



## Instrukcja obsługi certyfikatów w programie Mozilla 1.7 PL

## Spis treści

Wstęp .....	2
Import certyfikatów urzędów oraz list CRL.....	2
<i>Import certyfikatów urzędów</i> .....	2
<i>Import list CRL</i> .....	3
Instalacja certyfikatów osobistych .....	4
<i>Instalacja z karty mikroprocesorowej</i> .....	4
<i>Instalacja ze strony www.signet.pl</i> .....	8
<i>Instalacja certyfikatu w programie pocztowym</i> .....	9
Instalacja certyfikatów innych osób.....	10
<i>Import certyfikatów innych osób przez odebranie podpisanej wiadomości</i> .....	10
Import z pliku .....	11
<i>Import ze strony www.signet.pl</i> .....	12
Kopia zapasowa.....	14
<i>Eksport do pliku</i> .....	14
<i>Import z pliku</i> .....	15
Usuwanie certyfikatów .....	17
Podpisywanie i szyfrowanie wiadomości .....	19
<i>Wysyłanie wiadomości z podpisem cyfrowym</i> .....	19
<i>Szyfrowanie wysyłanych wiadomości</i> .....	20
<i>Odbieranie wiadomości szyfrowanych i podpisanych elektronicznie</i> .....	21

## Wstęp

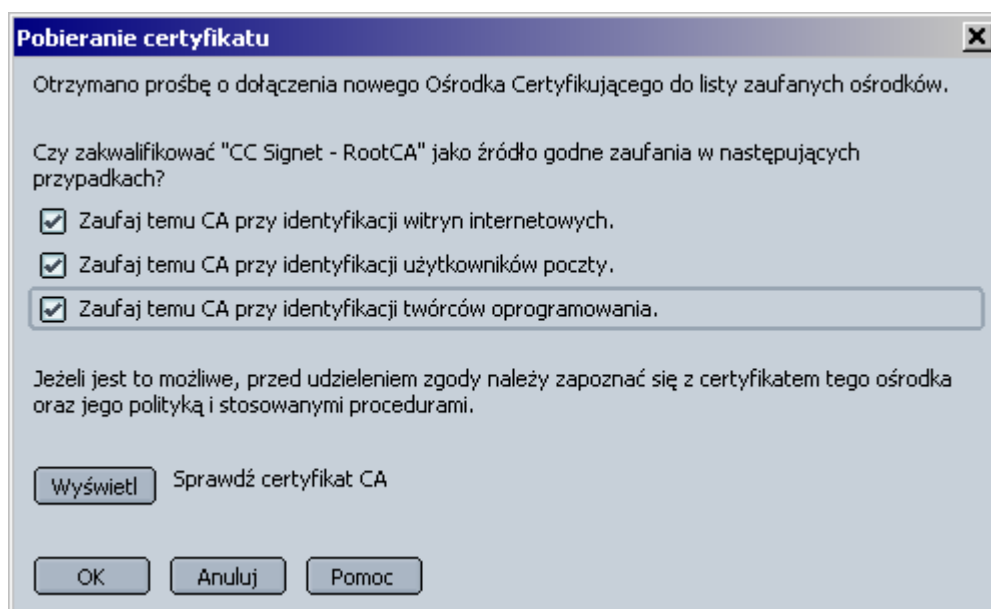
Jest to dokument, który pokaże Ci, jak poprawnie skonfigurować program **Mozilla 1.7 PL**, aby korzystać z certyfikatów wystawionych przez **Centrum Certyfikacji Signet**. Kolejne rozdziały pomogą Ci przejść przez wszystkie etapy instalacji certyfikatów. W efekcie będziesz mógł z łatwością korzystać z certyfikatów.

Program **Mozilla** jest przeglądarką internetową przeznaczoną dla użytkowników wielu systemów operacyjnych (MS Windows, Linux, Mac OS). Jest to aplikacja bezpłatna, jej polska wersja jest dostępna na stronie <http://mozillapl.org/pobierz/>. Inne wersje językowe są dostępne na stronie <http://www.mozilla.org/products/mozilla1.x/>.

## Import certyfikatów urzędów oraz list CRL

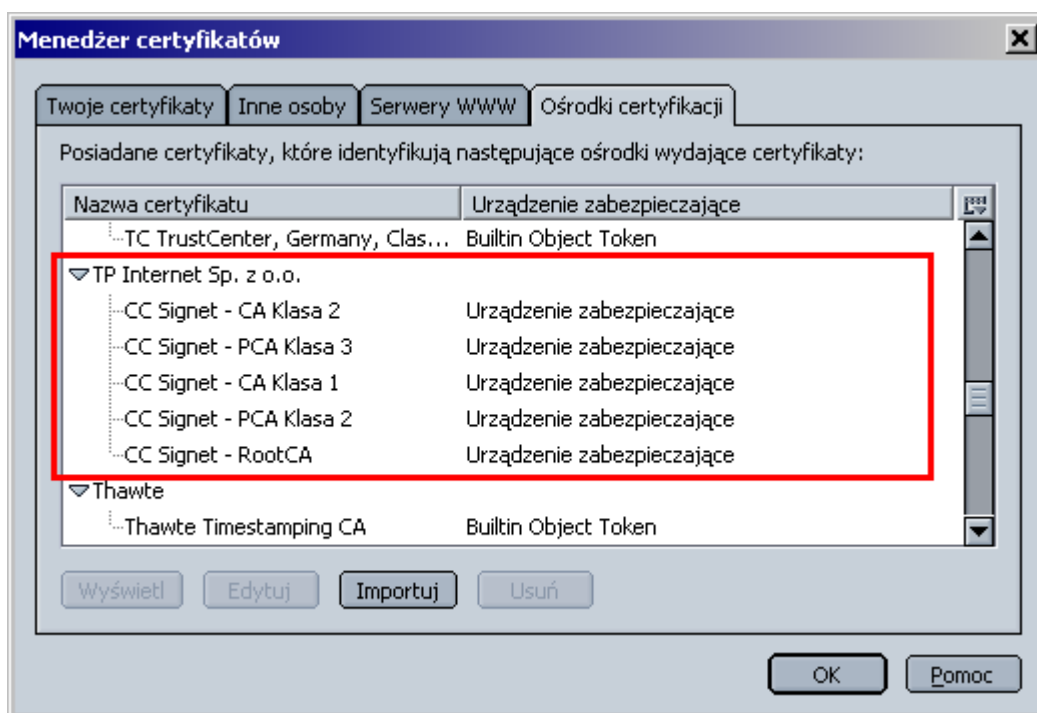
### *Import certyfikatów urzędów*

Podstawowym krokiem, jaki należy podjąć przed rozpoczęciem korzystania z certyfikatów osobistych wystawionych przez centrum certyfikacji jest import certyfikatów urzędów tego centrum oraz tworzonych przez to centrum list CRL. W programie **Mozilla 1.7 PL** można te elementy 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 DER. Po każdym kliknięciu pojawi się poniższy komunikat:



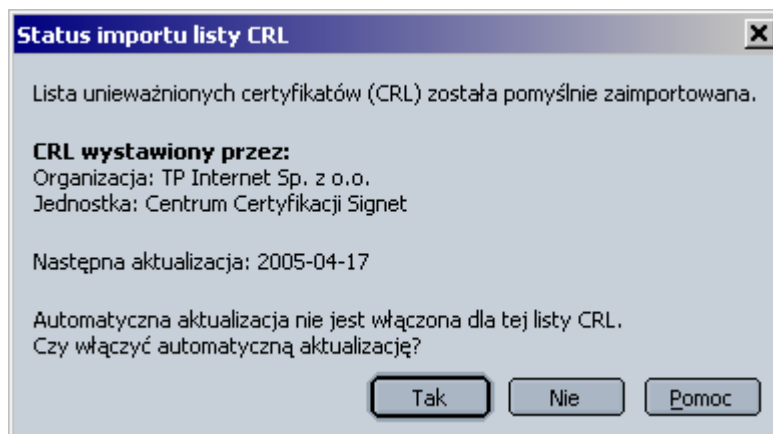
Należy zaznaczyć opcje tak jak to pokazano powyżej i nacisnąć **OK**. Powyższą czynność należy powtórzyć dla każdego z urzędów.

Po wykonaniu importu certyfikatów można sprawdzić czy okno **Edycja/Preferencje/Prywatność i zabezpieczenia/Certyfikaty/Menedżer certyfikatów** w zakładce **Ośrodki certyfikacji** wygląda następująco:

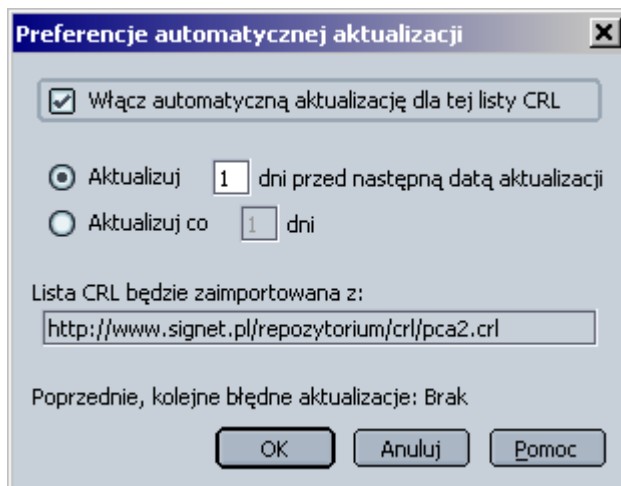


### Import list CRL

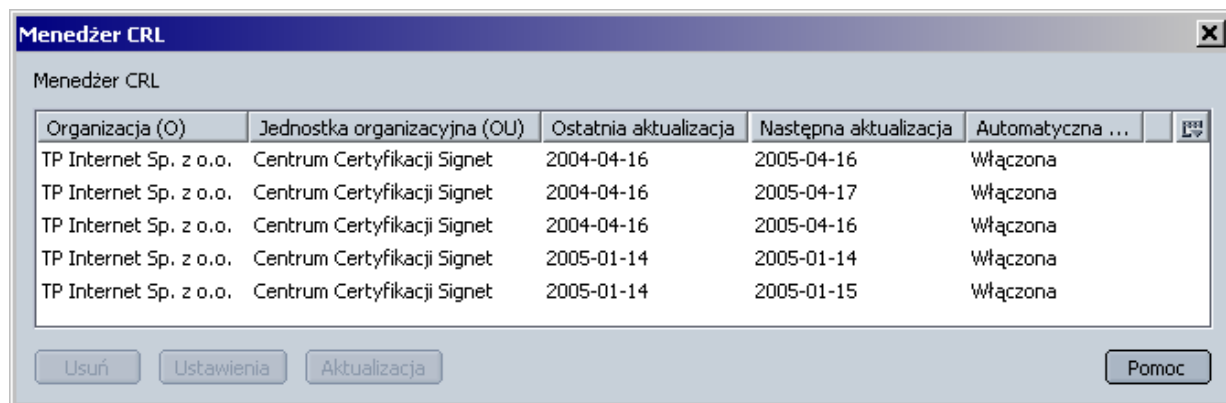
Po pomyślnym imporcie certyfikatów urzędów należy dokonać importu list CRL tworzonych przez te urzędy. W tym celu na powyższej stronie należy przejść do tabeli **Listy certyfikatów unieważnionych (CRL)** oraz zaimportować każdą z list klikając na kolejnych linkach. Po każdym kliknięciu pojawi się komunikat:



Należy wybrać przycisk **Tak**, w kolejnym oknie zaznaczyć opcję **Włącz automatyczną aktualizację dla tej listy CRL** i wybrać przycisk **OK**:



Po wykonaniu importu certyfikatów można sprawdzić czy okno **Edycja/Preferencje/Prywatność i zabezpieczenia/Weryfikacja/Menedżer CRL** wygląda następująco:



