

UNIZETO



POWSZECHNE
CENTRUM CERTYFIKACJI



instrukcja użytkownika

Certyfikat Certum Basic ID

Instrukcja dla użytkowników Windows Vista

wersja 1.3

Spis treści

1. INSTALACJA CERTYFIKATU	3
1.1. KLUCZ ZAPISANY BEZPOŚREDNIO DO PRZEGLĄDARKI (NA TYM KOMPUTERZE),	3
1.2. KLUCZ ZAPISANY BEZPOŚREDNIO NA KARCIE KRYPTOGRAFICZNEJ,	5
1.3. KLUCZ GENEROWANY ZA POMOCĄ ŻĄDANIA WYDANIA CERTYFIKATU CSR.	7
2. IMPORTOWANIE CERTYFIKATU DO PROGRAMU POCZTA SYSTEMU WINDOWS	8
3. WYSYŁANIE PODPISANYCH WIADOMOŚCI	12
4. ODBIERANIE PODPISANYCH WIADOMOŚCI	13
5. WYSYŁANIE ZASZYFROWANYCH WIADOMOŚCI	15
6. WYSYŁANIE PODPISANYCH I ZASZYFROWANYCH WIADOMOŚCI	19
7. ODBIERANIE PODPISANYCH I ZASZYFROWANYCH WIADOMOŚCI	20
8. EKSPORT CERTYFIKATU Z PROGRAMU POCZTOWEGO SYSTEMU WINDOWS	22
9. SPIS RYSUNKÓW	28

1. Instalacja Certyfikatu

Instalacja certyfikatu zależy od wybranej metody zapisania klucza kryptograficznego (patrz rozdział 1 podpunkt 17 – Rejestracja certyfikatu Basic ID) :

1.1. Klucz zapisany bezpośrednio do przeglądarki (Na tym komputerze),

1. Instalacji certyfikatu można dokonać za pośrednictwem konta klienta w systemie CERTUM PCC. Wchodzimy na stronę <https://sklep.unizeto.pl/> → zakładka **Zarządzanie certyfikatami**

The screenshot shows the 'Zarządzanie certyfikatami' page. On the left is a navigation menu with options: 'Kody elektroniczne', 'Aktywacja certyfikatów', 'Zarządzanie certyfikatami' (highlighted), 'Historia zamówień', 'Dane adresowe', 'Narzędzia', and 'Newsletter'. The main content area has a search form with fields for 'Profil certyfikatu', 'Nazwa', 'Email', 'Wydany po', and 'Wydany przed', along with a 'Szukaj' button. To the right of the search form are status filters: 'Ważny', 'Unieważniony', 'Wygasty', and 'Uzyska ważność'. Below the search form is a table of certificates:

Nr seryjny	Profil certyfikatu	Email	Nazwa	Ważny od	Ważny do	Status
24a012fe7cbe3 ad3e32e3fc33a 5bf133	Basic ID	marcin.sztyrbicki@unizeto.pl	Basic ID	17 październik 2011 12:27:52	16 październik 2012 12:27:52	Ważny

Rysunek 1 - Profil certyfikatu Basic ID

2. W celu zainstalowania certyfikatu, dla którego klucz został wygenerowany w przeglądarce należy odnaleźć ten certyfikat na liście certyfikatów przypisanych do konta użytkownika i następnie należy kliknąć w obrębie tego certyfikatu. Wyświetlone zostaną opcje dotyczące wybranego certyfikatu. Aby zainstalować certyfikat wybieramy przycisk **Zainstaluj własny**.

PRODUKTY POMOC O FIRMIE

Szukaj w sklepie

Strona główna » Moje konto » Zarządzanie certyfikatami

Zarządzanie certyfikatami

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

Zarządzanie certyfikatami

Profil certyfikatu: [Wybierz]
Nazwa: [Wpisz]
Email: [Wpisz]
Wydany po: [Wybierz] Wydany przed: [Wybierz]

Status:
 Ważny
 Unieważniony
 Wygaśły
 Uzyska ważność

Szukaj

Nr seryjny	Profil certyfikatu	Email	Nazwa	Ważny od	Ważny do	Status
24a0d2fe7c be3ad3e32e 3fc33a5bf1 33	Basic ID	marcin.sztyrbicki@unizeto.pl	Basic ID	17 październik 2011 12:27:52	16 październik 2012 12:27:52	Ważny

Nazwa: Basic ID
Email: marcin.sztyrbicki@unizeto.pl

Basic ID

Unieważnij Odnów
Zainstaluj własny
Zapisz binarnie Zapisz tekstowo

Rysunek 2 – Instalacja certyfikatu Basic ID

3. Użytkownik jest informowany o instalacji certyfikatu z zapytaniem o potwierdzenie chęci instalacji certyfikatu. Należy wybrać opcję **TAK** aby kontynuować wgrywanie certyfikatu.

Potencjalne naruszenie kodu skryptów

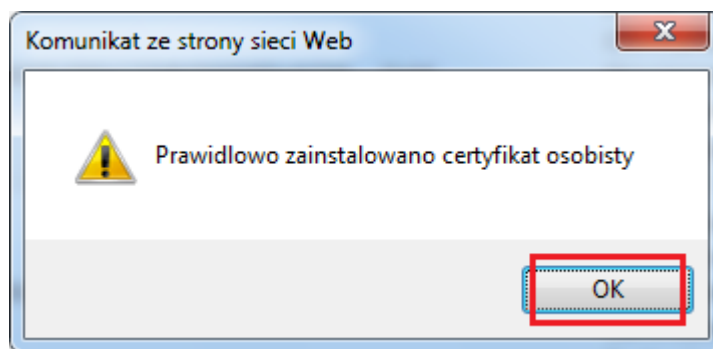
⚠ Ta witryna sieci Web dodaje jeden lub więcej certyfikatów do tego komputera. Zezwolenie niezauwanej witrynie sieci Web na aktualizację certyfikatów stanowi zagrożenie bezpieczeństwa. Witryna sieci Web może zainstalować certyfikaty, którym nie ufasz, co mogłoby umożliwić niezauwanym programom uruchamianie się na tym komputerze i uzyskiwanie dostępu do danych.

Czy chcesz, aby ten program dodał certyfikaty teraz? Kliknij przycisk Tak, jeśli ufasz tej witrynie sieci Web. W przeciwnym wypadku kliknij przycisk Nie.

Tak Nie

Rysunek 3 – Instalacja certyfikatu Basic ID – Informacja o instalacji certyfikatu

4. Po zatwierdzeniu chęci instalacji certyfikatu zostanie on zainstalowany w przeglądarce i zostanie wyświetlona stosowna informacja o tym. Wybieramy przycisk **OK**.



Rysunek 4 – Potwierdzenie wgrania certyfikatu Basic ID

1.2. Klucz zapisany bezpośrednio na karcie kryptograficznej,

W celu zainstalowania certyfikatu, dla którego klucz został wygenerowany na karcie należy najpierw umieścić tę kartę w czytniku, następnie należy odnaleźć ten certyfikat na liście certyfikatów przypisanych do konta użytkownika i kliknąć w obrębie tego certyfikatu. Wyświetlone zostaną opcje dotyczące wybranego certyfikatu.

1. Instalacji certyfikatu można dokonać za pośrednictwem konta klienta w systemie CERTUM PCC. Wchodzimy na stronę <https://sklep.unizeto.pl/> → zakładka **Zarządzanie certyfikatami**

Strona główna » Moje konto » Zarządzanie certyfikatami

Zarządzanie certyfikatami

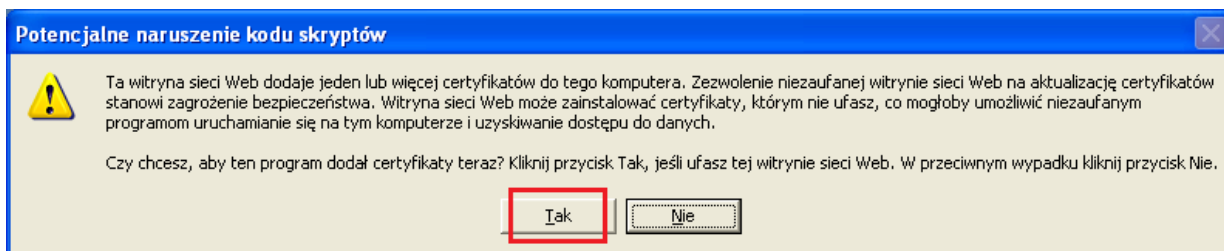
Profil certyfikatu: [Wybierz profil]
Nazwa: [Wpisz nazwę]
Email: [Wpisz email]
Wydany po: [Wybierz urządzenie] Wydany przed: [Wybierz urządzenie]
Szukaj

Status:
 Ważny
 Unieważniony
 Wygasły
 Uzyska ważność

Nr seryjny	Profil certyfikatu	Email	Nazwa	Ważny od	Ważny do	Status
24a0d2fe7cbe3 ad3e32e3fc33a 5bf133	Basic ID	marcin.sztyrbicki@unizeto.pl	Basic ID	17 październik 2011 12:27:52	16 październik 2012 12:27:52	Ważny

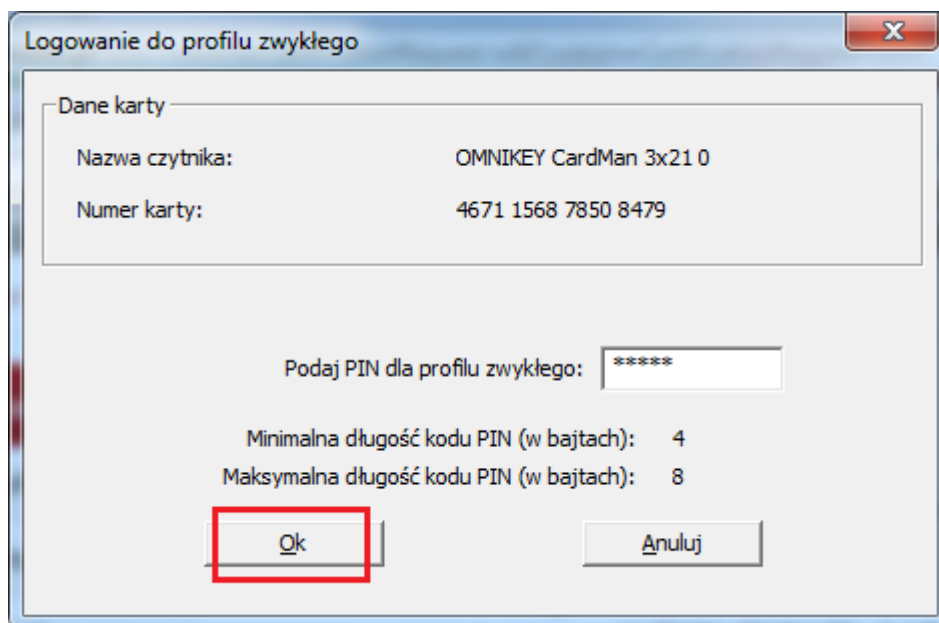
Rysunek 5 – Profil certyfikatu Basic ID

2. Użytkownik jest informowany o instalacji certyfikatu z zapytaniem o potwierdzenie chęci instalacji certyfikatu. Należy wybrać opcję **TAK** aby kontynuować wgrywanie certyfikatu.



