

## Instrukcja obsługi certyfikatów w programie pocztowym Netscape Communicator 4.x

Spis treści	
Wstęp .....	1
Instalacja certyfikatu w programie pocztowym .....	1
Instalacja certyfikatów własnych.....	1
Instalacja certyfikatów innych osób.....	2
Import certyfikatów innych osób przez odebranie podpisanej wiadomości .....	2
Import certyfikatów innych osób za pośrednictwem serwisu <a href="http://www.signet.pl">www.signet.pl</a> .....	2
Usuwanie certyfikatów .....	3
Podpisywanie i szyfrowanie wiadomości .....	4
Wysyłanie wiadomości z podpisem cyfrowym.....	4
Szyfrowanie wysyłanych wiadomości .....	5
Odbieranie wiadomości szyfrowanych i podpisanych elektronicznie.....	6

## Wstęp

Jest to dokument, który pokaże Ci, jak poprawnie skonfigurować program pocztowy **Netscape Messenger** w przeglądarce **Netscape Communicator**, abyś mógł korzystać z certyfikatów wystawionych przez Centrum Certyfikacji Signet.

## Instalacja certyfikatu w programie pocztowym

Poniższy rozdział opisuje, jak skonfigurować własny certyfikat w programie **Netscape Messenger** oraz jak pobrać i zainstalować certyfikaty innych użytkowników.

Zanim przystąpisz do konfiguracji programu **Netscape Messenger** musisz mieć certyfikat własny.

### Instalacja certyfikatów własnych

Aby skonfigurować własny certyfikat w programie **Netscape Messenger**, wybierz ikonę **Security** (lub z menu opcję **Communicator**, następnie **Tools** i **Security Info**), a następnie pozycję **Messenger**. Otwarte okno służy do konfiguracji ustawień związanych z wysyłaniem wiadomości pocztowych. W polu **Certificate for your Signed and Encrypted Messages** wybierz z listy certyfikat, którego chcesz używać. Jeżeli masz więcej niż jeden certyfikat własny zainstalowany w **Netscape Communicator**, możesz zaznaczyć jeden z nich jako certyfikat domyślny.



Jeżeli chcesz, aby Twoje wiadomości pocztowe były automatycznie podpisywane lub szyfrowane, włącz opcje z sekcji **Sending Signed/Encrypted Mail**.

## Instalacja certyfikatów innych osób

Certyfikaty innych użytkowników są niezbędne do szyfrowania wysyłanych do nich wiadomości pocztowych. Powinieneś pobrać certyfikaty wszystkich osób, z którymi chcesz wymieniać zaszyfrowaną pocztę. Certyfikaty innych użytkowników (zawierające klucz publiczny) można importować na różne sposoby, w zależności od tego, jak zostały one udostępnione:

- przez odebranie wiadomości podpisanej cyfrowo przez właściciela certyfikatu,
- z wykorzystaniem serwera LDAP,
- za pośrednictwem serwisu [www.signet.pl](http://www.signet.pl).

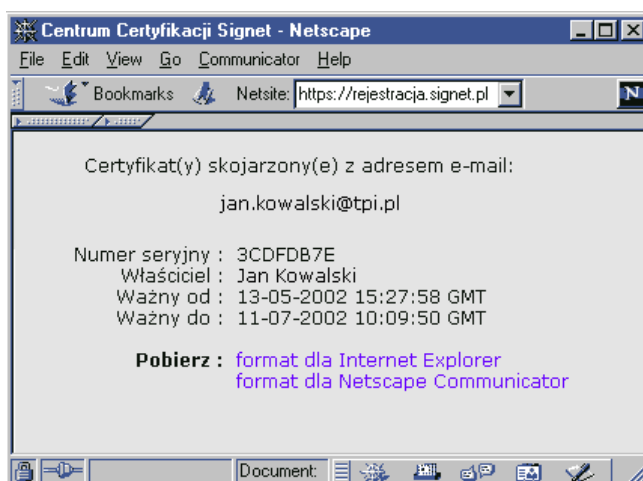
### Import certyfikatów innych osób przez odebranie podpisanej wiadomości

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

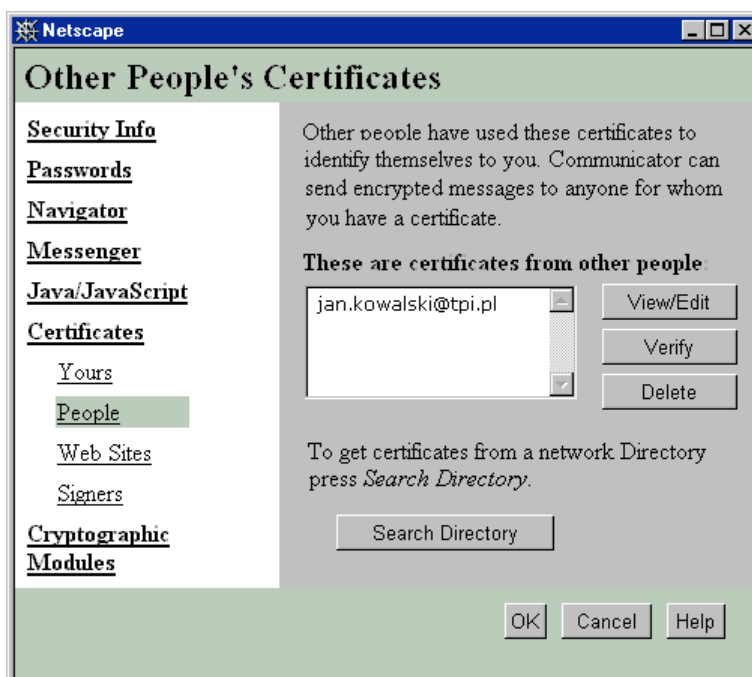
### Import certyfikatów innych osób za pośrednictwem serwisu [www.signet.pl](http://www.signet.pl)