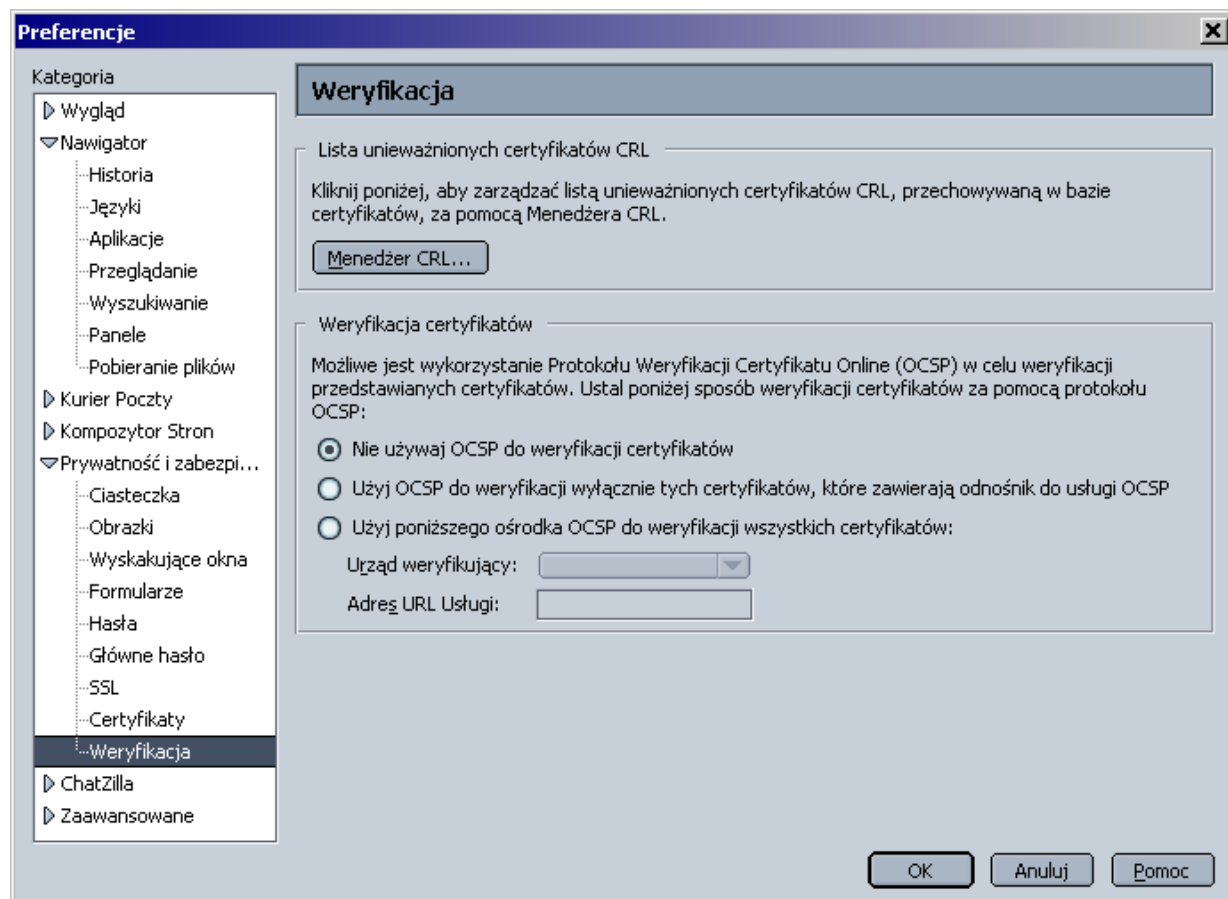
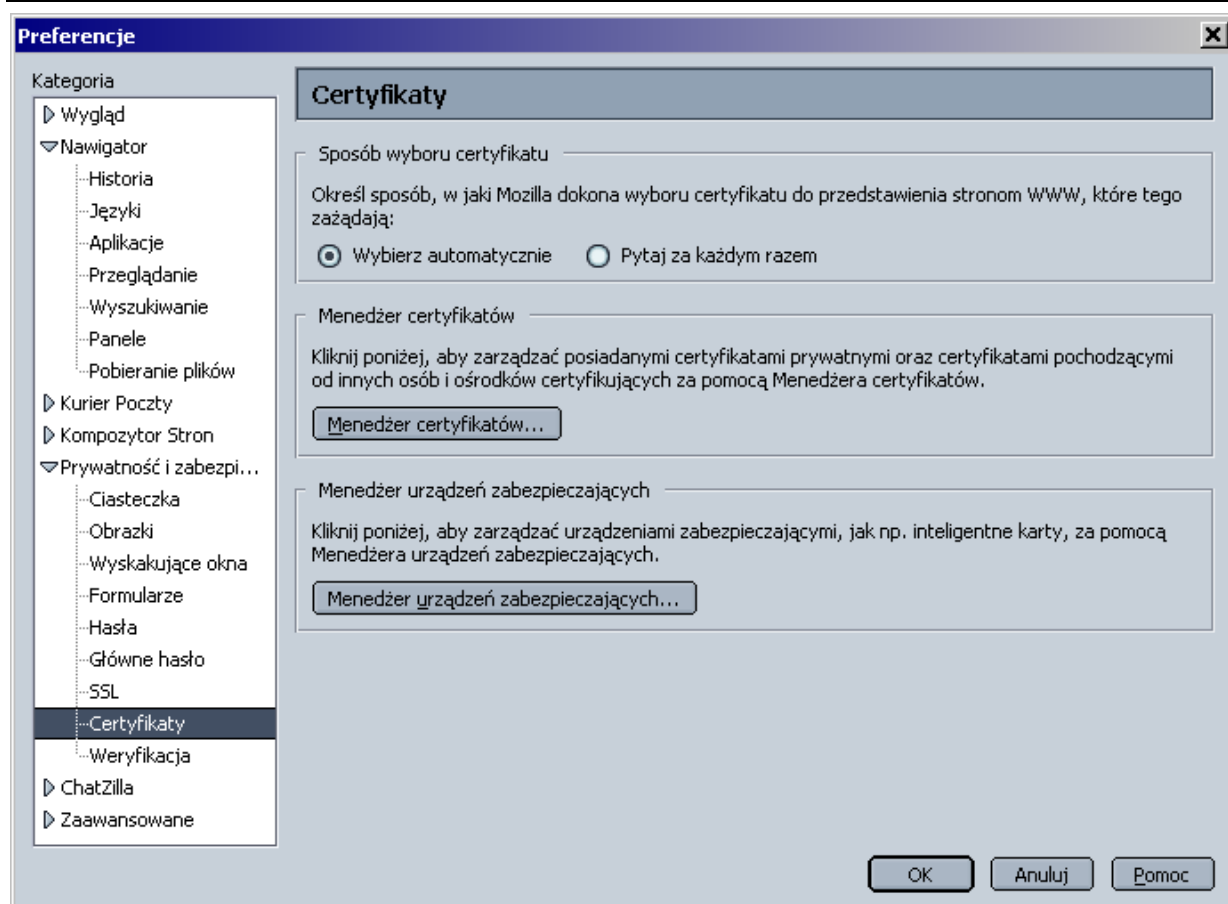
## Instalacja certyfikatów osobistych

Aby można było korzystać z własnych certyfikatów w programie **Mozilla 1.7 PL**, należy je zainstalować. Istnieją dwie możliwości w zależności od tego, jakiego certyfikatu chcemy użyć. Pierwszą możliwość zastosujemy, gdy otrzymaliśmy z centrum certyfikacji gotowy do użycia certyfikat na karcie mikroprocesorowej. Druga możliwość to wystawienie certyfikatu korzystając z serwisu <http://www.signet.pl/>.

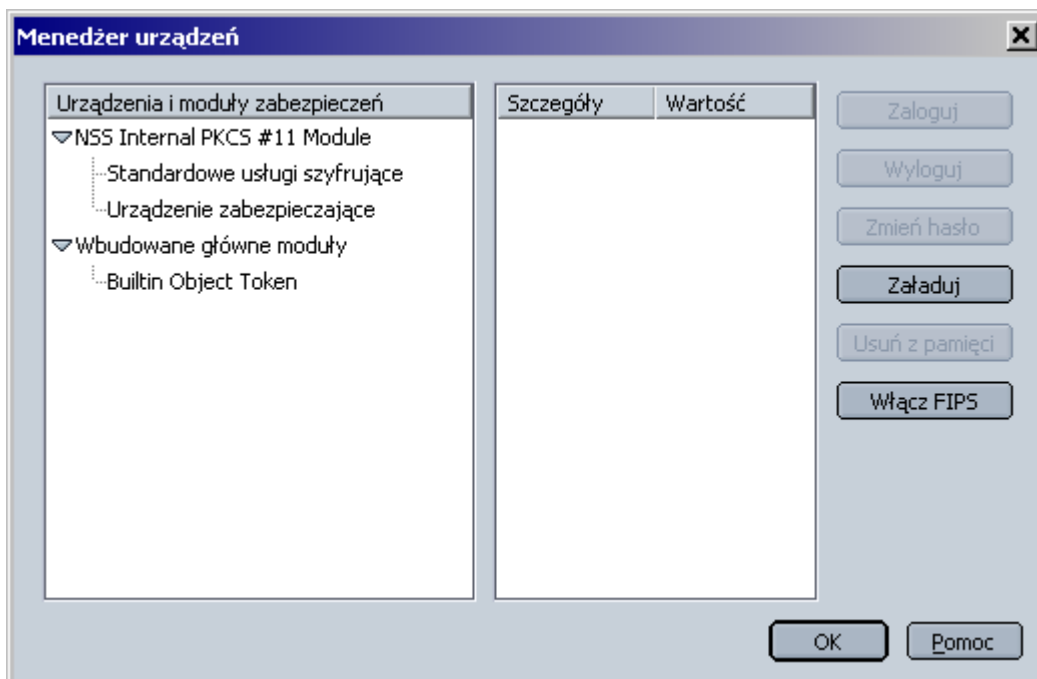
### *Instalacja z karty mikroprocesorowej*

Aby możliwe było korzystanie z karty mikroprocesorowej należy przede wszystkim zainstalować biblioteki do karty oraz sterownik do czytnika kart (oba programy dostarczane są dodatkowo na płycie CD wraz z kartą i czytnikiem). **Bez tego kroku korzystanie z karty jest niemożliwe.**

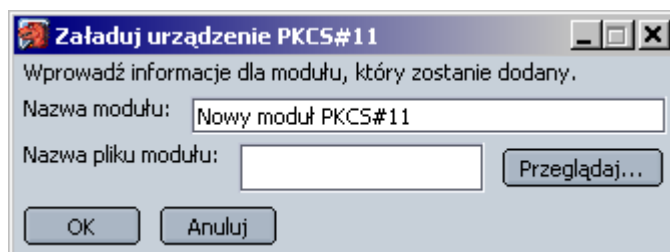
Po instalacji obu elementów, oraz ewentualnym restarcie systemu wymaganym przez niektóre programy, możemy przystąpić do konfiguracji obsługi karty mikroprocesorowej w programie **Mozilla 1.7 PL**. W tym celu uruchamiamy program i otwieramy okno **Edycja/Preferencje/Prywatność i zabezpieczenia**:



Z tego okna wybieramy przycisk **Menedżer urządzeń zabezpieczających**:



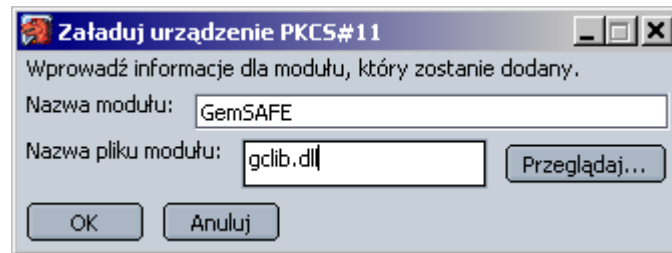
Aby dodać obsługę karty mikroprocesorowej wybieramy przycisk **Załaduj**.