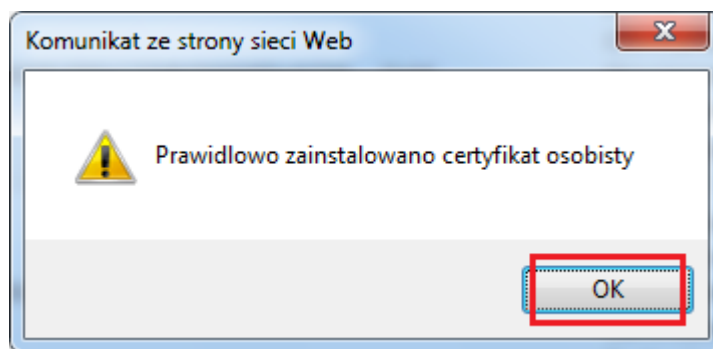
Rysunek 6 – Instalacja certyfikatu Basic ID – Informacja o instalacji certyfikatu

3. Po zatwierdzeniu chęci instalacji certyfikatu zostanie wyświetlona prośba o wprowadzenie kodu **PIN** do **Profilu Zwykłego** Karty.



Rysunek 7 – Prośba o wprowadzenie kodu PIN do Profilu Zwykłego karty

4. Po wprowadzeniu poprawnego kodu **PIN** i zatwierdzeniu go certyfikat zostanie zainstalowany na karcie i zostanie wyświetlona stosowna informacja o tym.



Rysunek 8 – Potwierdzenie wgrania certyfikatu Basic ID

1.3. Klucz generowany za pomocą żądania wydania certyfikatu CSR.

Wybranie opcji uzyskania certyfikatu przy pomocy żądania CSR umożliwia użytkownikowi pobranie certyfikatu w formie pliku. Pobrany plik certyfikatu należy połączyć z kluczem prywatnym, który był wygenerowanym przy pomocy (np.: serwer, aplet Javy itp.) innych narzędzi niż przeglądarka internetowa.

1. Uzyskany certyfikat można pobrać za pośrednictwem konta klienta w systemie CERTUM PCC. Wchodzimy na stronę <https://sklep.unizeto.pl/> → zakładka **Zarządzanie certyfikatami**

Strona główna » Moje konto » Zarządzanie certyfikatami

Zarządzanie certyfikatami

Profil certyfikatu: [Wybierz] Status: Ważny, Unieważniony, Wygasły, Uzyska ważność

Nazwa: [Wpisz] Email: [Wpisz]

Wydany po: [Wybierz] Wydany przed: [Wybierz]

[Szukaj]

Nr seryjny	Profil certyfikatu	Email	Nazwa	Ważny od	Ważny do	Status
24a012fe7cbe3 ad3e32e3fc33a 5bf133	Basic ID	marcin.sztyrbicki@unizeto.pl	Basic ID	17 październik 2011 12:27:52	16 październik 2012 12:27:52	Ważny

Rysunek 9 – Profil certyfikatu Basic ID

2. W celu pobrania certyfikatu, dla którego klucz został wygenerowany przy pomocy innych narzędzi, należy odnaleźć ten certyfikat na liście certyfikatów przypisanych do konta użytkownika i następnie

należy kliknąć w obrębie tego certyfikatu. Wyświetlone zostaną opcje dotyczące wybranego certyfikatu. Aby pobrać certyfikat wybieramy przycisk **Zapisz binarnie** lub **zapisz tekstowo**. Po zapisaniu certyfikatu w formie pliku, możemy wykonać import pobranego certyfikatu do maszyny, z której wcześniej utworzyliśmy żądania CSR (na tej maszynie powinien być zapisany klucz prywatny do uzyskanego certyfikatu).

Zarządzanie certyfikatami

Profil certyfikatu: [Wybierz profil] Status: Ważny, Unieważniony, Wygasły, Uzyska ważność

Nazwa: [Wpisz nazwę] Email: [Wpisz email]

Wydany po: [Wybierz datę] Wydany przed: [Wybierz datę]

Szukaj

Nr seryjny	Profil certyfikatu	Email	Nazwa	Ważny od	Ważny do	Status
24a012fe7cbe3 a43e32e3fc33a 5bf133	Basic ID	marcin.sztyrbicki@unizeto.pl	Basic ID	17 październik 2011 12:27:52	16 październik 2012 12:27:52	Ważny

Nazwa: Basic ID Email: marcin.sztyrbicki@unizeto.pl

Unieważnij Zainstaluj własny Odnów

Zapisz binarnie Zapisz tekstowo

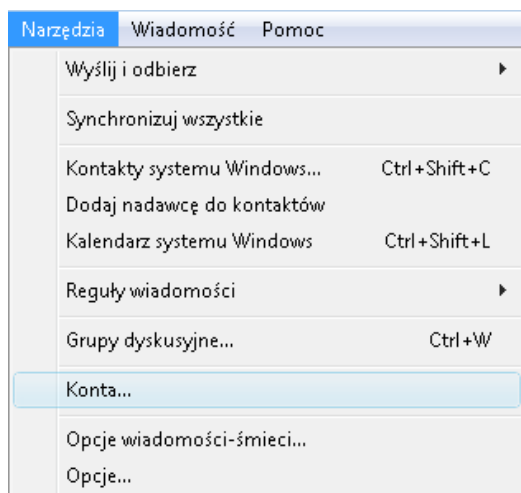
Rysunek 10 – Pobranie certyfikatu Basic ID do pliku

2. Importowanie certyfikatu do programu Poczta systemu Windows

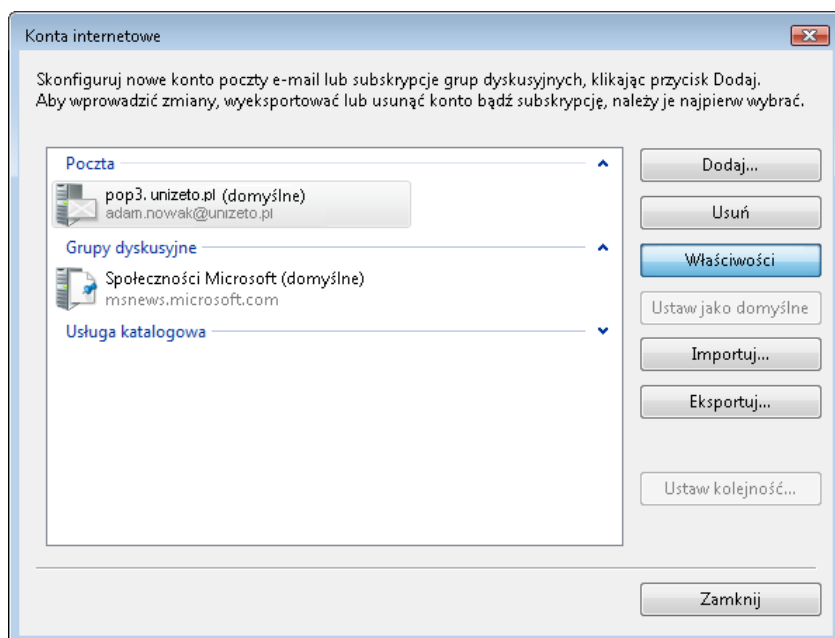
Internet Explorer i program pocztowy systemu Windows mają wspólną bibliotekę certyfikatów. Jeżeli certyfikaty i lista CRL są już zainstalowane w systemie Windows, można przystąpić do konfiguracji programu pocztowego Outlook Express.

Przy założeniu, iż program pocztowy ma już zdefiniowane konto pocztowe, mamy za zadanie dodać obsługę szyfrowania i podpisywania wiadomości. W tym celu wykonaj następujące czynności:

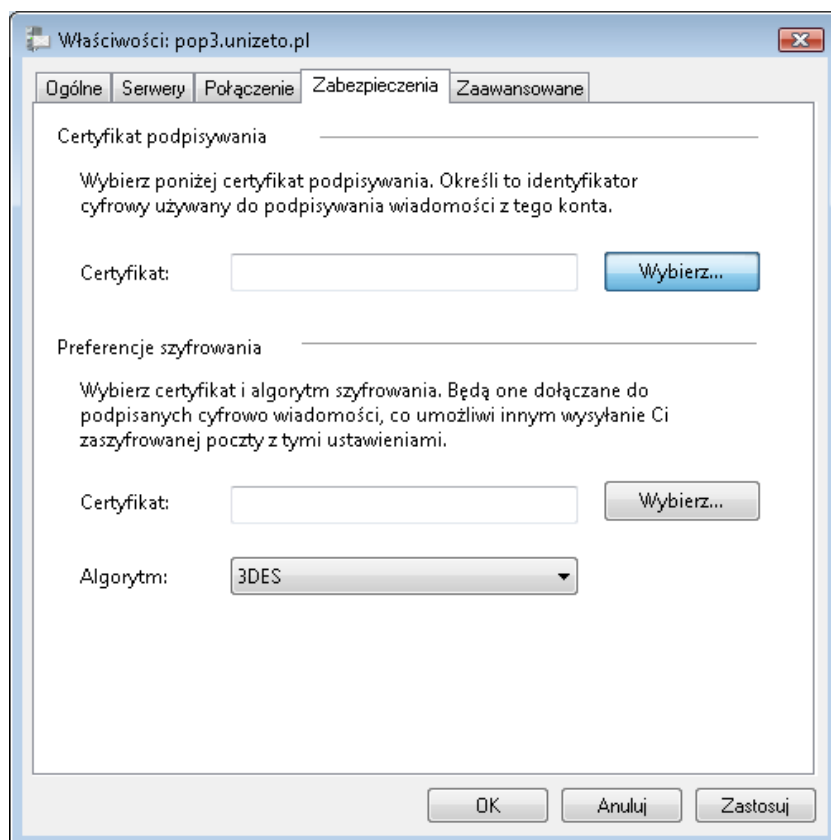
1. Otwórz program pocztowy systemu Windows.
2. Z menu **Narzędzia** wybierz **Konta**.



