Podpis Elektroniczny

Instrukcja instalacji i obsługi

Spis treści

Wstęp

Szanowny Kliencie!
EuroCert ma przyjemność przedstawić Ci niniejszą instrukcję. Załączona karta lub token USB pozwala na złożenie podpisu elektronicznego weryfikowanego certyfikatem kwalifikowanym.
W niniejszym pakiecie startowym znajdują się:

- Karta mikroprocesorowa lub token USB do podpisu elektronicznego
- Płyta CD-ROM zawierająca oprogramowanie do zarządzania certyfikatem

Aktywacja usługi

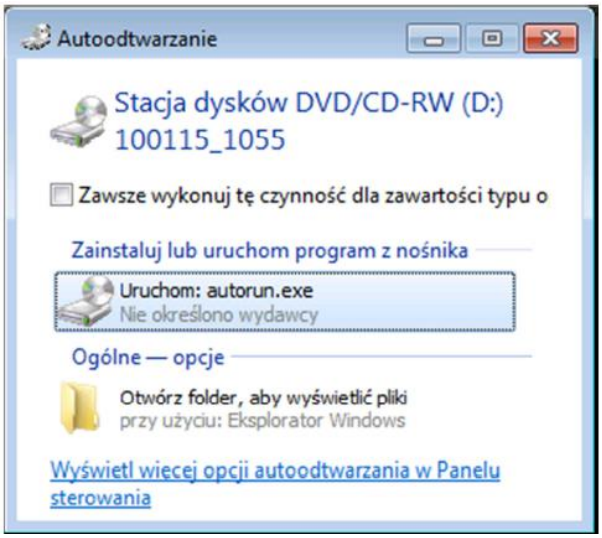
Aby móc korzystać z usługi podpisu elektronicznego wystarczy zainstalować na komputerze oprogramowanie do zarządzania certyfikatem znajdujące się na płycie.

Instalacja aplikacji

Upewnij się, że komputer spełnia poniższe wymagania:

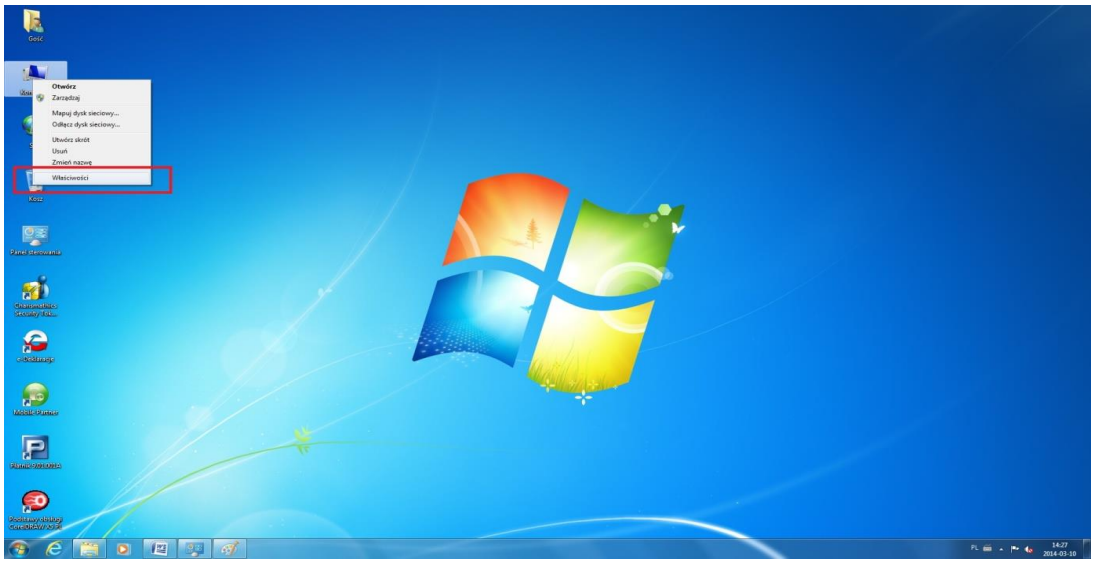
- System operascyjny: Zainstalowana wersja systemu MS Windows 2000, MS Windows XP, MS Windows Vista, MS Windows 7, MS Windows 8,
- Miejsce na twardym dysku 10 MB
- Pamięć RAM 256 MB