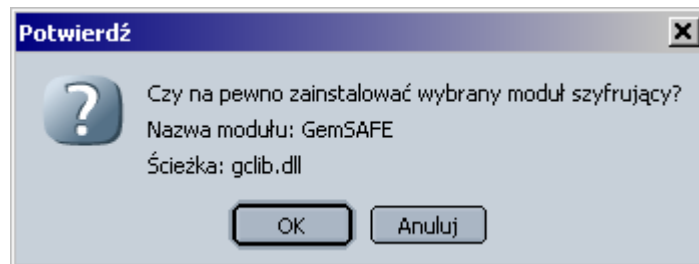
W pole **Nazwa modułu** należy wpisać dowolną (przyjazną dla użytkownika) nazwę określającą kartę. Może to być nazwa producenta karty itp. Natomiast w pole **Nazwa pliku modułu** należy wpisać nazwę biblioteki (zainstalowanej wcześniej) do obsługi danego typu kart. Oto przykładowe wartości tego pola dla poszczególnych producentów kart:

Producent	Nazwa biblioteki
Gemplus	gclib.dll
Siemens	CardOS_PKCS11.dll
Setec	C:\Program Files\SetWeb\settoki.dll
Cryptotech	CCPkiP11.dll

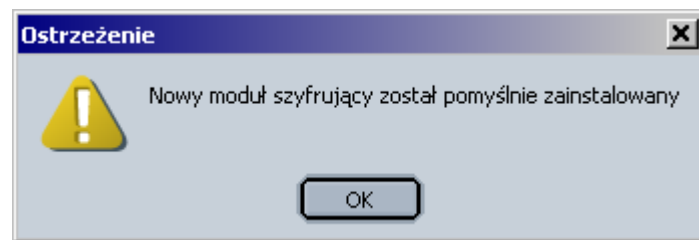
Oto przykładowo wypełnione okno dla kart Gemplus:



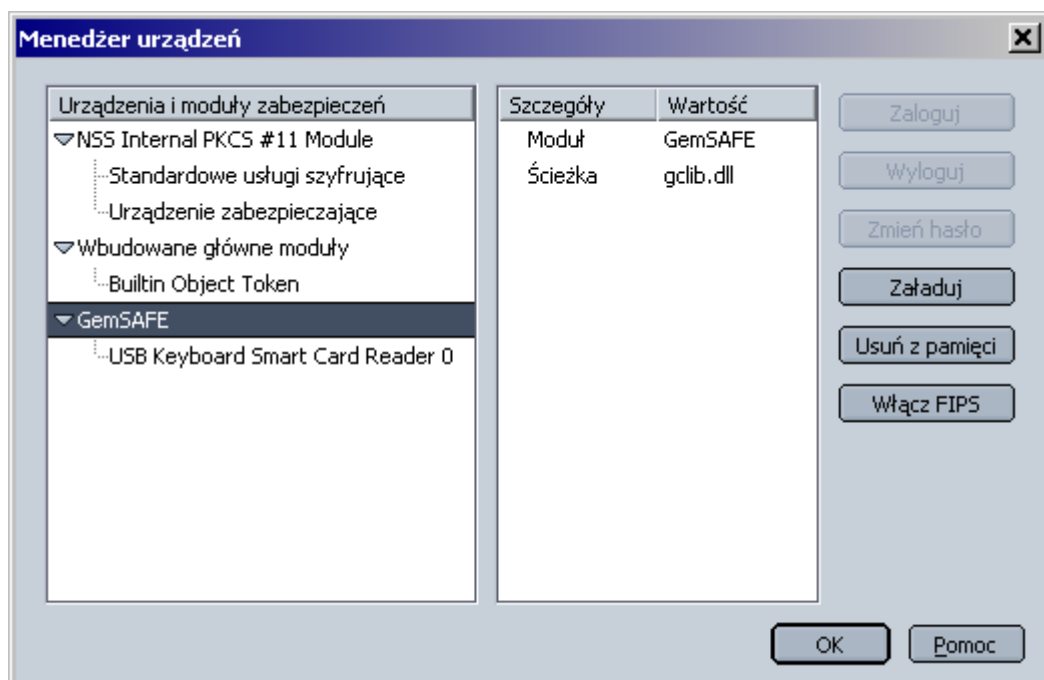
Następnie wybieramy przycisk **OK**. Pojawi się komunikat z pytaniem czy chcemy dodać moduł szyfrujący:



Wybieramy **OK** i otrzymujemy komunikat o pomyślnym dodaniu modułu:

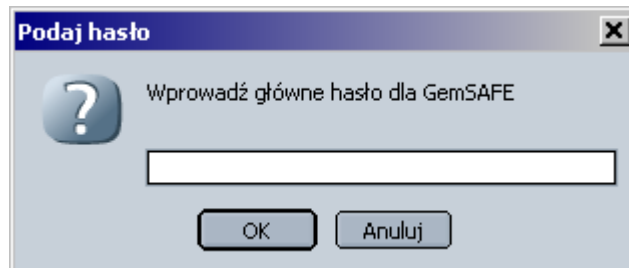


Zamykamy okno i ponownie je otwieramy. Powinien być widoczny nowy moduł:

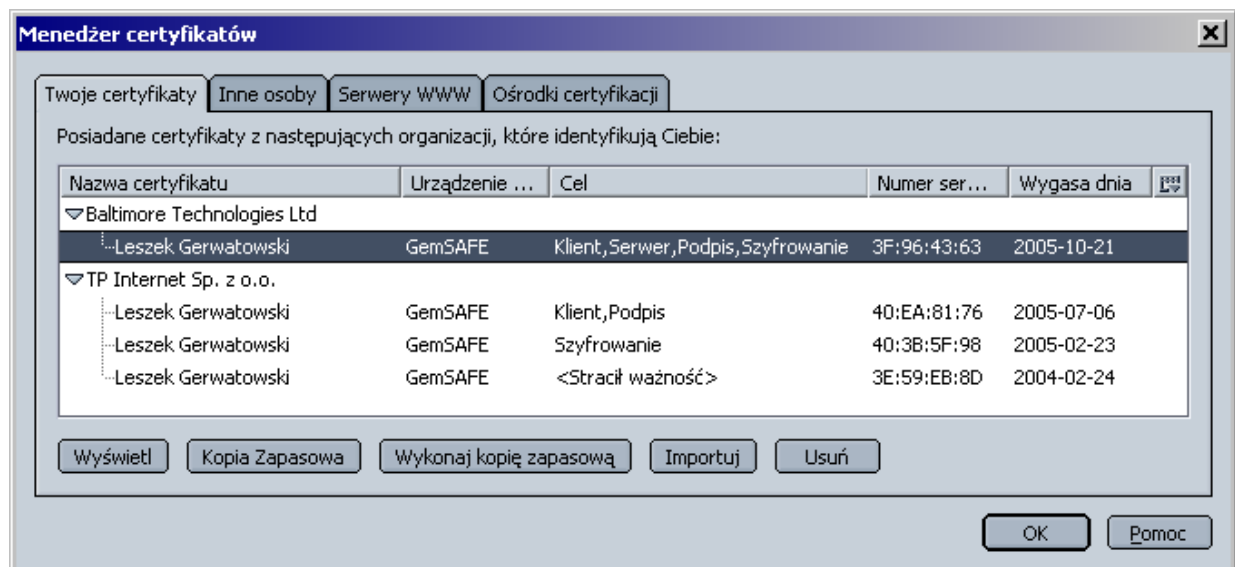


Jeśli wszystko jest widoczne, to możemy przejść do okna **Edycja/Preferencje/Prywatność i zabezpieczenia/Certyfikaty/Menedżer certyfikatów**

Przy otwieraniu tego okna, jeśli tylko jest włożona do czytnika karta, program **Mozilla 1.7 PL** powinien zapytać o **kod PIN** do zdefiniowanej karty:



Po podaniu kodu PIN otwiera się okno pokazujące certyfikaty osobiste zarówno plikowe, jak i znajdujące się na karcie:

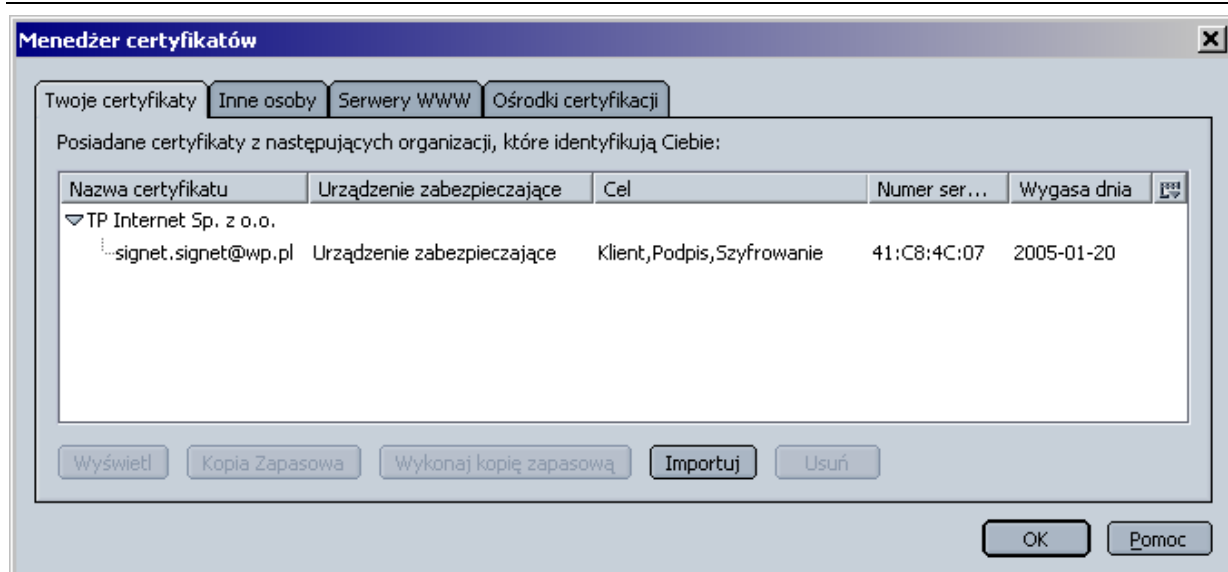


Wszystkie certyfikaty znajdujące się na karcie w kolumnie **Urządzenie zabezpieczające** będą miały wpisana nazwę karty.

Po takiej konfiguracji można w pełni korzystać w programie **Mozilla 1.7 PL** z certyfikatów znajdujących się na karcie - możliwe jest też uwierzytelnienie użytkownika na stronach WWW wymagających dokonania tej czynności za pomocą certyfikatu.