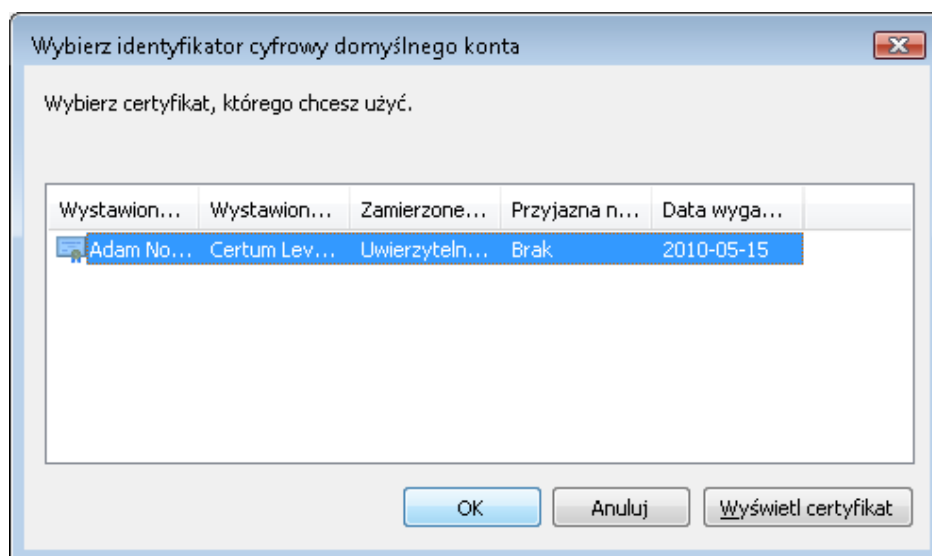
3. Naciśnij **Właściwości** konta, dla którego chcesz zdefiniować mechanizmy zabezpieczające.



4. W oknie **Właściwości** naciśnij zakładkę **Zabezpieczenia**.

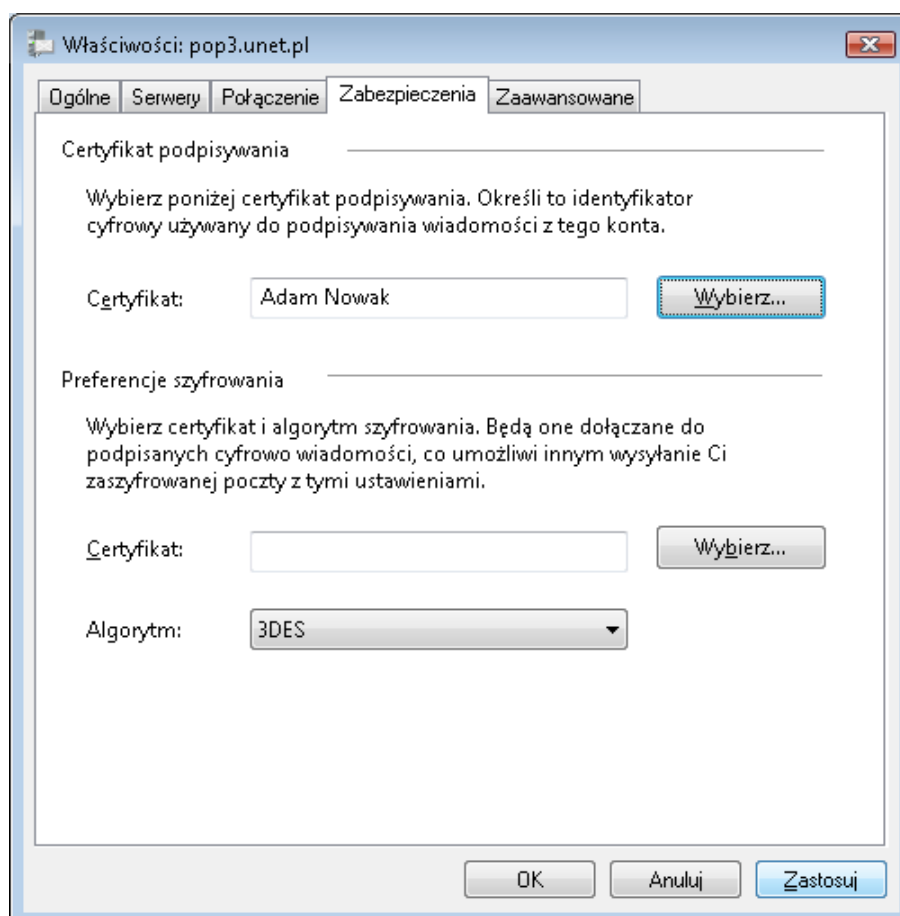


5. Otwórz okno wyboru certyfikatu podpisującego naciskając **Wybierz**.



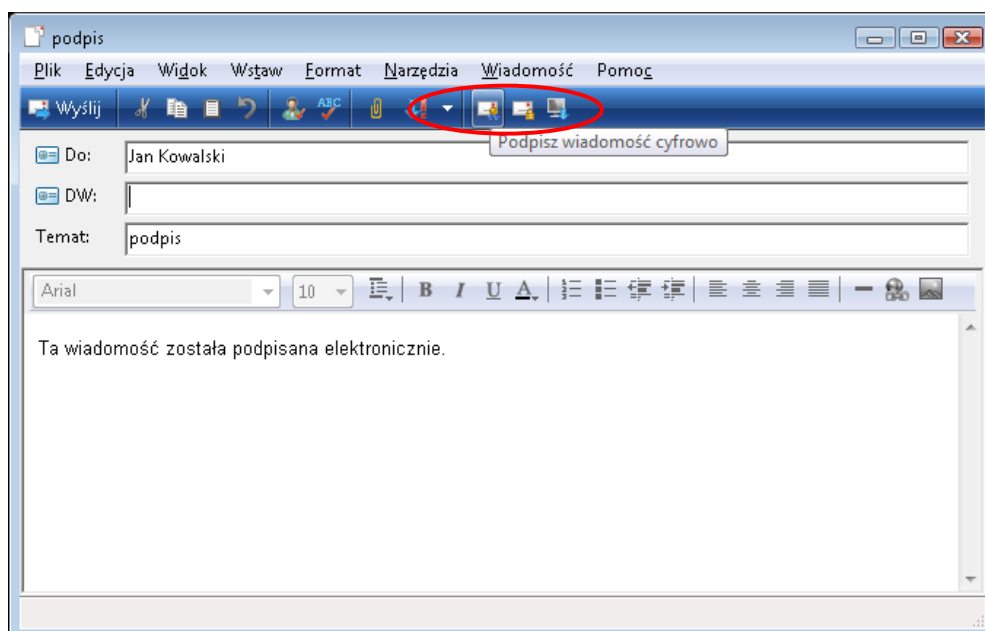
6. Wybierz z listy certyfikat i naciśnij **OK**.

7. W oknie poniżej naciśnij **Zastosuj**, a następnie **OK**. Można już wysłać wiadomości podpisane certyfikatem.

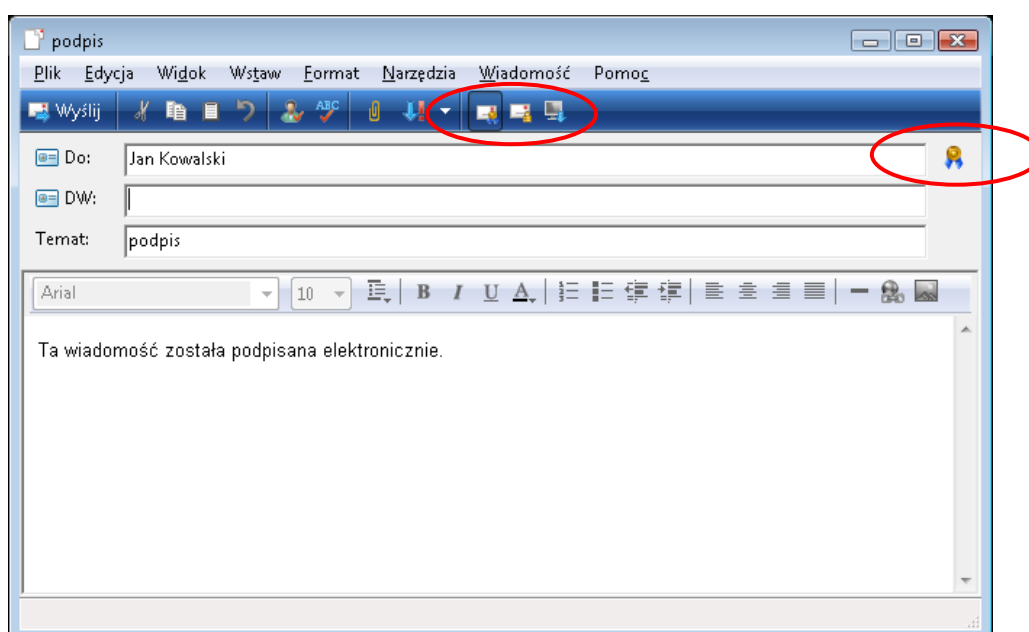


3. Wysyłanie podpisanych wiadomości

1. W Poczcie systemu Windows otwórz nową wiadomość naciskając **Utwórz pocztę**.
2. W oknie wiadomości wybierz adresata i napisz treść, a następnie naciśnij na niedużą ikonę koperty z kotylionem.