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 Signet.

Aby zaimportować certyfikat innej osoby, musisz połączyć się z serwisem [www.signet.pl](http://www.signet.pl). Z menu weryfikuj na stronie głównej wybierz rodzaj certyfikatu, który ma ta osoba. Na kolejnej stronie serwisu zostaniesz poproszony o podanie jej adresu poczty elektronicznej. Wpisz adres e-mail osoby, której certyfikat zamierzasz importować i przyciśnij Sprawdz.



W sekcji **Pobierz** wybierz **format dla Netscape Communicator**. W otwartym oknie dialogowym wyświetlona zostanie informacja o imporcie certyfikatu. Certyfikat zostanie dołączony do bazy certyfikatów programu Netscape Communicator. Możesz obejrzeć go wybierając opcję **Communicator**, następnie **Tools** i **Security Info**, dalej zakładkę **Certificates** i opcję **People**.



## Usuwanie certyfikatów

W celu usunięcia certyfikatu, wybierz z menu opcję **Communicator**, następnie opcję **Tools**, dalej **Security Info** oraz zakładkę **Certificates**. Jeżeli chcesz usunąć certyfikat własny, wybierz opcję **Yours**, zaznacz własny certyfikat i przyciśnij **Delete**. Aby usunąć certyfikat innej osoby, wybierz opcję **People**, zaznacz certyfikat przeznaczony do usunięcia i kliknij przycisk **Delete**. Chcąc usunąć certyfikat podpisujący, wybierz opcję **Signers**, zaznacz certyfikat urzędu certyfikacji CA i kliknij przycisk **Delete**. Po usunięciu certyfikatu urzędu certyfikacji, żaden certyfikat wystawiony przez ten urząd nie będzie mógł być użyty w programie poczty

Netscape Communicator do podpisania lub szyfrowania wiadomości, ponieważ zostanie on zweryfikowany jako certyfikat niewiarygodny.

## Podpisywanie i szyfrowanie wiadomości

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

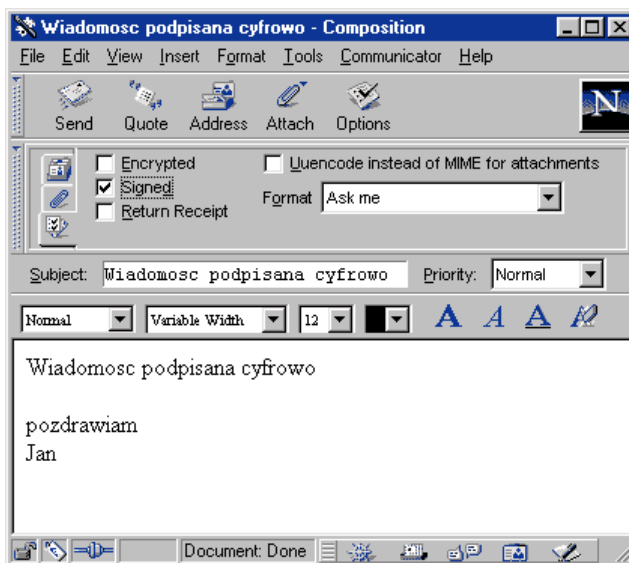
Złożenie podpisu powoduje, że wysyłana wiadomość zostanie podpisana z wykorzystaniem Twojego klucza prywatnego, a do przesyłki dołączony zostanie certyfikat wystawiony dla Ciebie przez Centrum Certyfikacji Signet. Uzyskany w ten sposób podpis elektroniczny stanowi gwarancję, że użytkownik, który wysłał 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).

Funkcja szyfrowania wiadomości powoduje 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 zapewniana jest 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