### **Instalacja ze strony [www.signet.pl](http://www.signet.pl)**

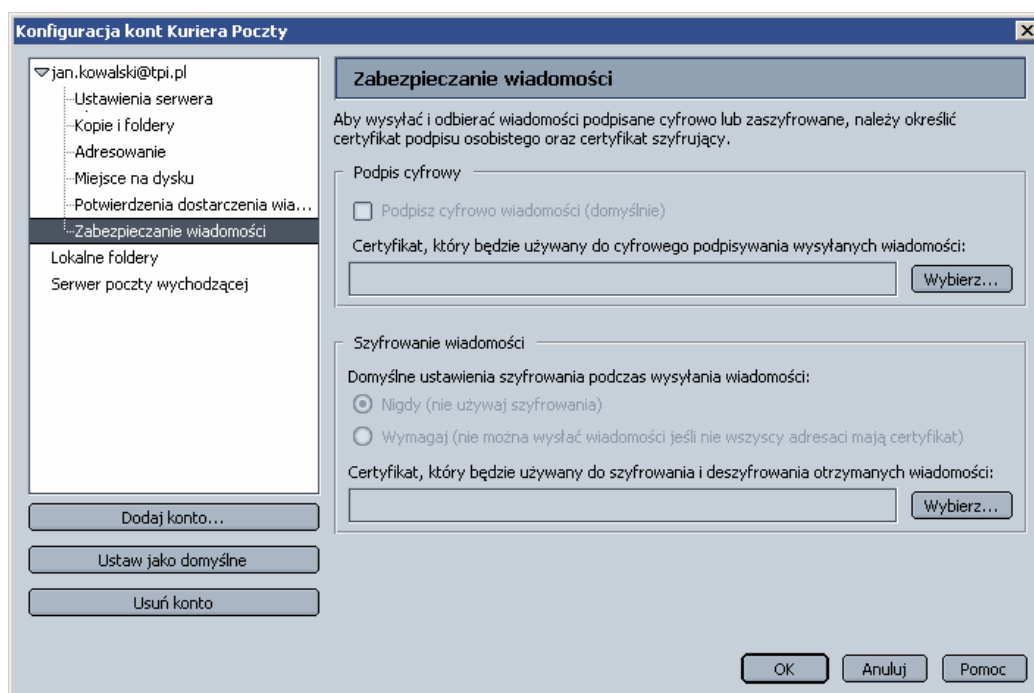
Aby uzyskać certyfikat ze strony [http://www.signet.pl/](http://www.signet.pl) należy po wejściu na stronę wybrać interesujący nas produkt, a następnie przejść całą wymaganą dla tego produktu procedurę certyfikacyjną, cały czas jako przeglądarki używając programu **Mozilla 1.7 PL**. Po przejściu całej procedury w oknie **Edycja/Preferencje/Prywatność i zabezpieczenia/Certyfikaty/Menedżer certyfikatów** w zakładce **Twoje certyfikaty** powinien być widoczny uzyskany certyfikat:

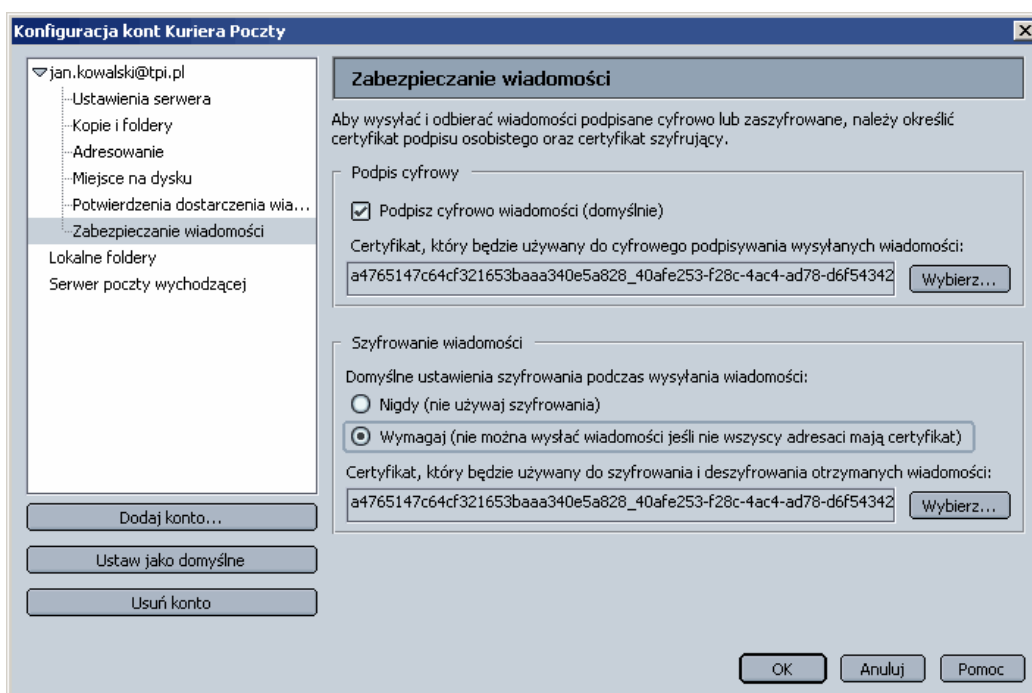
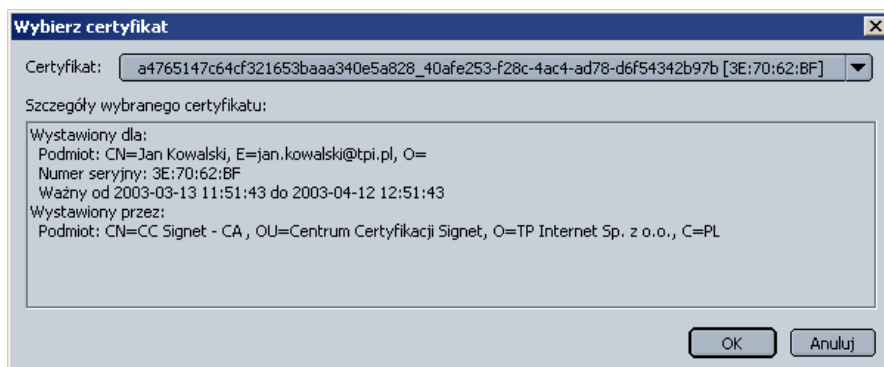


## Instalacja certyfikatu w programie pocztowym

Poniższy rozdział opisuje jak skonfigurować własny certyfikat w programie **Mozilla Kurier Poczty**. Zanim przystąpisz do konfiguracji programu **Mozilla Kurier Poczty** musisz mieć certyfikat własny wystawiony na skonfigurowane konto pocztowe.

Jeżeli masz więcej niż jeden certyfikat własny zainstalowany w **Mozilla 1.7 PL**, możesz wybrać oddzielnie certyfikat do podpisu i szyfrowania. W tym celu wybierz z menu **Edycja** pozycję **Konfiguracja kont Kuriera Poczty**, a następnie pozycję **Zabezpieczanie wiadomości**. Otwarte okno służy do konfiguracji ustawień związanych z zabezpieczeniem wiadomości pocztowych. W polu **Podpis cyfrowy** naciśnij **Wybierz** i wskaż z listy certyfikat, którego chcesz używać do podpisywania wiadomości. W polu **Szyfrowanie wiadomości** naciśnij **Wybierz** i wskaż z listy certyfikat, którego chcesz używać do szyfrowania i deszyfrowania otrzymanych wiadomości:





Jeżeli chcesz, aby Twoje wiadomości pocztowe były automatycznie podpisywane lub/i szyfrowane, możesz włączyć opcje **Podpisz cyfrowo wiadomości** lub/i **Wymagaj**.

## Instalacja certyfikatów innych osób

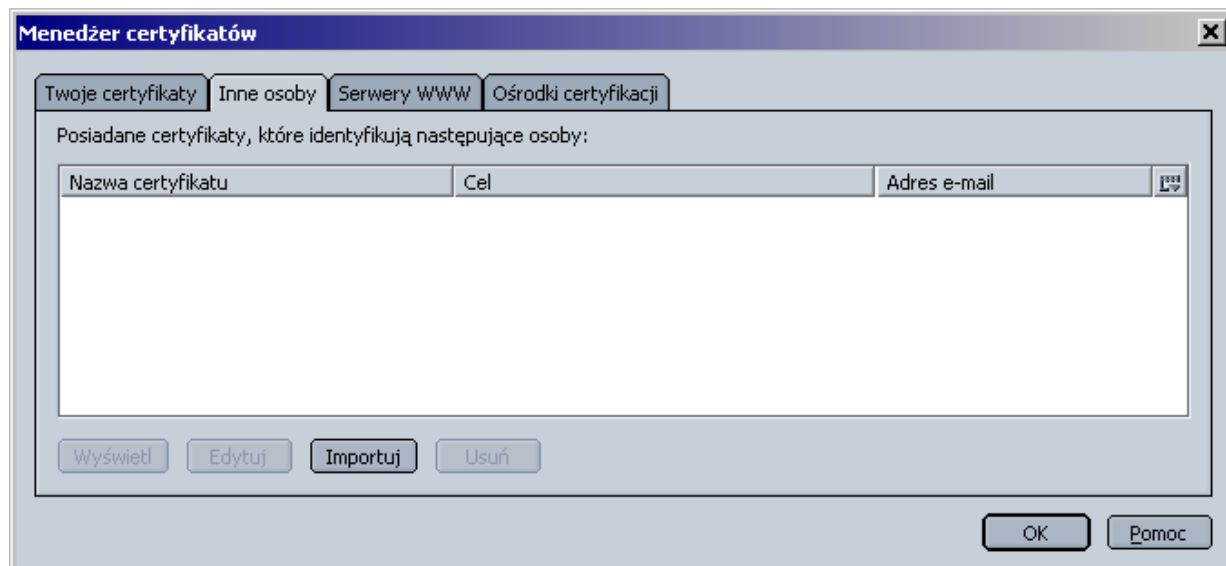
W programie **Mozilla 1.7 PL** możliwa jest również instalacja certyfikatów innych osób (znajomych, współpracowników). W celu przeprowadzenia instalacji certyfikatu innej osoby należy zdecydować się na jedną z dwóch możliwości - instalację certyfikatu z pliku (np. wyeksportowanego z programu pocztowego) bądź korzystając z wyszukiwarki certyfikatów dostępnej na stronie <http://www.signet.pl/>.

### *Import certyfikatów innych osób przez odebranie podpisanej wiadomości*

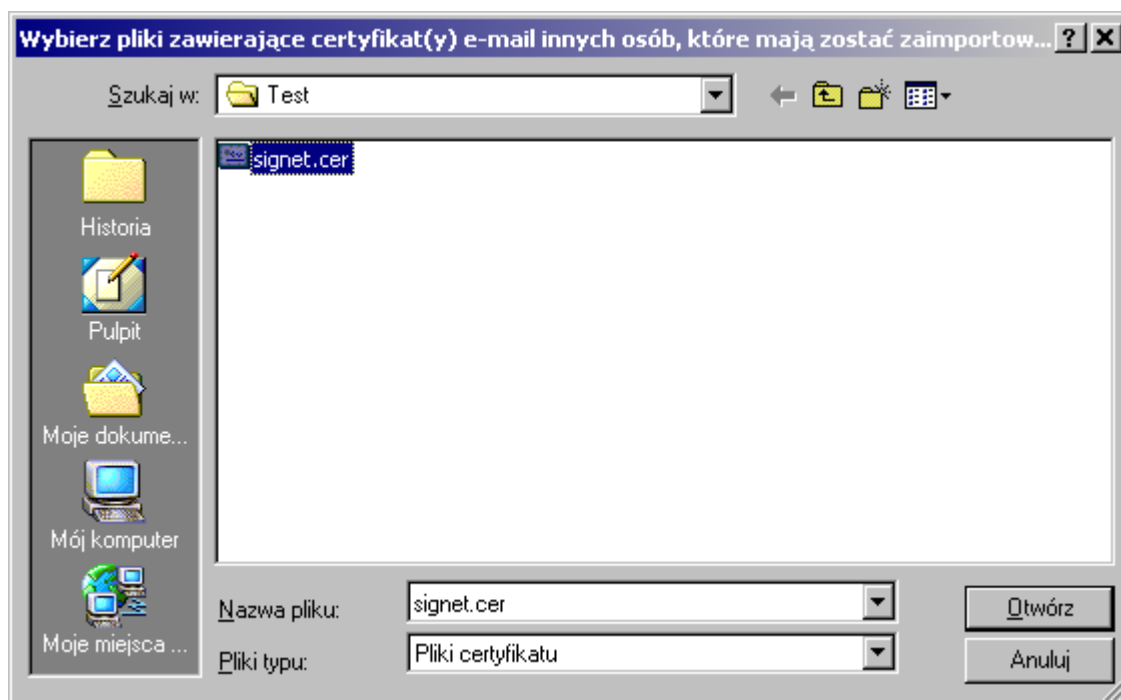
Najprostszym sposobem zaimportowania certyfikatu osoby, z którą chcesz korespondować używając zaszyfrowanej poczty, jest poproszenie jej o przysłanie podpisanej elektronicznie wiadomości. W chwili, gdy otrzymamy taką wiadomość, certyfikat nadawcy zostanie automatycznie dołączony do naszej książki adresowej.