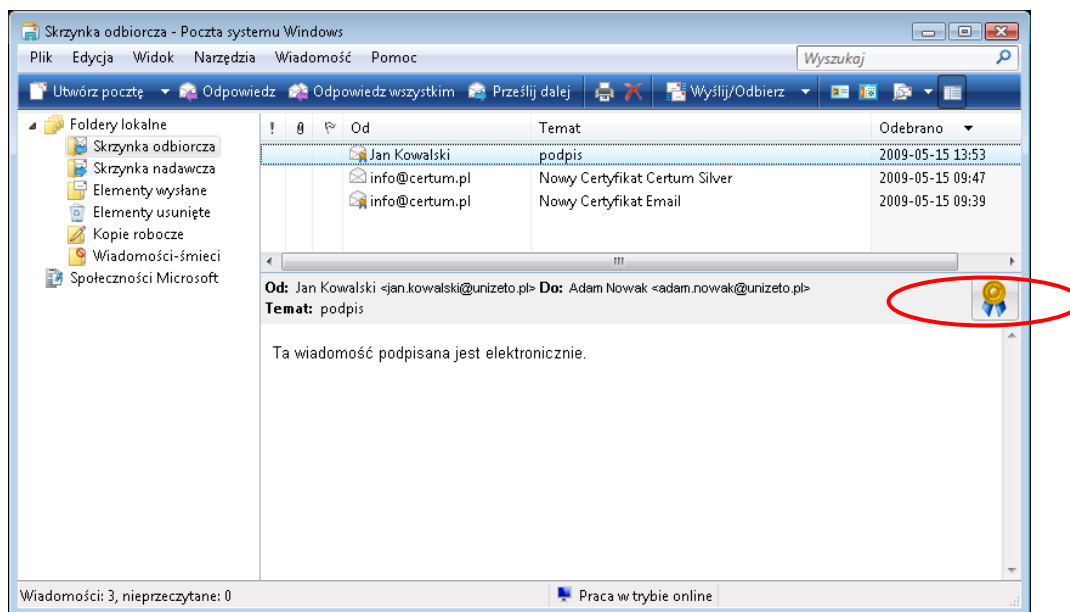
3. Kiedy przycisk jest już włączony, po prawej stronie paska adresu „Do:” ukaże się znak kotyliona.



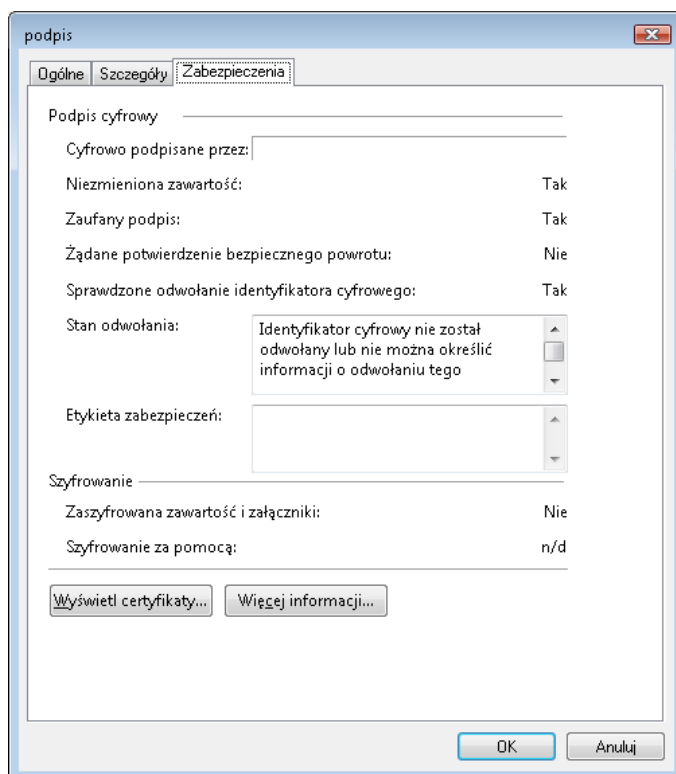
4. Naciśnij przycisk **Wyślij**. Podpisana wiadomość została wysłana.

4. Odbieranie podpisanych wiadomości

1. Wiadomość podpisana elektronicznie jest specjalnie oznakowana w programie pocztowym.

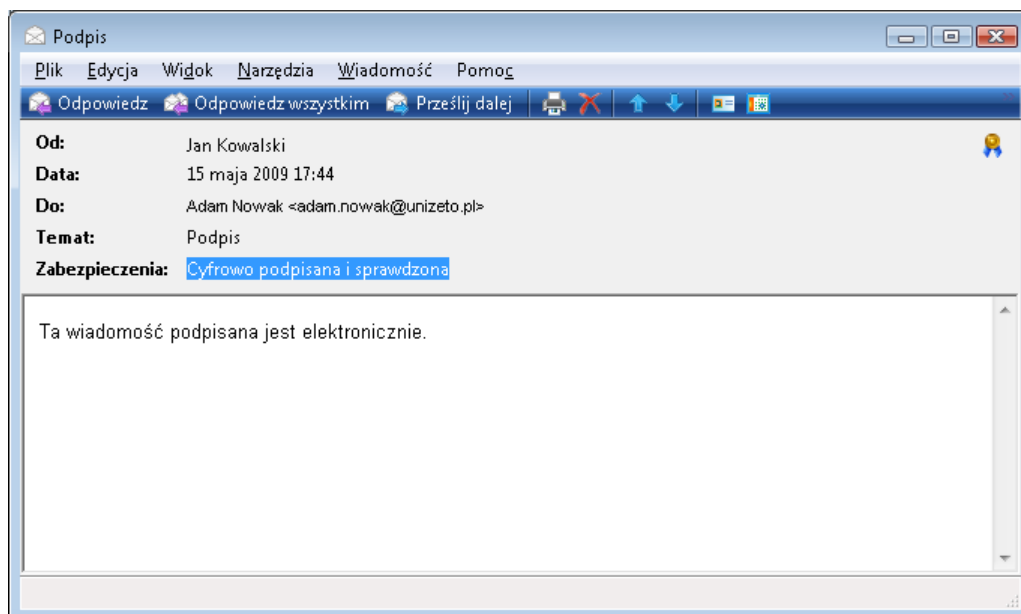


2. W celu sprawdzenia certyfikatu nadawcy, kliknij dwukrotnie na ikonę kotyliona. Otworzy się okno ze szczegółami podpisu. Podpis jest zaufany, a zawartość nie została zmieniona.



3. Naciśnij **OK**.

4. Można też kliknąć dwukrotnie na wiadomość z listy programu pocztowego i otworzyć ją w nowym oknie. Oprócz znaku kotyliona, widnieje tu informacja o zabezpieczeniach.

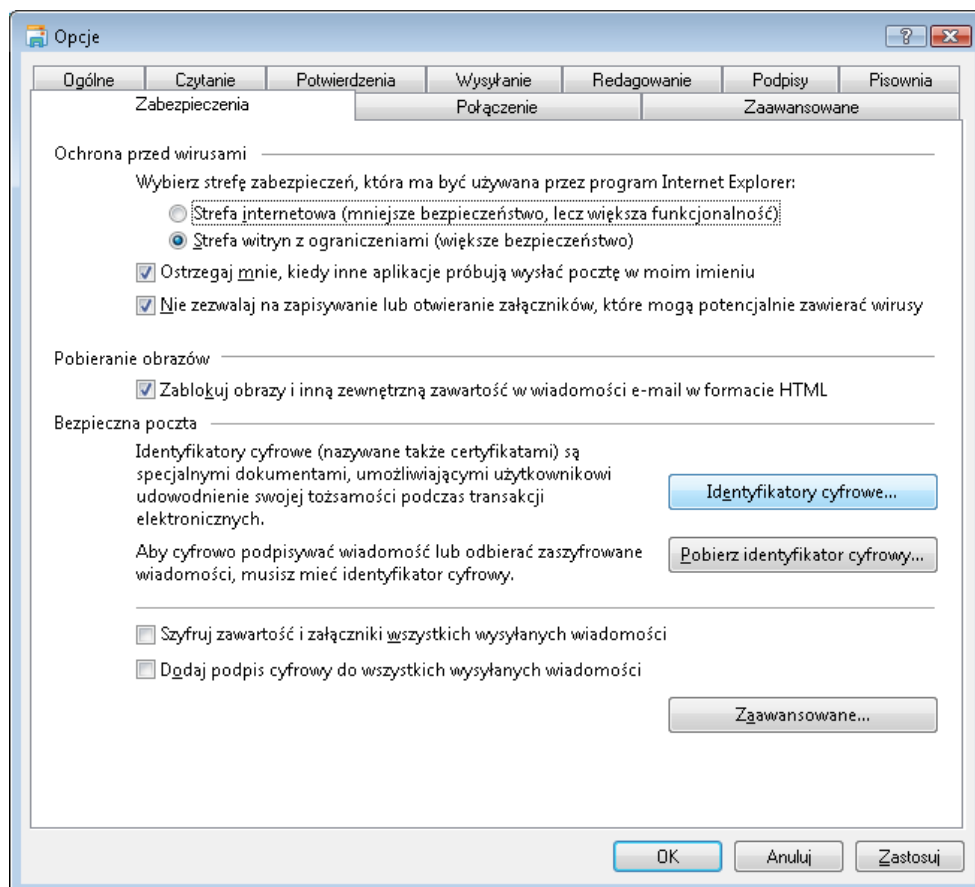


5. Po kliknięciu na znak kotyliona otworzy się okno ze szczegółami podpisu (jak powyżej).

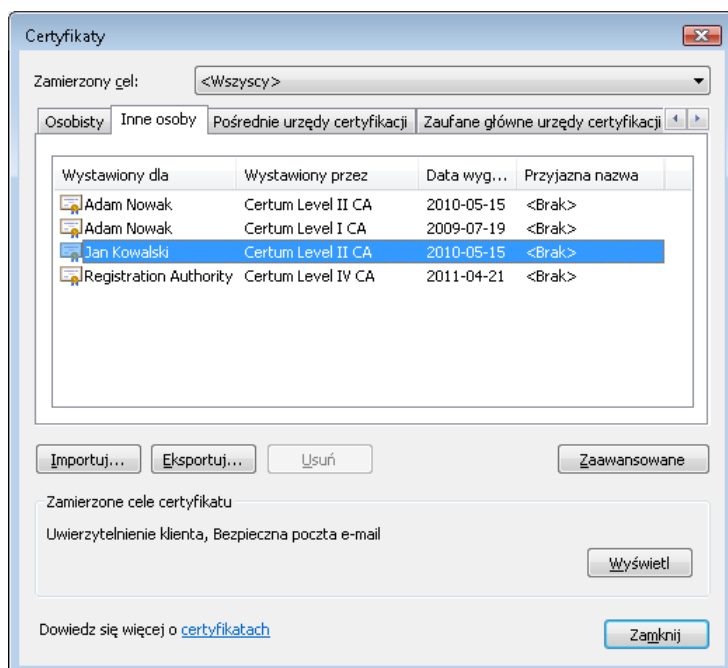
5. Wysłanie zaszyfrowanych wiadomości

W momencie, gdy otrzymujemy podpisaną wiadomość, certyfikat nadawcy dodawany jest do magazynu certyfikatów Windows. Umożliwia to wysłanie wiadomości zaszyfrowanych, gdyż do ich szyfrowania używany jest certyfikat drugiej osoby.