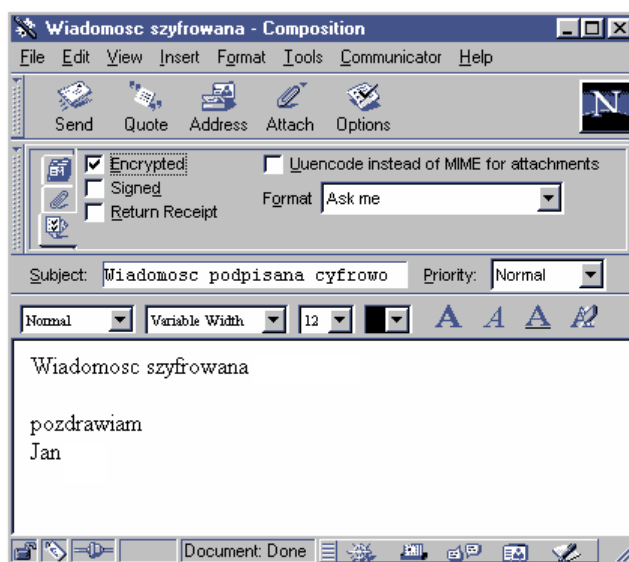
Wysłanie wiadomości podpisanej elektronicznie jest możliwe jedynie wtedy, gdy w bazie certyfikatów Netscape Communicator znajduje się zaimportowany certyfikat własny (patrz [Instalacja certyfikatów własnych](#)). Jeżeli masz już przygotowaną do wysłania wiadomość pocztową (menu **Communicator**, opcja **Messenger**, opcja **New Message**), w celu podpisania jej elektronicznie wybierz w oknie wiadomości z menu opcję **View**, a następnie **Options** (lub ikonę **Options** z paska menu). Pojawi się następujące okno, w którym zaznacz opcję **Signed**.



Wyślij wiadomość przyciskiem **Send**.

### Szyfrowanie wysyłanych wiadomości

Wysłanie wiadomości zaszyfrowanej wymaga pobrania i zaimportowania do bazy certyfikatów Netscape Communicator certyfikatu osoby, do której chcesz wysłać zaszyfrowaną wiadomość (patrz [Instalacja certyfikatów innych osób](#)). Jeżeli masz już napisaną wiadomość pocztową, w celu zaszyfrowania jej wybierz z menu opcję **View**, a następnie **Options** (lub ikonę **Options** z paska menu).



Zaznacz opcję **Encrypted**.

Jeżeli okaże się, że nie masz certyfikatu odbiorcy poczty, możesz pobrać go wybierając z menu opcję **Communicator, Tools**, a następnie **Security Info** (lub przycisk **Security**). Otworzy się okno informujące, że nie masz zaimportowanego certyfikatu dla odbiorcy wiadomości.

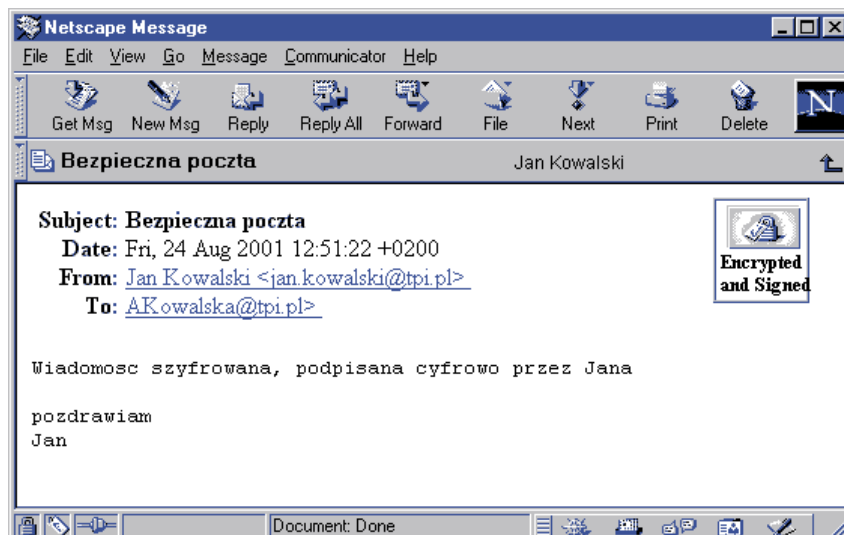


Przyciskiem **Get Certificates** możesz pobrać certyfikat odbiorcy z serwera usług katalogowych (patrz [Instalacja certyfikatów innych osób](#)). Certyfikat zostanie automatycznie dopisany do bazy certyfikatów. Wyślij wiadomość przyciskiem **Send**.

Istnieje możliwość ustawienia opcji szyfrowania każdej wysyłanej wiadomości, aż do odwołania. W tym celu otwórz okno **Security Info** (ikona **Security** na pasku nawigacyjnym), wybierz pozycję **Messenger** i włącz odpowiednią opcję w sekcji **Sending Signed/Encrypted Mail**.

## Odbieranie wiadomości szyfrowanych i podpisanych elektronicznie

Odebrane wiadomości pocztowe podpisane elektronicznie lub szyfrowane zaopatrzone są w specjalne ikony **Signed** lub **Encrypted** informujące, w jaki sposób nadawca zabezpieczył wiadomość.



Aby zweryfikować podpis elektroniczny dołączony do wiadomości, musisz mieć zaimportowany certyfikat nadawcy. Do odszyfrowania wiadomości wykorzystywany jest Twój klucz prywatny, dołączony do bazy certyfikatów Netscape Communicator (certyfikat własny). Jeżeli operacja weryfikacji podpisu cyfrowego lub odszyfrowania nie powiedzie się, wiadomość zostanie zaopatrzona w odpowiednią ikonę, np. **Invalid Encyption**, a jej treść nie będzie widoczna.