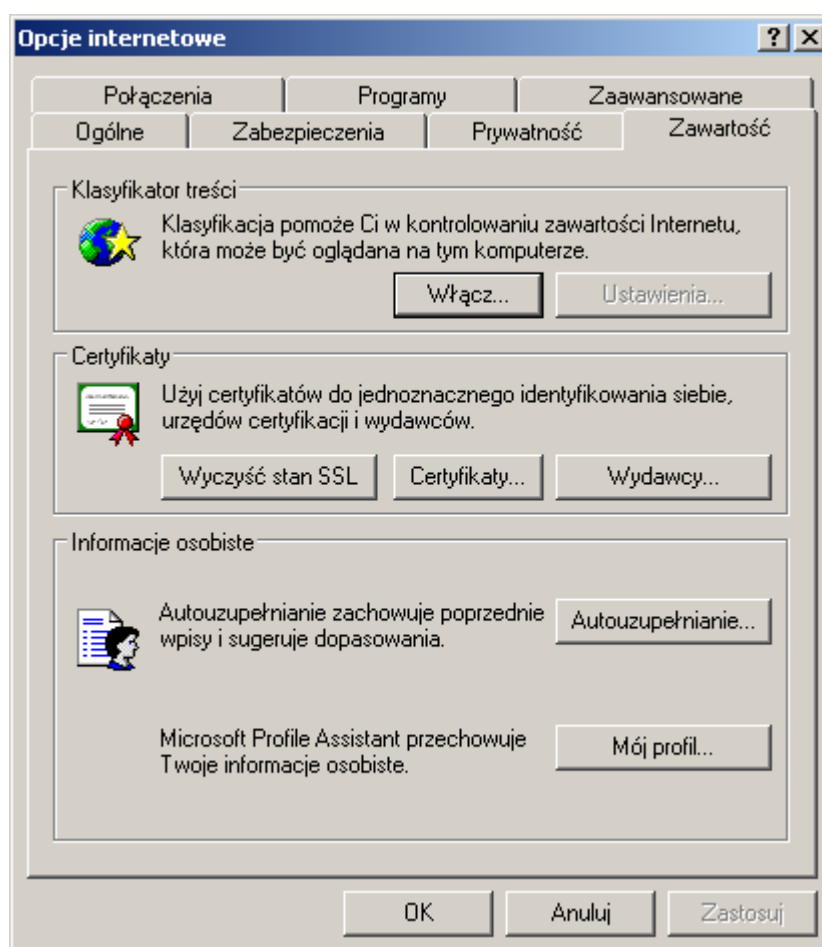
We wcześniej wybranym katalogu został utworzony plik z certyfikatem osobistym.