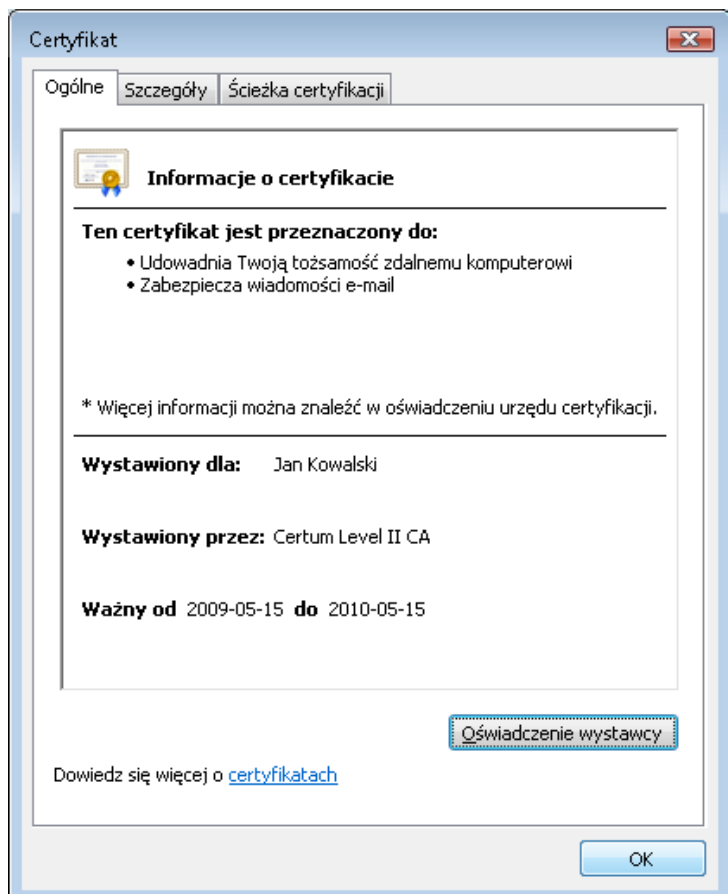
1. Aby sprawdzić czy posiadasz, potrzebny do szyfrowania, certyfikat drugiej osoby, wejdź do menu **Narzędzia** → **Opcje** i naciśnij zakładkę **Zabezpieczenia**.



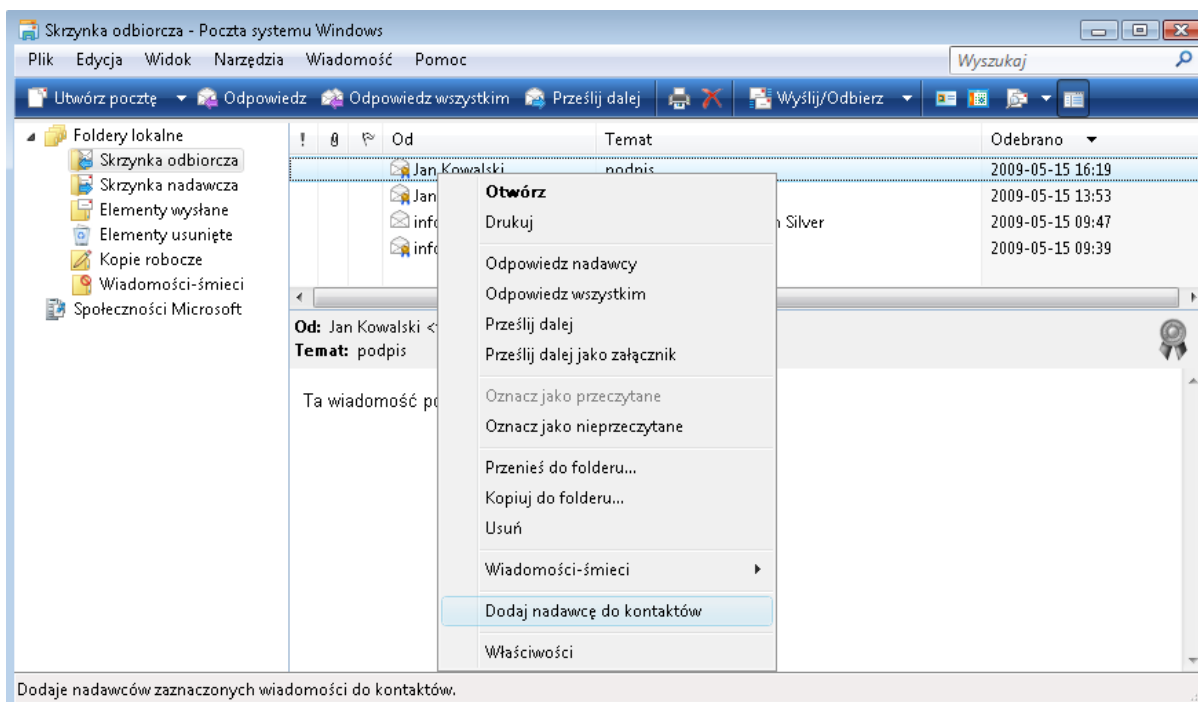
2. Naciśnij **Identyfikatory cyfrowe**, a w nowym oknie naciśnij zakładkę **Inne osoby**.



3. Aby sprawdzić informacje o certyfikacie, naciśnij **Wyświetl**.

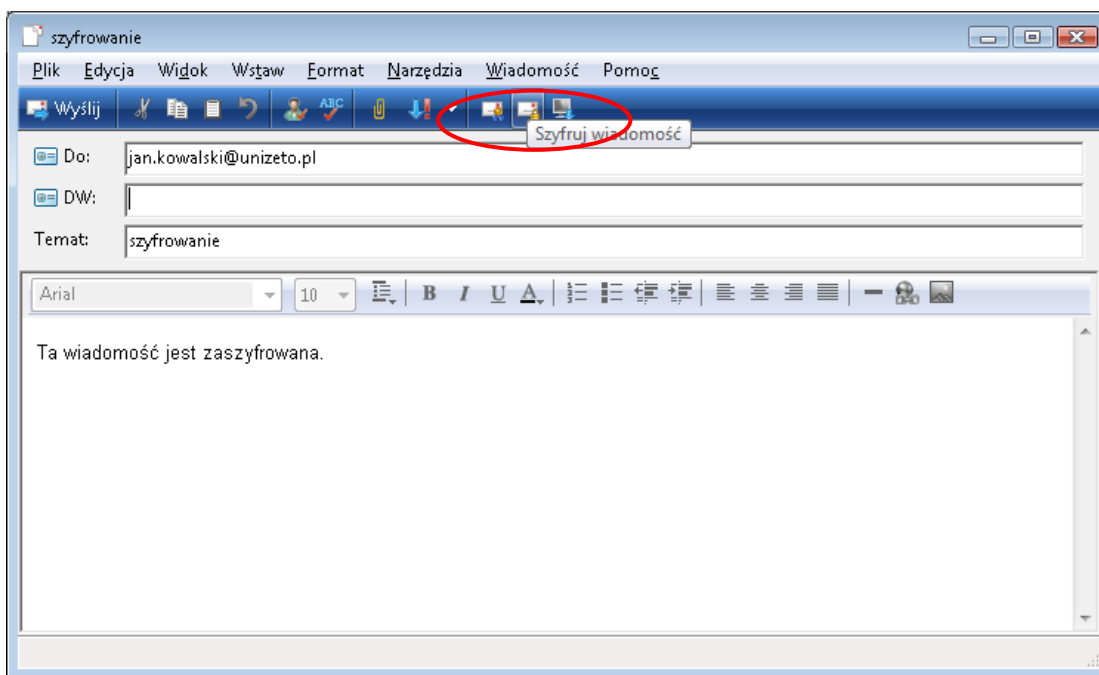


4. System automatycznie dodaje nadawców do kontaktów. Przejdź do głównego okna Poczty systemu Windows i naciśnij prawym klawiszem myszy na wiadomość.