## Import z pliku

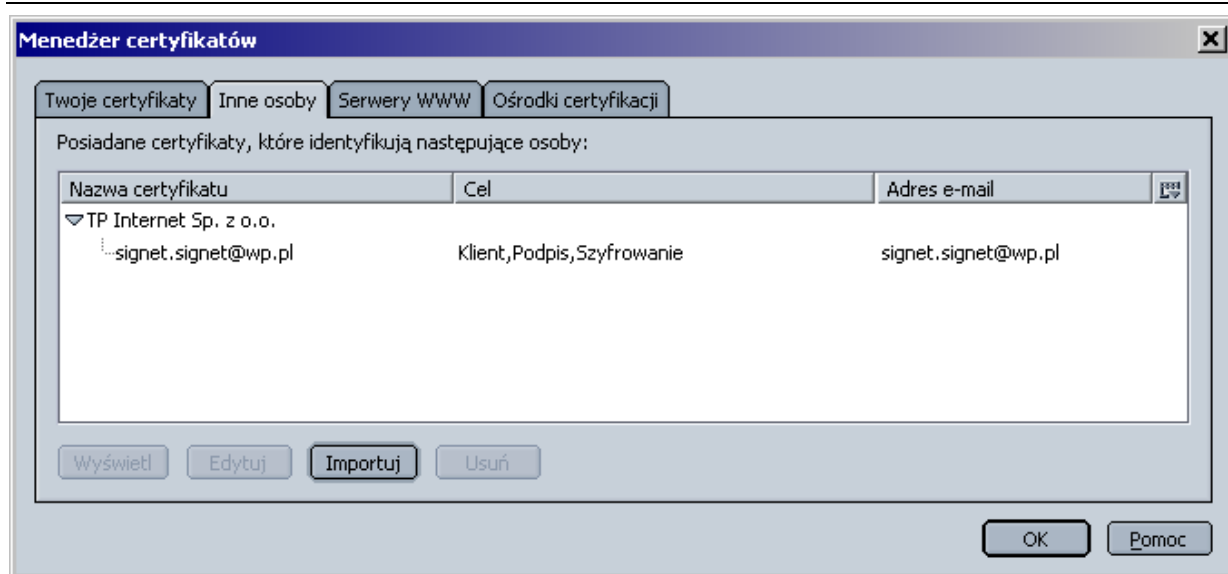
Aby zaimportować certyfikat z pliku należy otworzyć okno **Edycja/Preferencje/Prywatność i zabezpieczenia/Certyfikaty/Menedżer certyfikatów**:



Będąc w zakładce **Inne osoby** należy wybrać przycisk **Importuj**, a następnie wskazać certyfikat do importu:



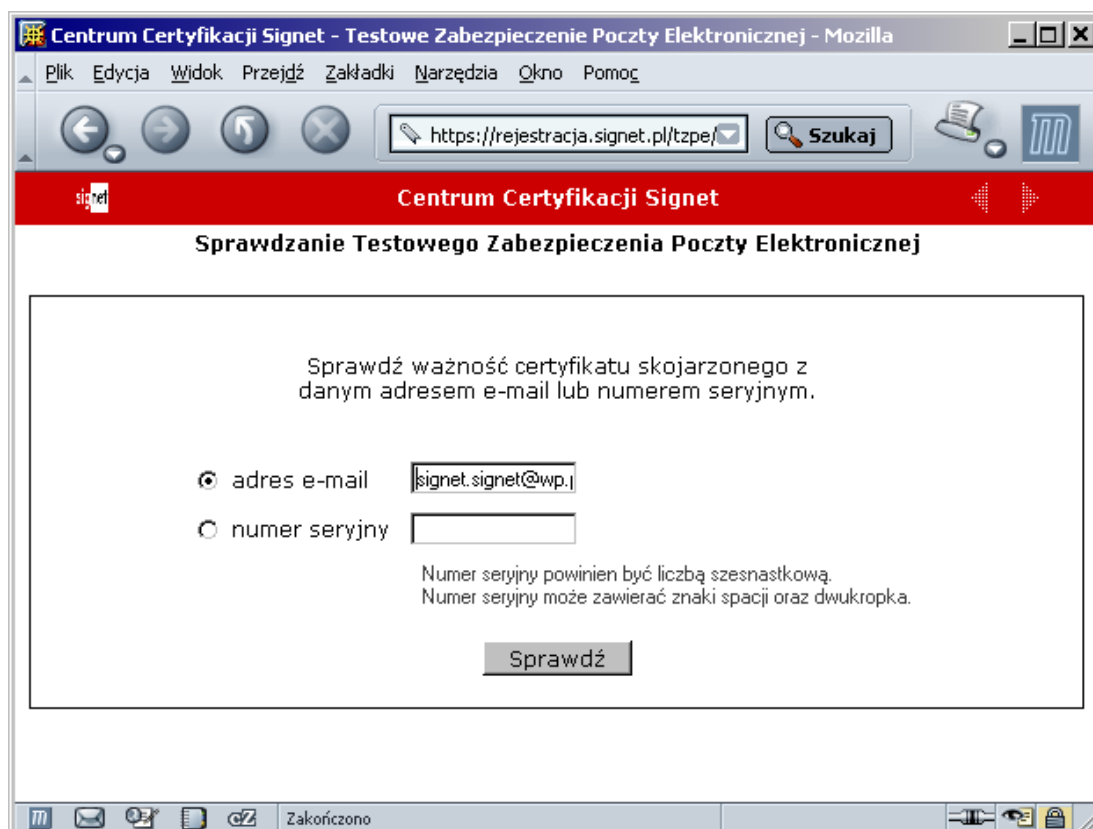
Po instalacji, certyfikat osoby pojawi się w zakładce **Inne osoby**:



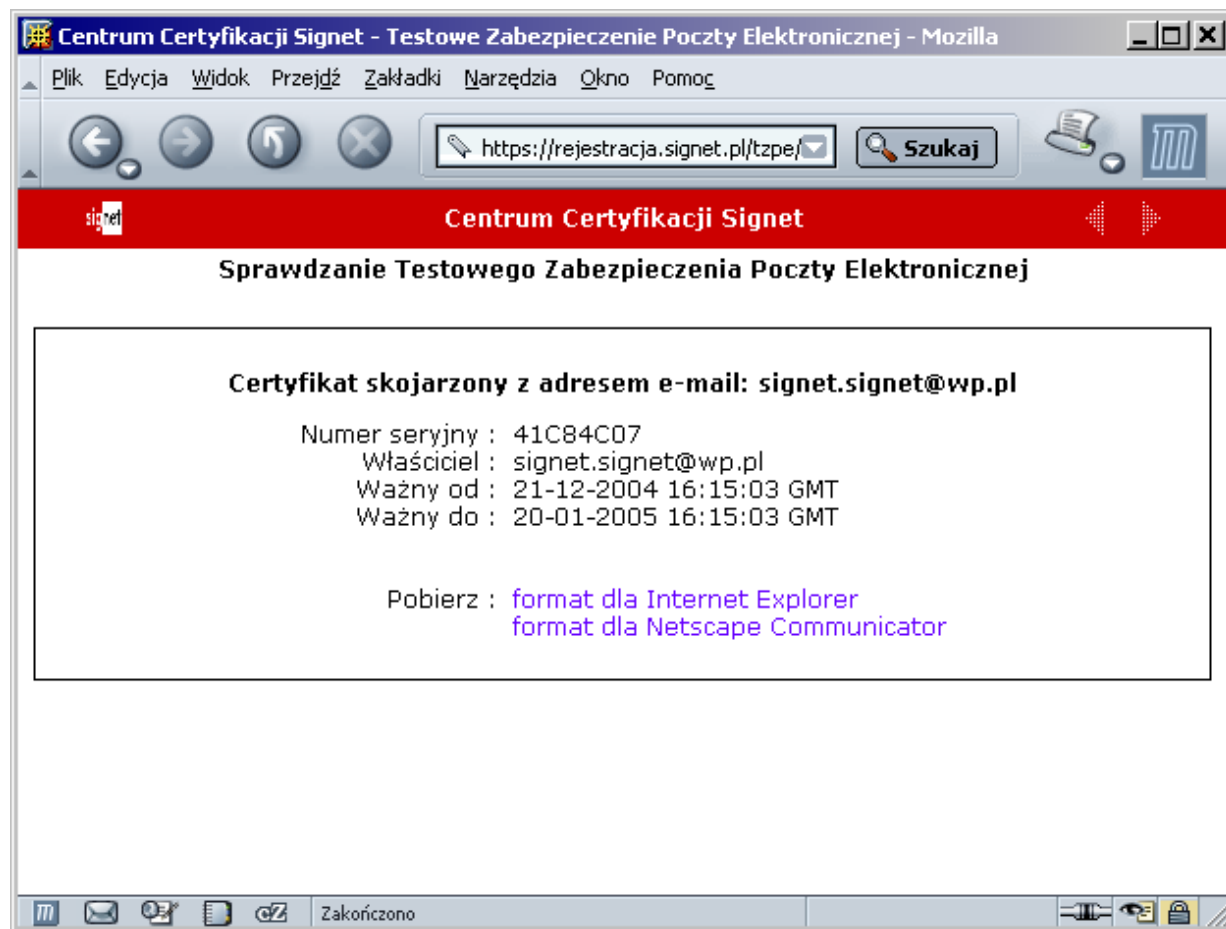
### Import ze strony [www.signet.pl](http://www.signet.pl)

Import certyfikatów innych osób za pośrednictwem serwisu [www.signet.pl](http://www.signet.pl) możliwy jest tylko wtedy, gdy osoba, z którą chcemy korespondować, ma certyfikat wystawiony przez Centrum Certyfikacji Signet.

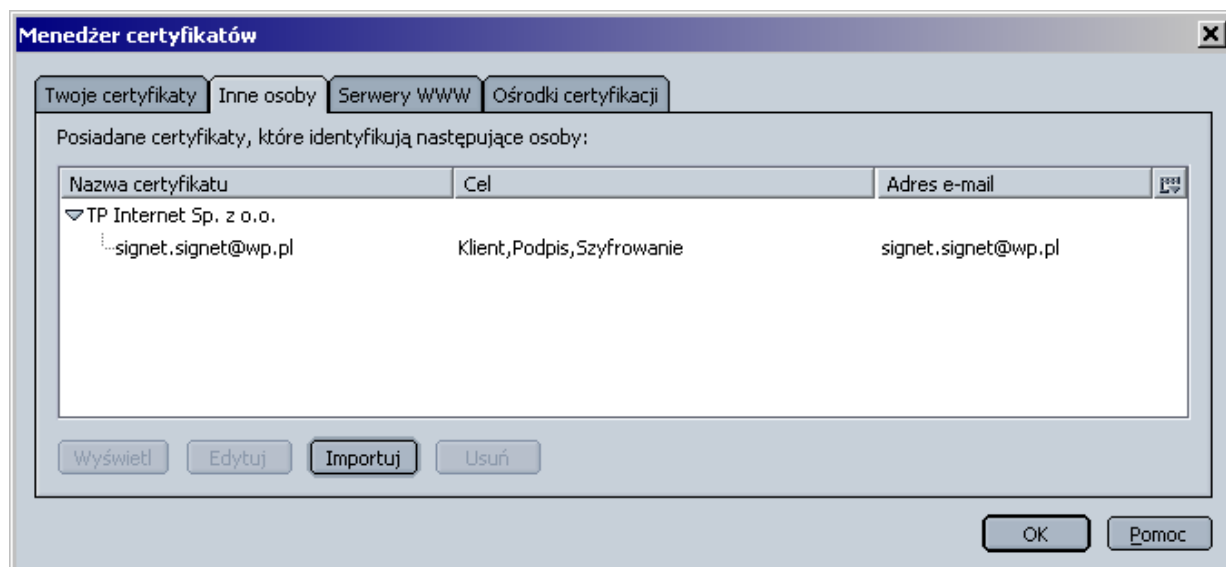
Aby zaimportować certyfikat innej osoby, musisz połączyć się z serwisem <http://www.signet.pl>. Z menu **Weryfikuj certyfikat** na stronie głównej wybierz pozycję odpowiadającą rodzajowi certyfikatu osoby, z którą chcesz korespondować. Na kolejnej stronie serwisu zostaniesz poproszony o podanie adresu e-mail. Wpisz adres e-mail osoby, której certyfikat zamierzasz importować i przyciśnij **Sprawdź**:



W sekcji **Pobierz** wybierz **format dla Netscape Communicator**.