4. Usuwanie certyfikatów

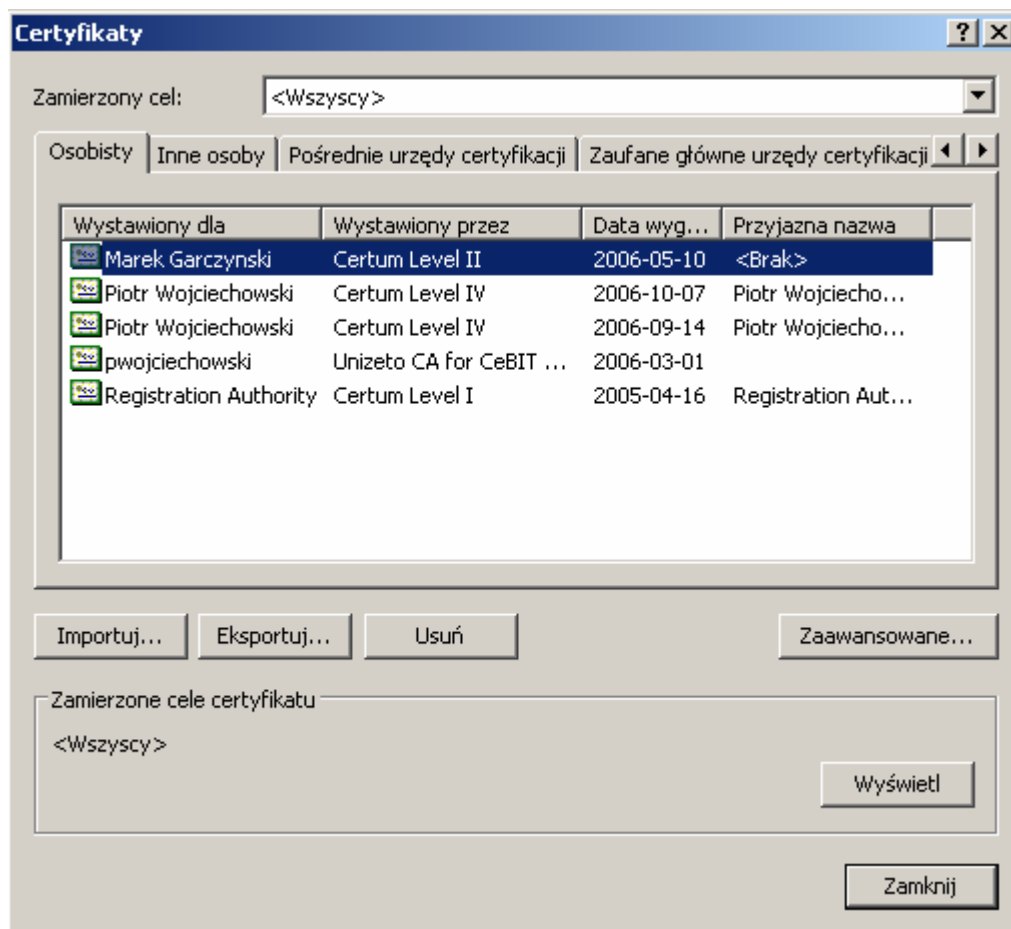
Aby usunąć własny certyfikat, należy w górnym menu programu Microsoft Internet Explorer wybrać **Narzędzia**, a następnie **Opcje internetowe**.



W nowo otwartym oknie „Opcje internetowe” wybieramy zakładkę **Zawartość**.

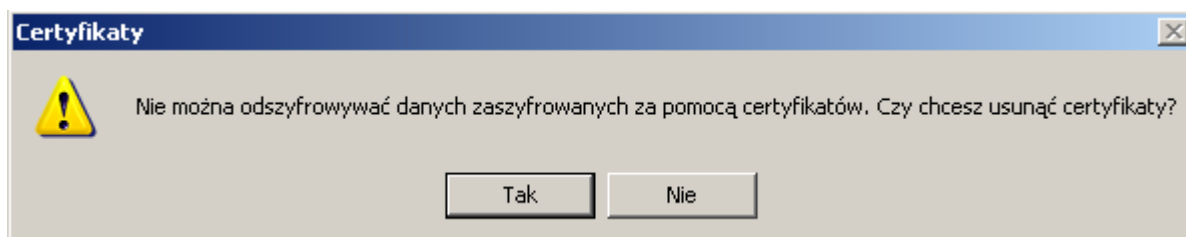


Klikamy przycisk **Certyfikaty**, a potem w oknie „Certyfikaty” zaznaczamy własny certyfikat, który chcemy usunąć.



Później klikamy przycisk **Usuń**.

Ukaże się komunikat z pytaniem czy jesteśmy pewni naszej decyzji.



Wybieramy przycisk **Tak**.

Usunięcie własnego certyfikatu powoduje utratę możliwości deszyfrowania dokumentów, które inni użytkownicy zaszyfrowali przy użyciu usuniętego certyfikatu. Jeżeli użytkownik przechowuje dokumenty, które są zaszyfrowane jego certyfikatem, nie powinien go usuwać. Po usunięciu certyfikatu nie ma żadnej możliwości odszyfrowania dokumentów zaszyfrowanych tym certyfikatem.

Certyfikaty innych osób oraz certyfikaty urzędów certyfikacji usuwa się tak samo, jak certyfikat własny, z tą tylko różnicą, że wyszukujemy je w innych zakładkach okna „Certyfikaty”. Różnica polega jedynie na wyświetleniu innego komunikatu przy kliknięciu przycisku **Usuń**.