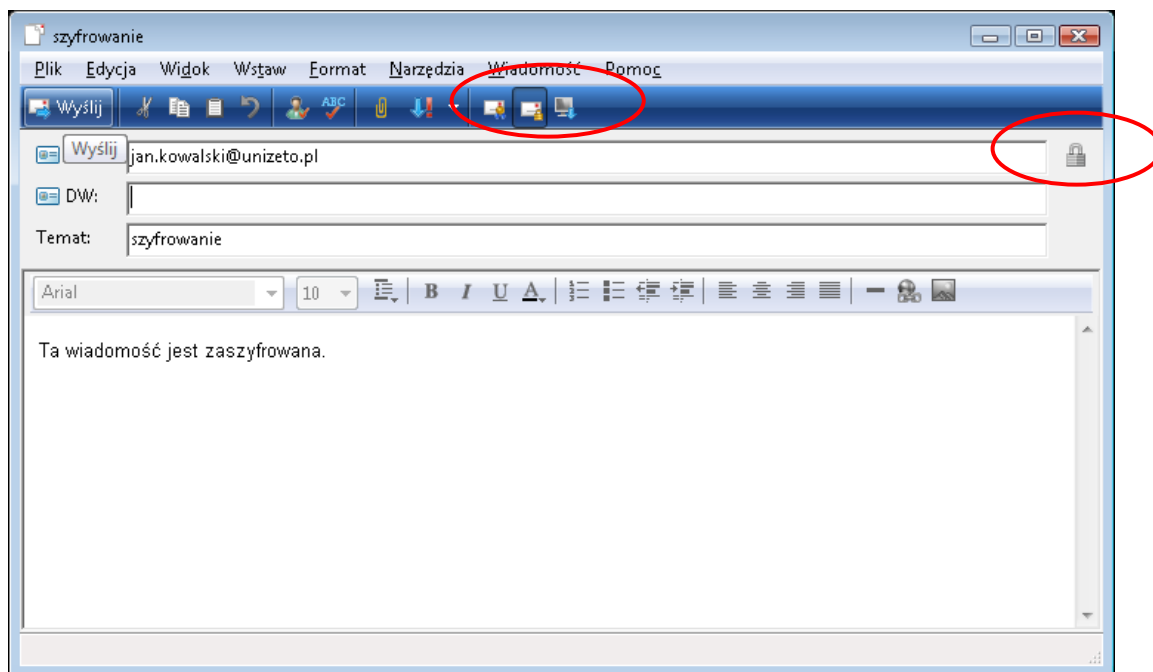
5. Naciśnij z listy **Dodaj nadawcę do kontaktów**. Jeżeli kontakt został prawidłowo dodany, system automatycznie nas o tym poinformuje komunikatem: **Ten kontakt jest już w kontaktach**.

6. Aby wysłać wiadomość, w głównym oknie programu pocztowego naciśnij **Utwórz pocztę**.



7. W oknie wiadomości wybierz adresata i napisz treść, a następnie naciśnij na niedużą ikonę koperty z kłódką.

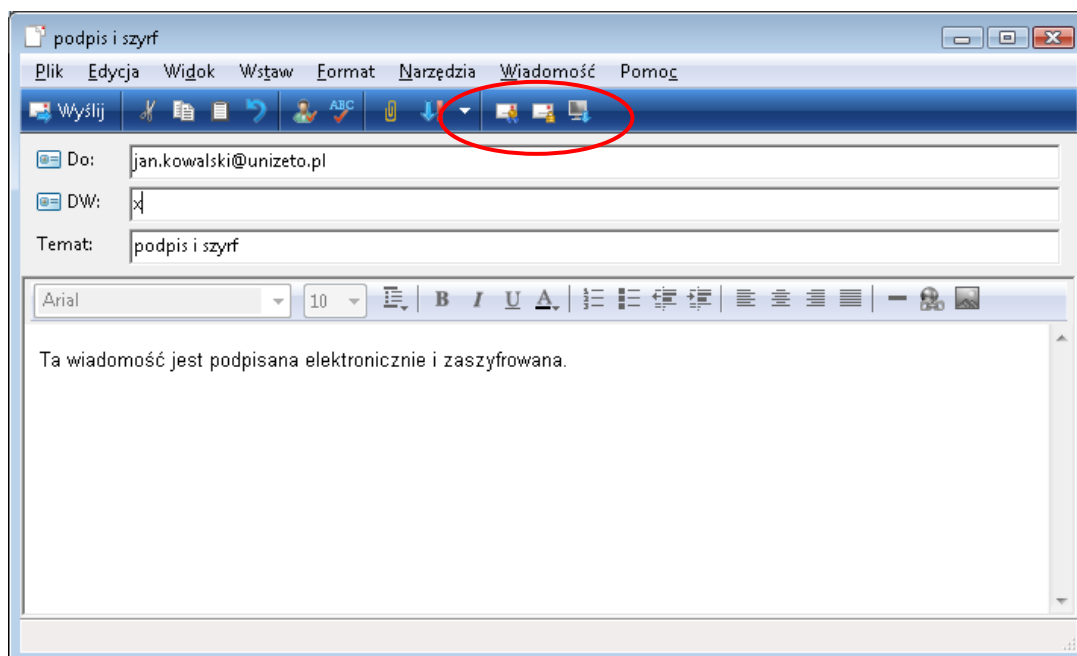
8. Kiedy przycisk jest już włączony, po prawej stronie paska adresu „Do:” ukaże się znak kłódki.



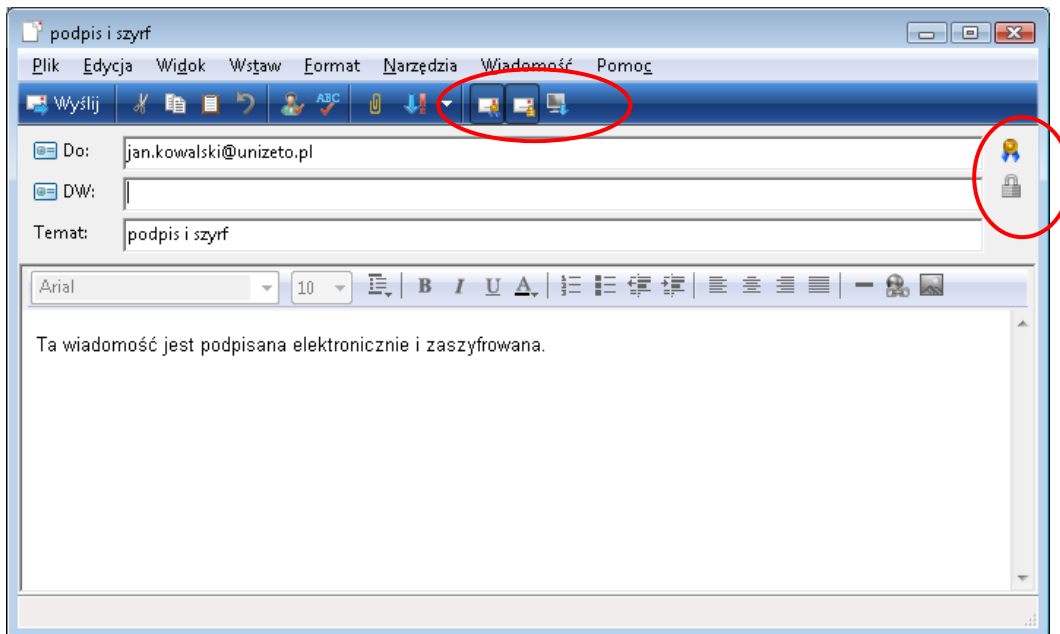
9. Naciśnij przycisk **Wyślij**. Zaszyfrowana wiadomość została wysłana.

6. Wysyłanie podpisanych i zaszyfrowanych wiadomości

1. W Poczcie systemu Windows otwórz nową wiadomość klikając **Utwórz pocztę**.
2. W oknie wiadomości wybierz adresata i napisz treść, a następnie naciśnij na dwie nieduże ikony kopert: z kotylionem i z kłódką.



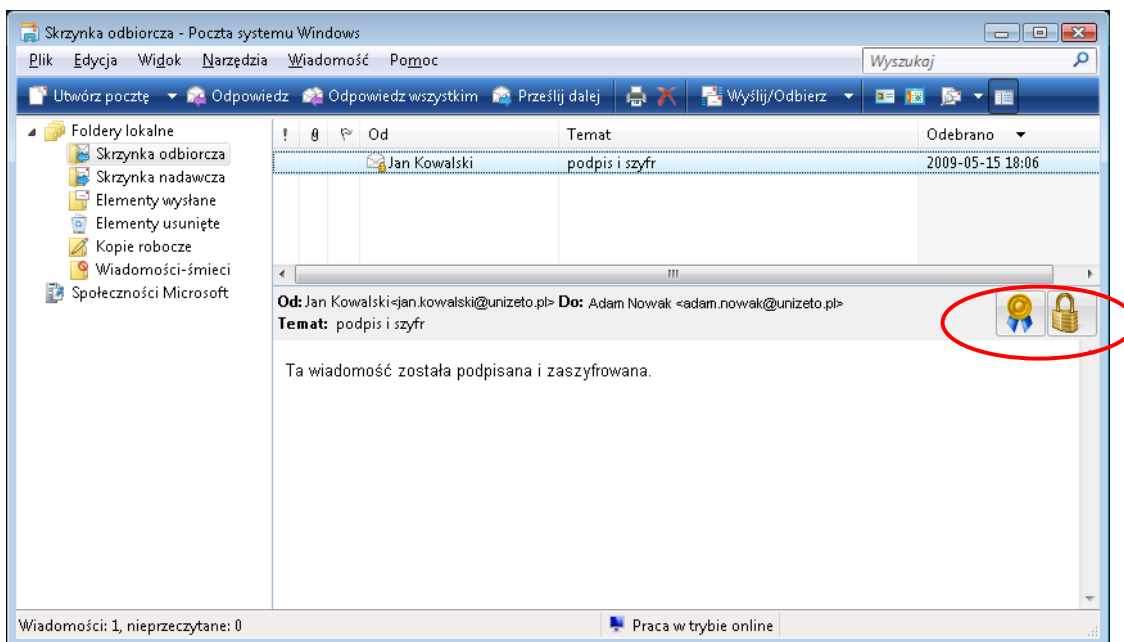
3. Kiedy przyciski są już włączone, po prawej stronie paska adresu „Do:” ukaże się znak kotyliona i kłódki.