Certyfikat zostanie automatycznie dołączony do bazy certyfikatów programu Mozilla. Można obejrzeć go otwierając okno **Edycja/Preferencje/Prywatność i zabezpieczenia/Certyfikaty/Menedżer certyfikatów** zakładka **Inne osoby**:



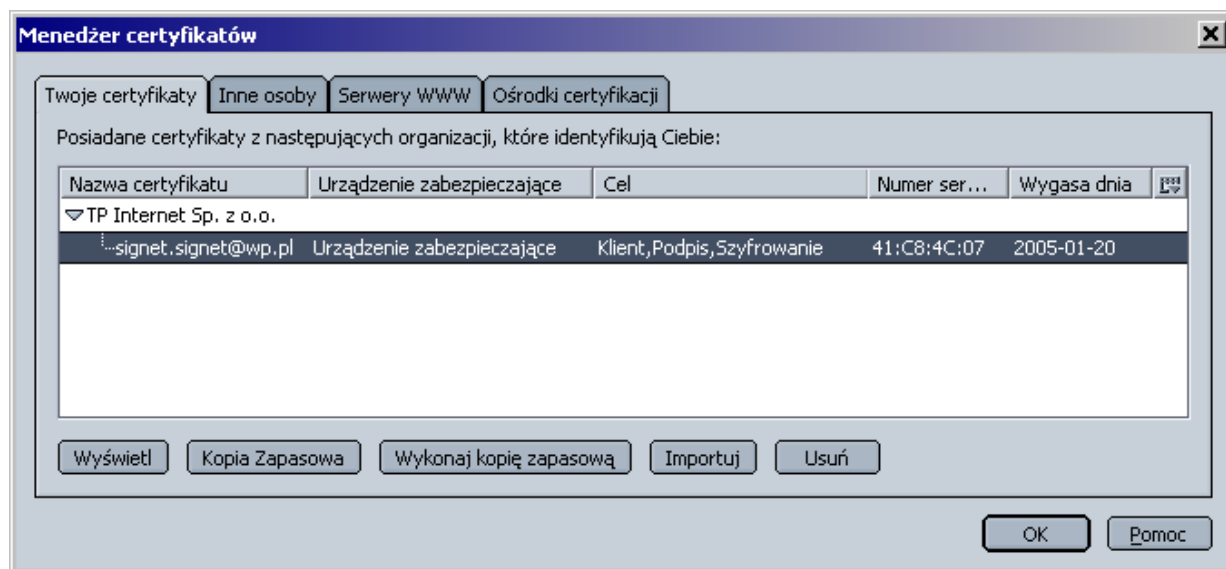
## Kopia zapasowa

W programie **Mozilla 1.7 PL** możliwe jest wykonanie kopii zapasowej certyfikatu wraz z kluczem prywatnym. Dzięki temu możliwe jest późniejsze odzyskanie certyfikatu np. po awarii komputera.

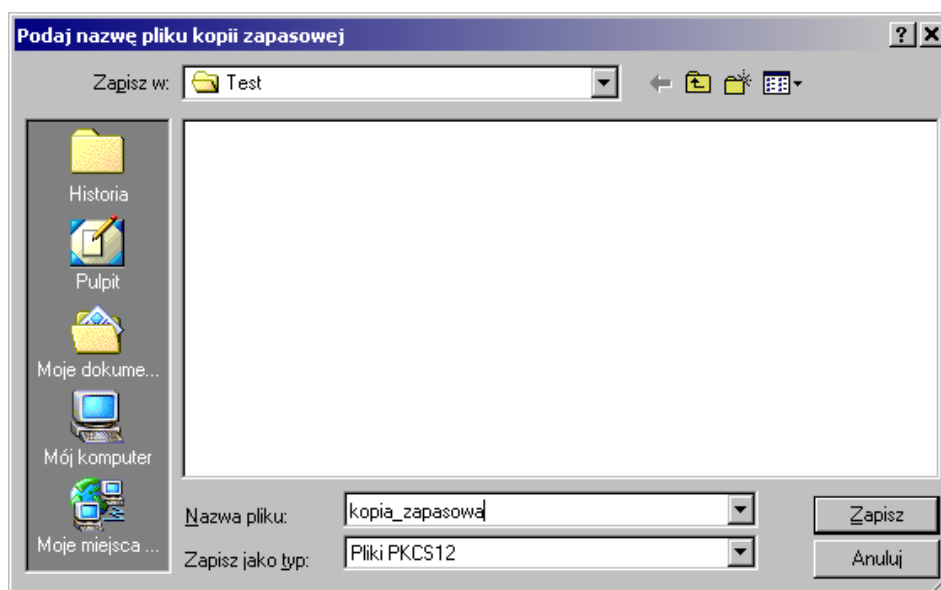
**UWAGA:** Wykonanie kopii zapasowej i późniejsze odzyskanie certyfikatu jest możliwe jedynie dla certyfikatów plikowych. **Nie jest to możliwe w przypadku certyfikatów na kartach mikroprocesorowych.**

### Eksport do pliku

Aby wykonać kopię zapasową certyfikatu i klucza prywatnego do pliku należy otworzyć okno **Edycja/Preferencje/ Prywatność i zabezpieczenia/ Certyfikaty/ Menedżer certyfikatów**. Po wybraniu zakładki **Moje certyfikaty** należy zaznaczyć certyfikat do eksportu i wybrać przycisk **Wykonaj kopię zapasową**:

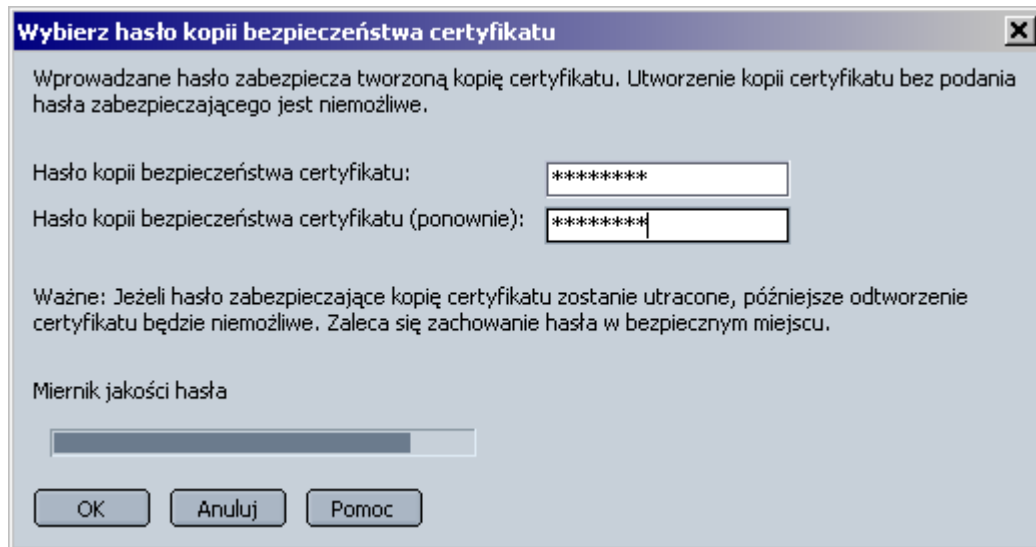


W kolejnym oknie należy wybrać katalog, w którym ma zostać zapisana kopia zapasowa oraz podać nazwę pliku dla kopii:

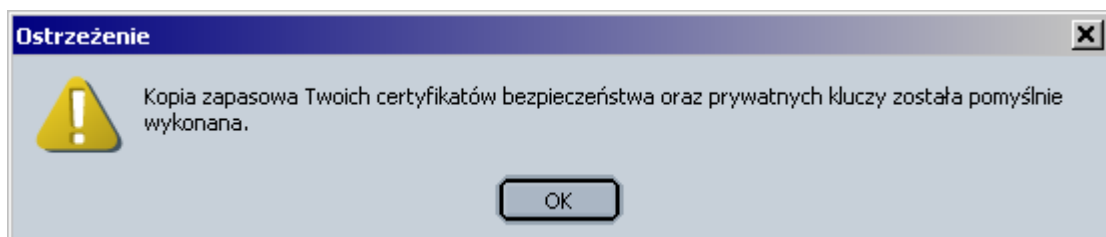


W kolejnym oknie należy podać hasło, którym chroniony będzie plik kopii zapasowej certyfikatu. Następnie należy wybrać przycisk **OK**.

**UWAGA:** Bez podania tego hasła odtworzenie kopii zapasowej będzie niemożliwe!



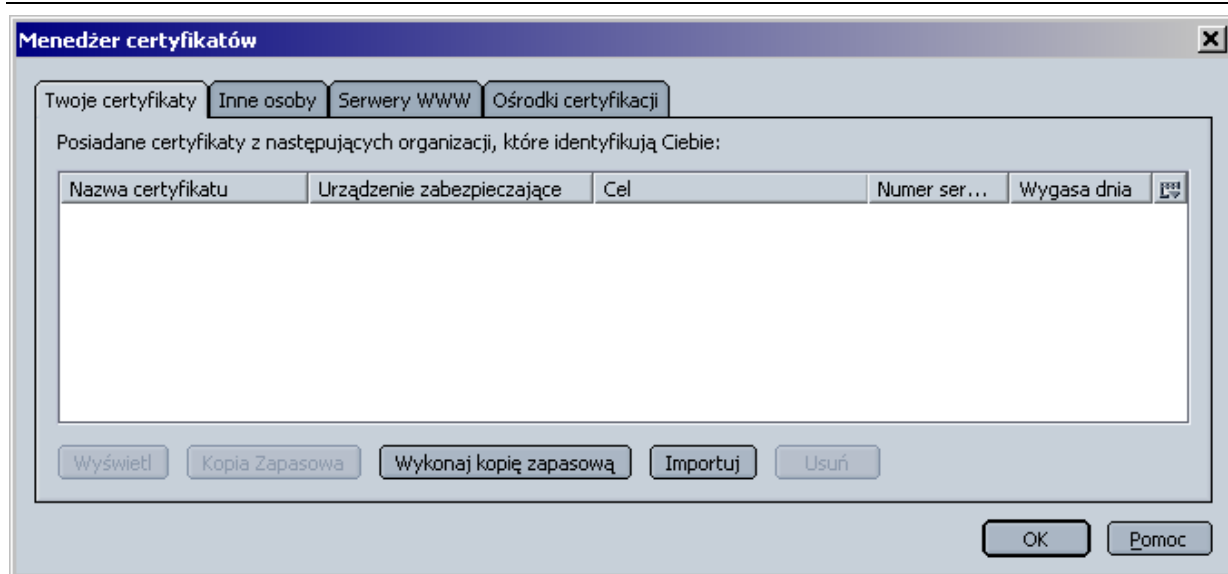
Po pomyślnym utworzeniu kopii zapasowej otrzymamy komunikat:



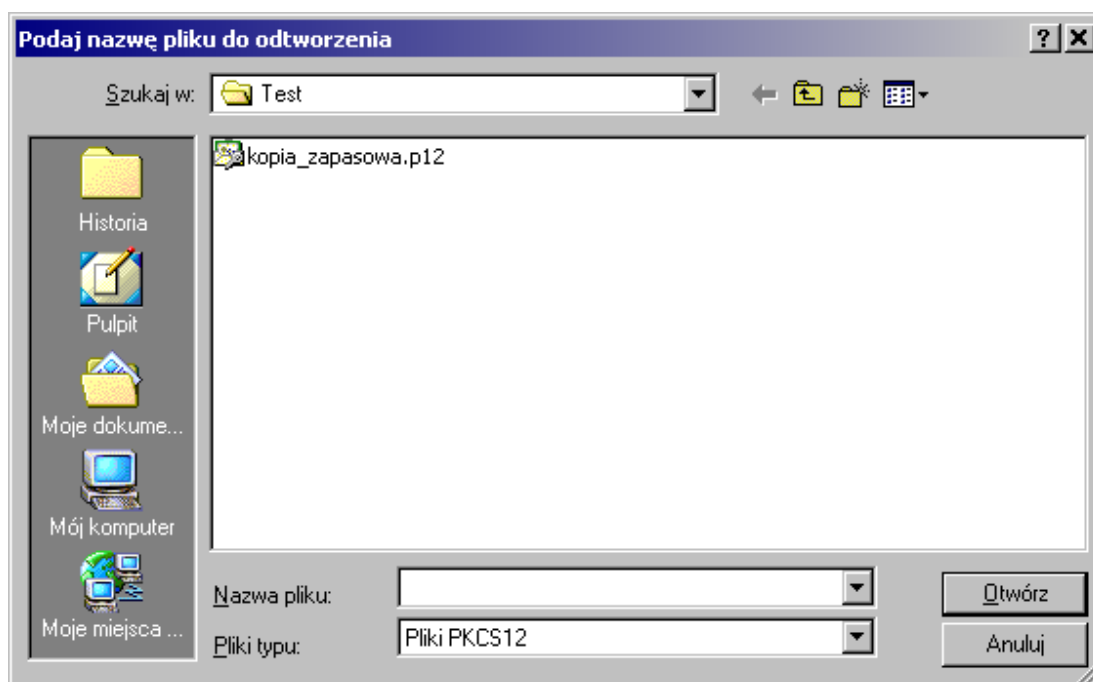
Tak sporządzoną kopię zapasową należy przechowywać w bezpiecznym miejscu (wraz z hasłem chroniącym plik), tak aby użycie jej bez naszej wiedzy było niemożliwe.

### **Import z pliku**

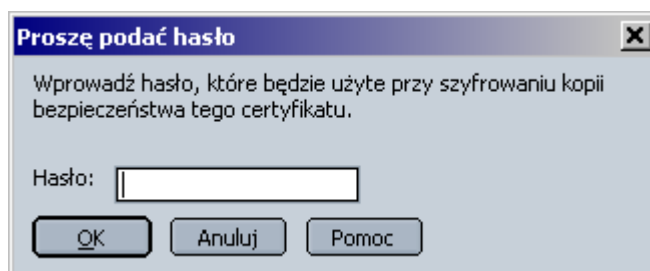
Aby zaimportować wcześniej utworzoną kopię zapasową certyfikatu oraz odpowiadającego mu klucza prywatnego należy otworzyć okno **Edycja/Preferencje/Prywatność i zabezpieczenia/Certyfikaty/Menedżer certyfikatów** a w nim zaznaczyć zakładkę **Moje certyfikaty**. Aby rozpocząć import certyfikatu wybieramy przycisk **Importuj**:



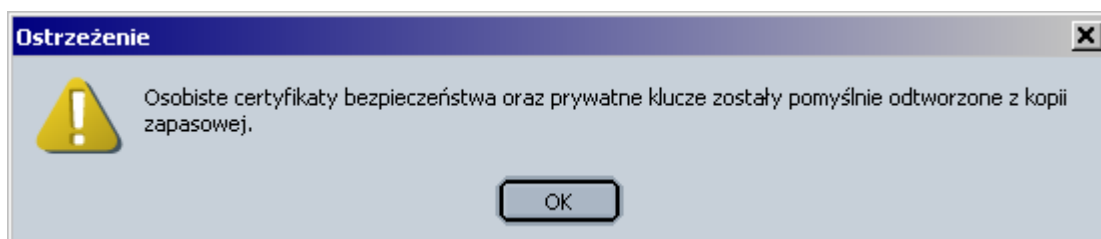
W kolejnym oknie wskazujemy katalog, w którym znajduje się plik kopii zapasowej oraz zaznaczamy ten plik:



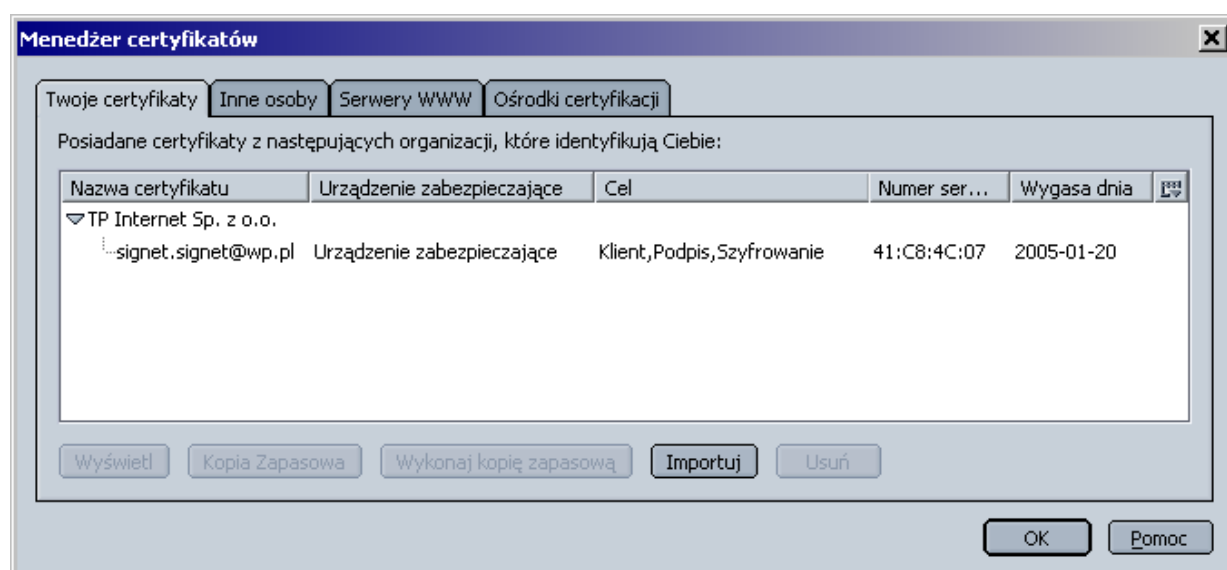
Następnie wprowadzamy hasło, którym zabezpieczony jest plik kopii zapasowej (trochę mylący jest komunikat w tym oknie - z powodu błędnego tłumaczenia, zamiast pytania o hasło, którym **był** zaszyfrowany plik mamy pytanie o hasło, którym **będzie** zaszyfrowany plik):



Po podaniu hasła następuje import certyfikatu oraz klucza prywatnego. O pomyślnym zakończeniu importu program informuje nas odpowiednim komunikatem:



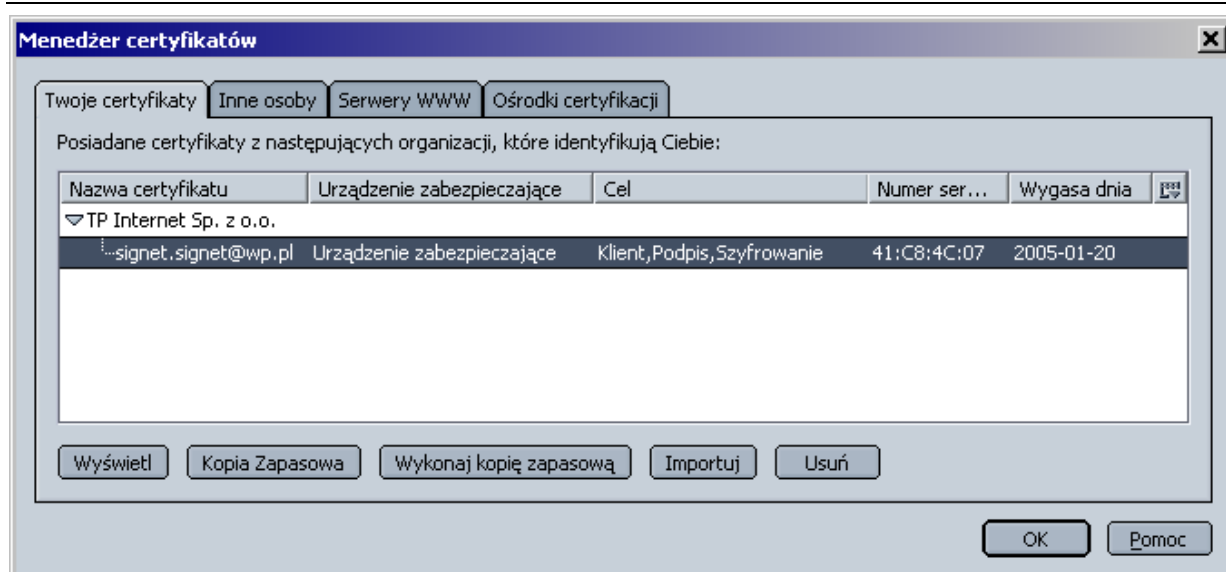
Po dokonaniu importu osobisty certyfikat użytkownika pojawia się w zakładce **Moje certyfikaty**:



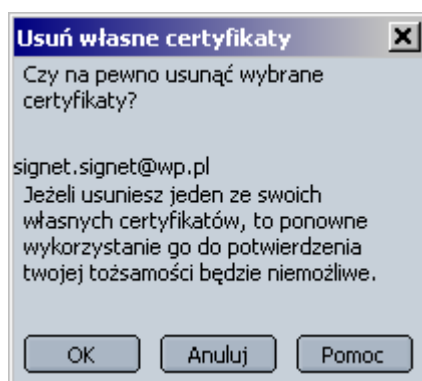
W ten sposób przywróciliśmy wcześniej wykonaną kopię zapasową certyfikatu oraz odpowiadającego mu klucza prywatnego. Po wykonaniu wyżej opisanych kroków certyfikat jest gotowy do dalszego użycia w programie **Mozilla 1.7 PL**.

## Usuwanie certyfikatów

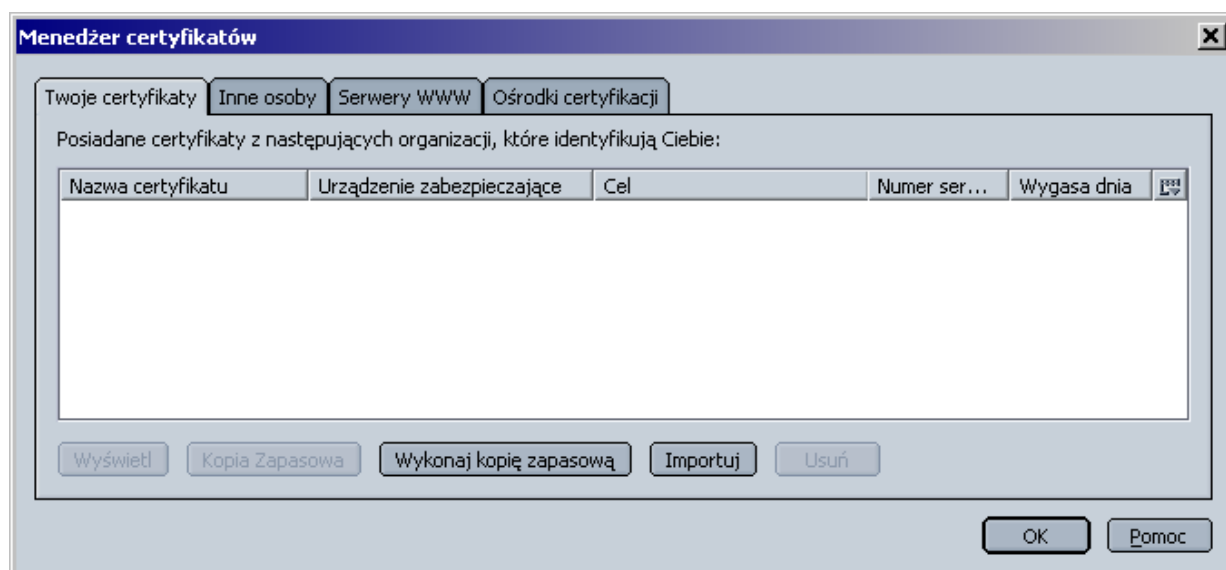
W celu usunięcia certyfikatu należy otworzyć okno **Edycja/Preferencje/Prywatność i zabezpieczenia/Certyfikaty/Menedżer certyfikatów**. Następnie należy wybrać zakładkę, w której znajduje się certyfikat do skasowania (np. Twoje certyfikaty):



Należy zaznaczyć certyfikat do usunięcia, a następnie wybrać przycisk **Usuń**. Pojawi się okno z pytaniem o potwierdzenie chęci usunięcia certyfikatu:



Po usunięciu certyfikatu nie jest on już widoczny w zakładce **Twoje certyfikaty**:



Aby usunąć certyfikat innej osoby, wybierz opcję **Inne osoby**, zaznacz certyfikat przeznaczony do usunięcia i naciśnij **Usuń**.