4. Naciśnij przycisk **Wyslij**. Podpisana i zaszyfrowana wiadomość została wysłana.

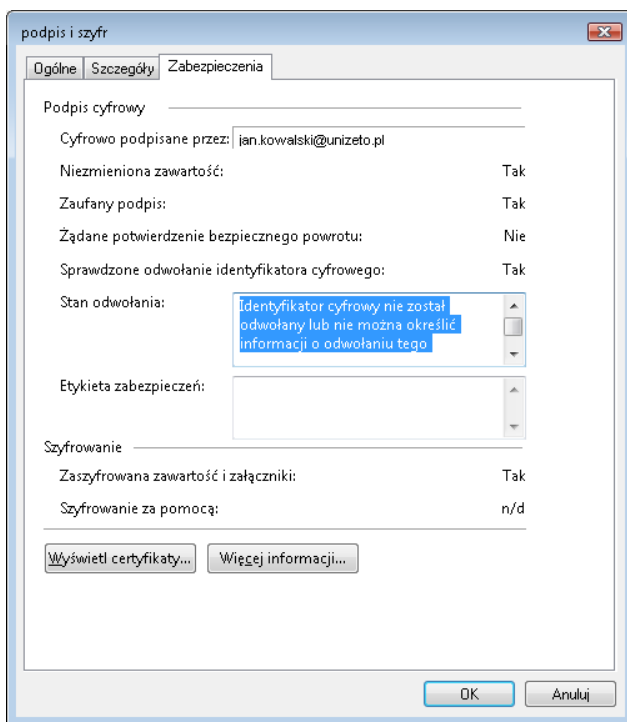
7. Odbieranie podpisanych i zaszyfrowanych wiadomości

1. Wiadomość podpisana i zaszyfrowana jest specjalnie oznakowana w programie pocztowym.



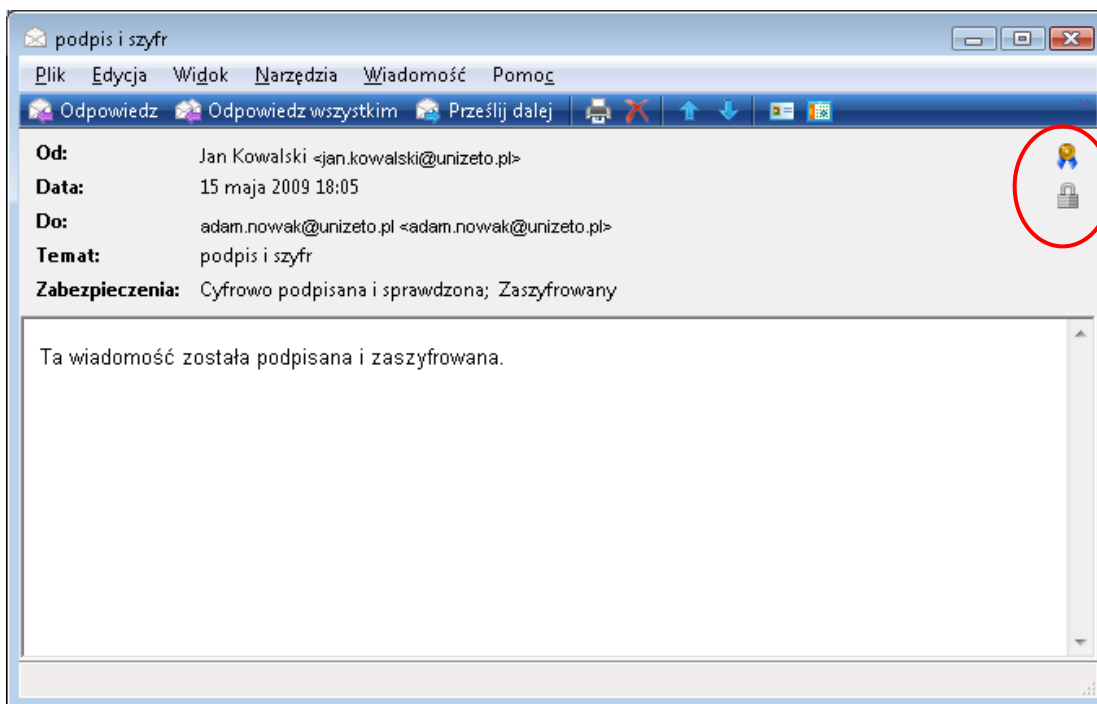
2. W celu sprawdzenia certyfikatu nadawcy, kliknij dwukrotnie na ikonę kotyliona lub kłódki. Otworzy się

okno ze szczegółami podpisu. Podpis jest zaufany, a zawartość nie została zmieniona.



3. Naciśnij **OK**.

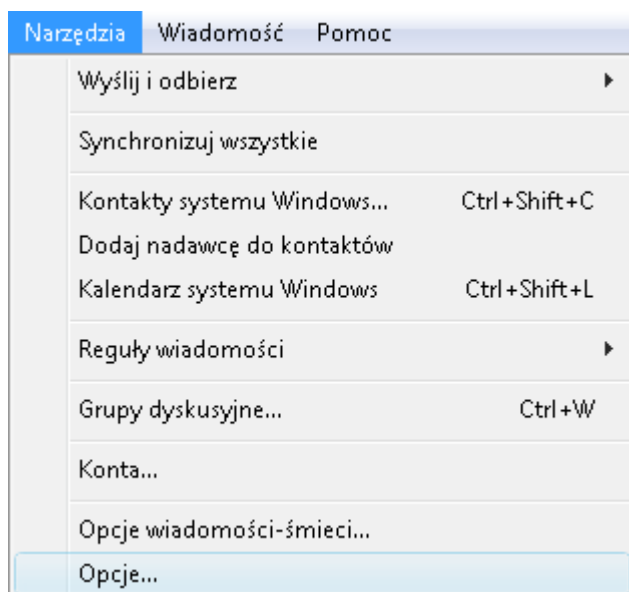
4. Można też kliknąć dwukrotnie na wiadomość z listy programu pocztowego i otworzyć ją w nowym oknie. Oprócz znaku kotyliona i kłódki, widnieje tu informacja o zabezpieczeniach.



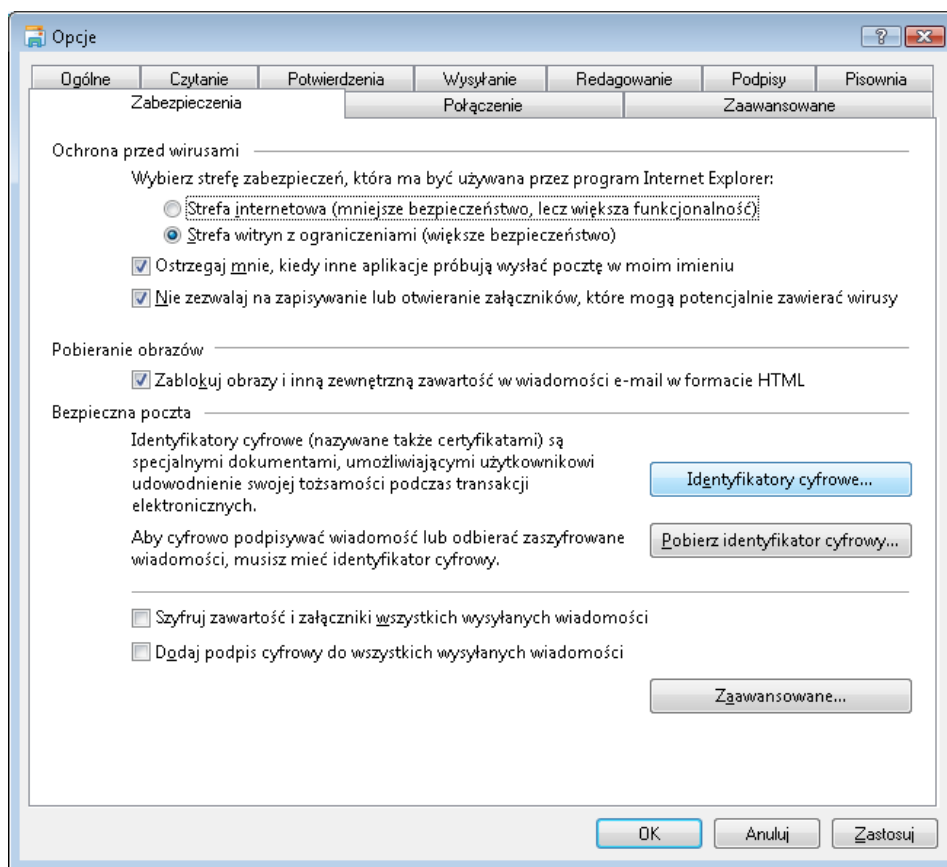
5. Po kliknięciu znaku kotyliona, otworzy się okno ze szczegółami podpisu (jak wyżej).

8. Eksport certyfikatu z programu pocztowego systemu Windows

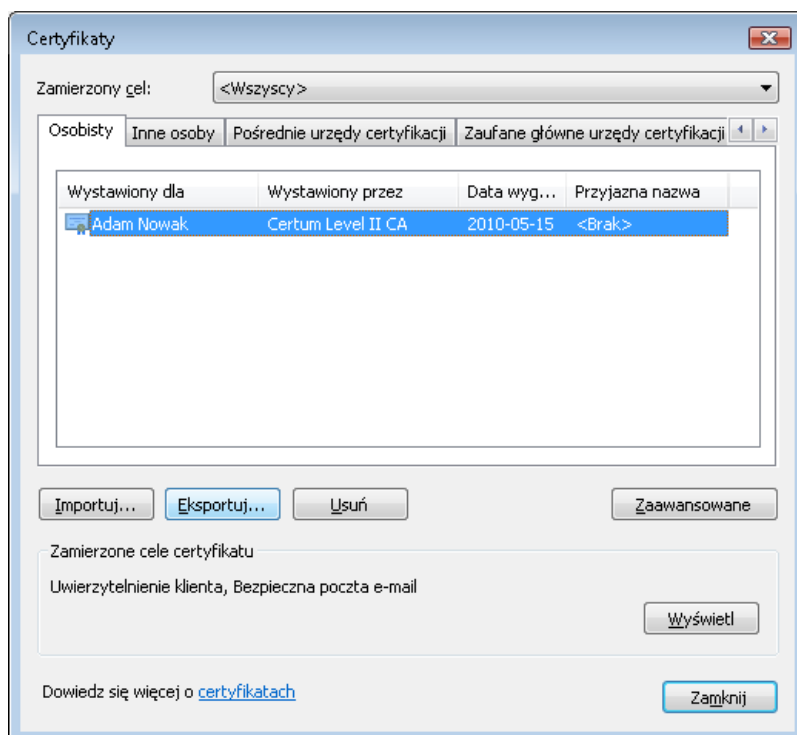
1. Naciśnij menu **Narzędzia** → **Opcje**.