Chcąc usunąć certyfikat urzędu, wybierz opcję **Ośrodki certyfikacji**, zaznacz certyfikat urzędu certyfikacji CA, a następnie przyciśnij **Usuń**. Po usunięciu tego certyfikatu, żaden certyfikat wystawiony przez ten urząd nie będzie mógł zostać użyty w programie do obsługi poczty do podpisania lub szyfrowania wiadomości, ponieważ zostanie on zweryfikowany jako certyfikat niewiarygodny.

## Podpisywanie i szyfrowanie wiadomości

Certyfikaty Centrum Certyfikacji Sigmet mogą służyć do podpisywania poczty elektronicznej, jak również do szyfrowania wysyłanych wiadomości. Możliwość skorzystania z jednej z powyższych opcji zależy jest od wersji wygenerowanego dla Ciebie certyfikatu.

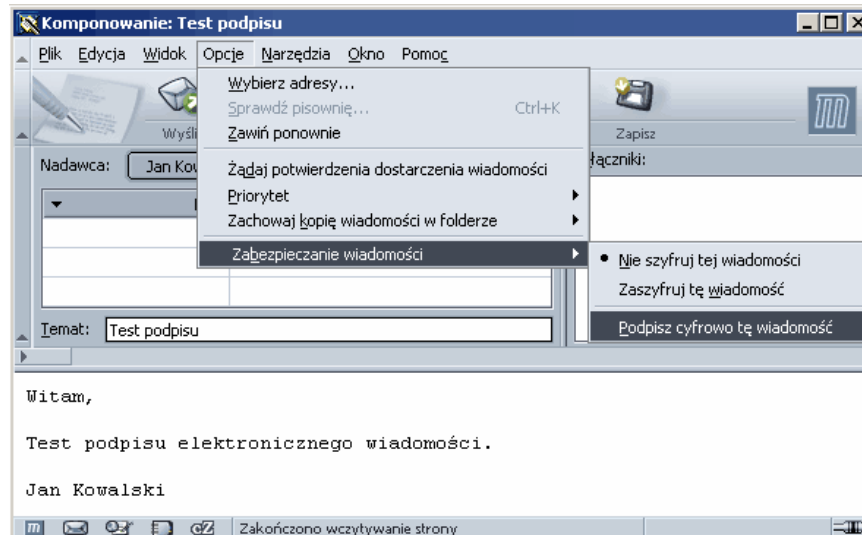
Podpisanie wiadomości powoduje, że wysłana wiadomość zostanie podpisana z wykorzystaniem Twojego klucza prywatnego oraz dołączonym certyfikatem wystawionym Tobie przez Centrum Certyfikacji Sigmet. Uzyskany w ten sposób podpis elektroniczny stanowi gwarancję, że użytkownik, który wysłał daną wiadomość jest tą osobą, za którą się podaje (uwierzytelnienie osoby wysyłającej daną wiadomość). Gwarantuje on również niezaprzeczalność i integralność przesyłanej informacji (odbiorca podpisanej wiadomości jest w stanie stwierdzić, czy wiadomość w trakcie przesyłania nie uległa modyfikacji).

Szyfrowanie wiadomości oznacza zaszyfrowanie danej wiadomości z wykorzystaniem klucza publicznego odbiorcy, do którego wiadomość ta jest kierowana. Tak chroniona wiadomość może zostać odczytana wyłącznie przez adresata. Tylko on, jako posiadacz drugiego klucza z pary (klucza prywatnego), może taką wiadomość odszyfrować i ją odczytać. Dzięki szyfrowaniu zapewniamy poufność przysyłanych pocztą elektroniczną informacji.

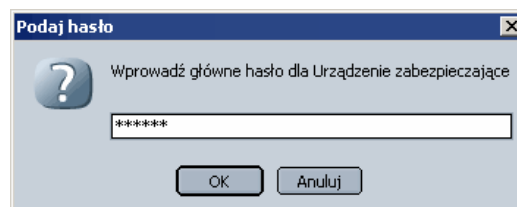
Trzecią z możliwości ochrony wysyłanej poczty elektronicznej jest zastosowanie obu powyższych metod jednocześnie. Wiadomość zostanie podpisana oraz zaszyfrowana, zapewniając tym samym pełną ochronę korespondencji użytkownika.

### *Wysyłanie wiadomości z podpisem cyfrowym*

Wysłanie wiadomości podpisanej elektronicznie jest możliwe jedynie wtedy, gdy w bazie certyfikatów programu **Mozilla 1.7 PL** znajduje się zaimportowany certyfikat własny (patrz **Instalacja certyfikatów własnych**). Jeżeli masz już przygotowaną do wysłania wiadomość pocztową (menu **Okno**, opcja **Kurier Poczty**, ikona **Nowa wiadomość**), w celu podpisania jej elektronicznie wybierz w oknie wiadomości z menu **Opcje**, a następnie **Zabezpieczenie wiadomości** (lub ikonę **Zabezpieczenia** z paska menu). Pojawi się następujące okno, w którym zaznacz opcję **Podpisz cyfrowo tę wiadomość**:



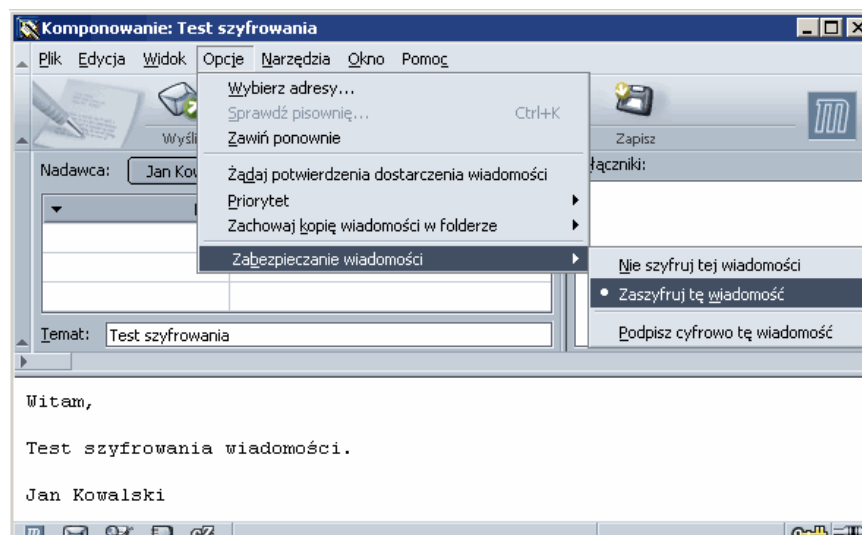
Wprowadź hasło:



Wyślij wiadomość przyciskiem **Wyślij**.

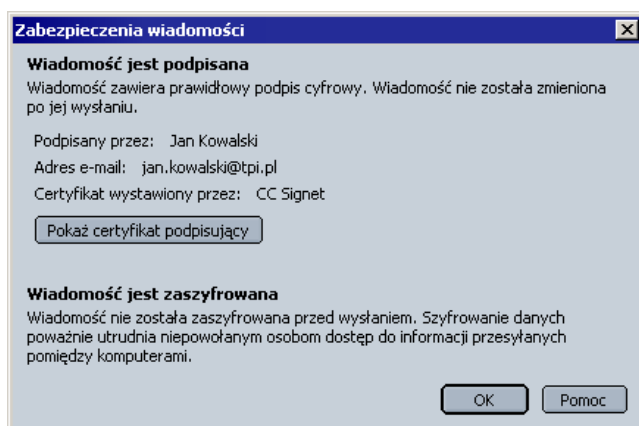
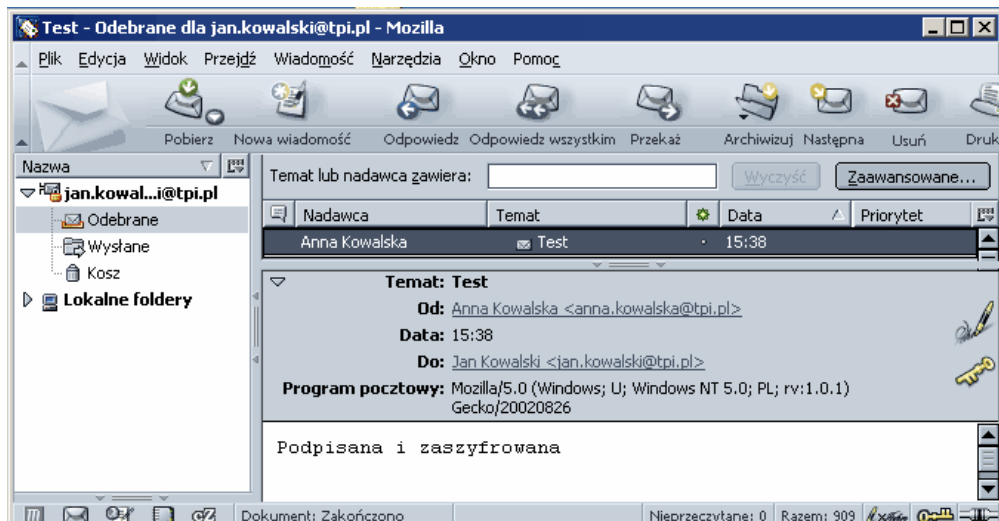
### ***Szyfrowanie wysłanych wiadomości***

Wysłanie wiadomości zaszyfrowanej wymaga pobrania i zaimportowania do bazy certyfikatów programu **Mozilla** certyfikatu osoby, do której chcesz wysłać zaszyfrowaną wiadomość (konfiguracja certyfikatów innych osób). Jeżeli masz już przygotowaną do wysłania wiadomość pocztową (menu **Okno**, opcja **Kurier Poczty**, ikona **Nowa wiadomość**), w celu zaszyfrowania jej, wybierz w oknie wiadomości z menu **Opcje**, a następnie **Zabezpieczanie wiadomości** (lub ikonę **Zabezpieczenia** z paska menu). Pojawi się następujące okno, w którym zaznacz opcję **Zaszyfruj tę wiadomość**:




## Odbieranie wiadomości szyfrowanych i podpisanych elektronicznie

Odebrane wiadomości pocztowe podpisane elektronicznie lub szyfrowane opatrzone są w specjalne ikony **Podpisana** lub **Zaszyfrowana**, informujące w jaki sposób nadawca zabezpieczył wiadomość:



Aby zweryfikować podpis elektroniczny dołączony do wiadomości, musisz mieć zaimportowany certyfikat nadawcy. W celu odszyfrowania wiadomości wykorzystywany jest Twój klucz prywatny dołączony do bazy certyfikatów **Mozilli 1.7 PL** (certyfikat własny).

Jeżeli operacja weryfikacji podpisu cyfrowego lub odszyfrowania nie powiedzie się, wiadomość zostanie opatrzona odpowiednią ikoną, np. , a jej treść nie będzie widoczna.