2. W zakładce **Zabezpieczenia** naciśnij **Identyfikatory cyfrowe**.

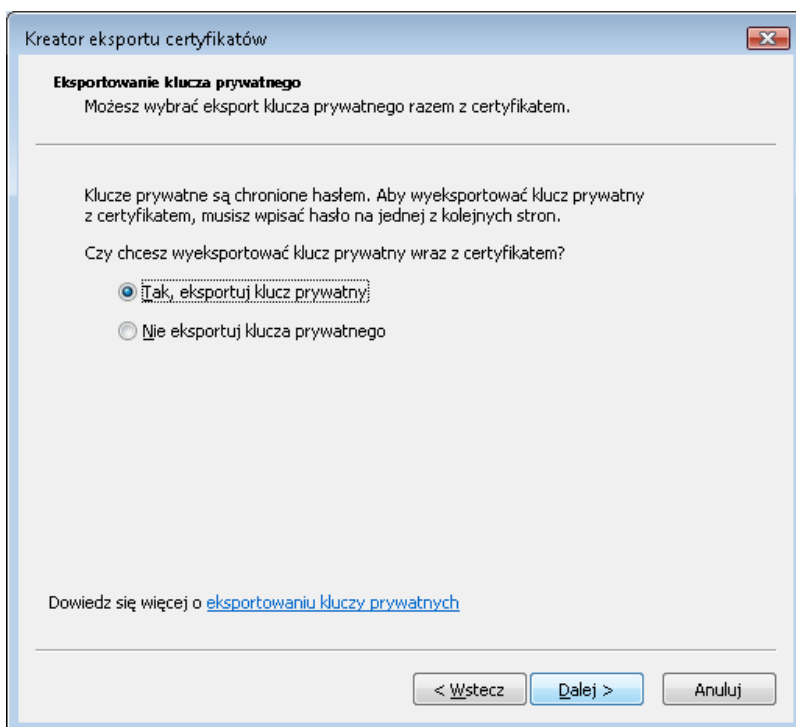


3. W nowym oknie wybierz z listy certyfikat, który chcesz eksportować, a następnie naciśnij **Eksportuj**.

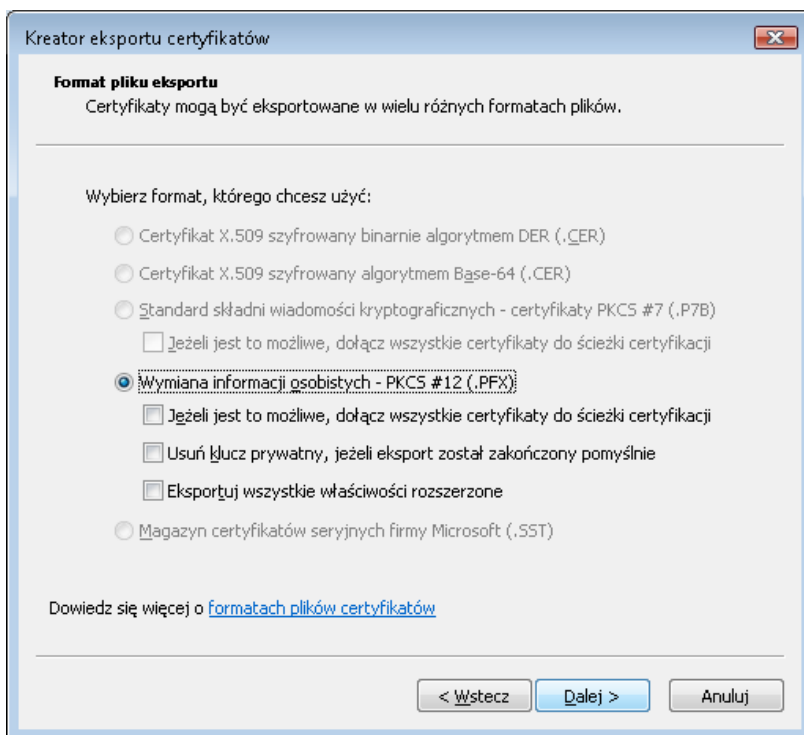


4. Otworzy się Kreator Certyfikatów. Naciśnij **Dalej**.

5. W kolejnym oknie naciśnij **Tak, eksportuj klucz prywatny**, a następnie naciśnij **Dalej**.



6. W następnym oknie należy pozostawić ustawienia domyślne. Naciśnij **Dalej**.



7. Następnie wpisz i potwierdź hasło do klucza prywatnego. Kliknij **Dalej**.

Kreator eksportu certyfikatów

Hasło
Aby zapewnić bezpieczeństwo, musisz zabezpieczyć klucz prywatny za pomocą hasła.

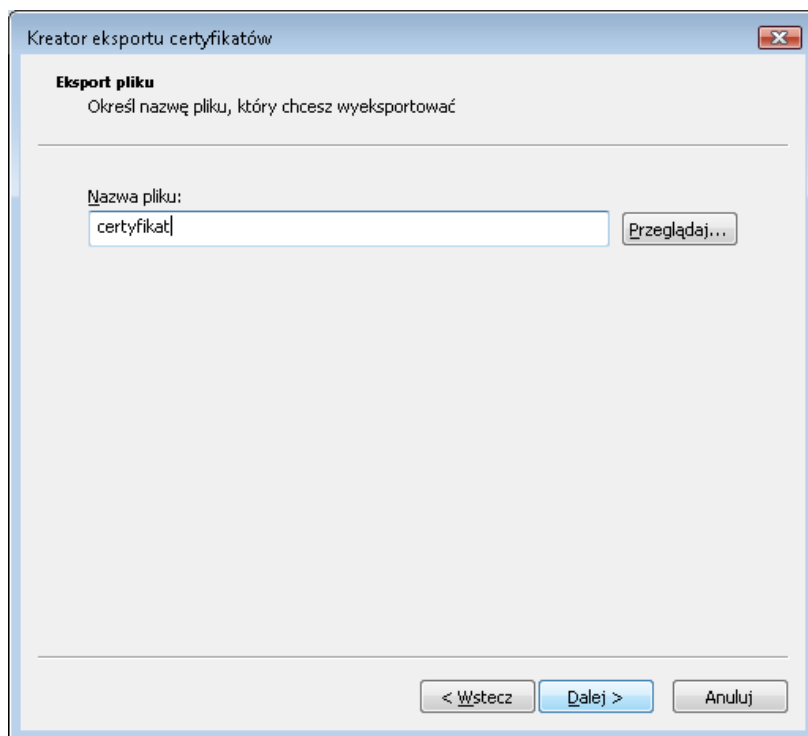
Wpisz i potwierdź hasło.

Hasło:

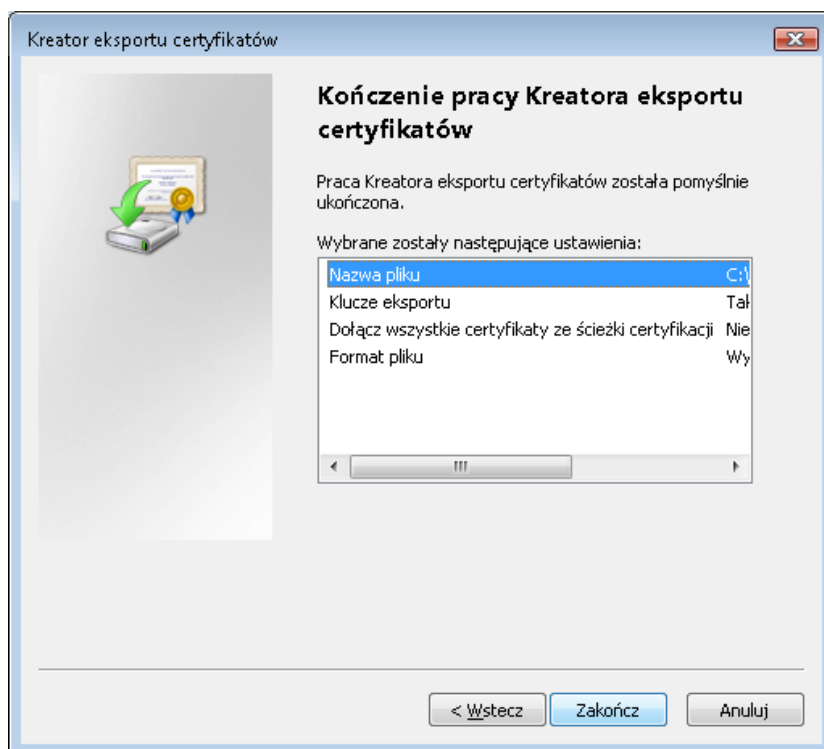
Wpisz i potwierdź hasło (obowiązkowe):

< Wstecz Dalej > Anuluj

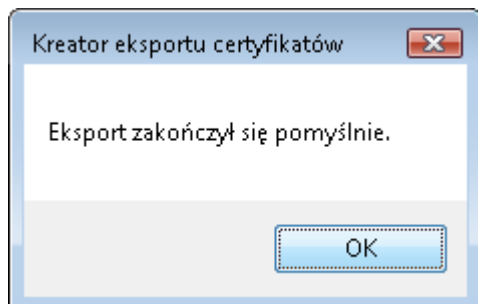
8. Wpisz nazwę pliku do wyeksportowania i wybierz miejsce, w którym ma zostać zapisany (za pomocą przycisku **Przeglądaj**).



9. Naciśnij **Dalej**, a następnie **Zakończ**.



11. Pomyślnie utworzyłeś kopię certyfikatu. Naciśnij **OK**.



9. Spis rysunków

Rysunek 1 - Profil certyfikatu Basic ID.....	3
Rysunek 2 – Instalacja certyfikatu Basic ID.....	4
Rysunek 3 – Instalacja certyfikatu Basic ID – Informacja o instalacji certyfikatu	4
Rysunek 4 – Potwierdzenie wgrania certyfikatu Basic ID.....	5
Rysunek 5 – Profil certyfikatu Basic ID.....	5
Rysunek 6 – Instalacja certyfikatu Basic ID – Informacja o instalacji certyfikatu	6
Rysunek 7 – Prośba o wprowadzenie kodu PIN do Profilu Zwyczajnego karty	6
Rysunek 8 – Potwierdzenie wgrania certyfikatu Basic ID.....	7
Rysunek 9 – Profil certyfikatu Basic ID.....	7
Rysunek 10 – Pobranie certyfikatu Basic ID do pliku	8