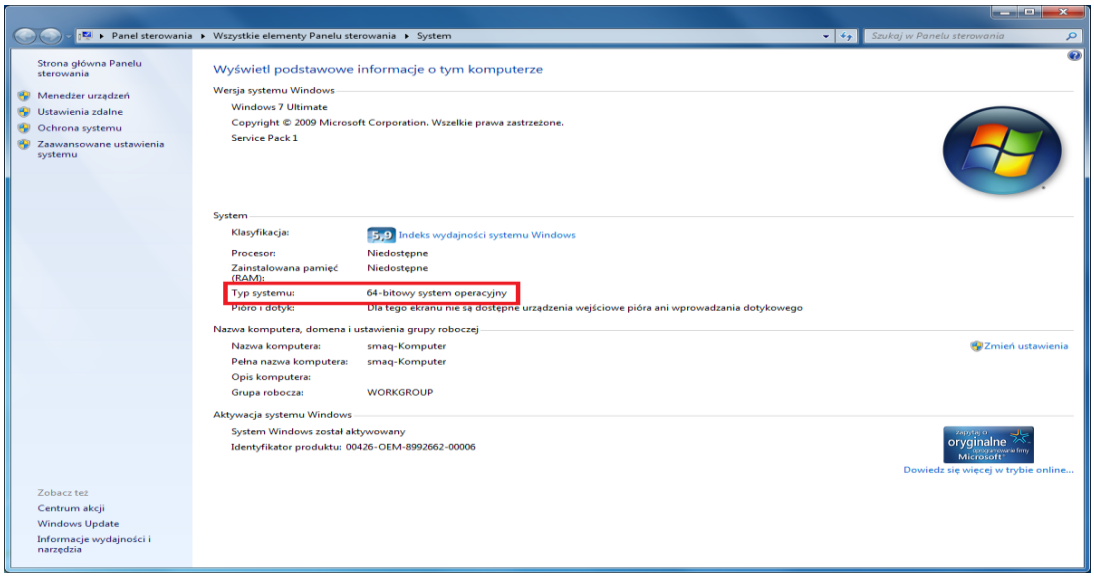
Włącz komputer, włóż do napędu CD-ROM płytę z instalatorem oprogramowania do zarządzania certyfikatem. Wybierz Uruchom:
autorun.exe.



Sprawdź wersję systemu operacyjnego:

Prawym przyciskiem myszy klikamy na **Mój Komputer> Właściwości**



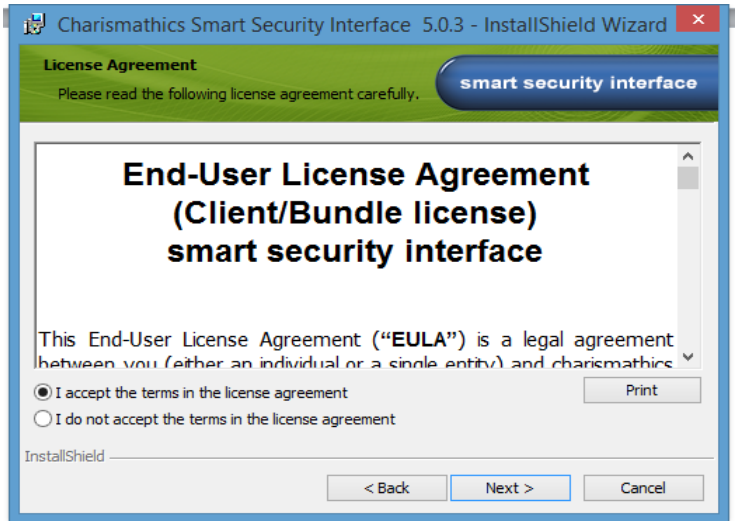


W zależności od wersji system wybierz:

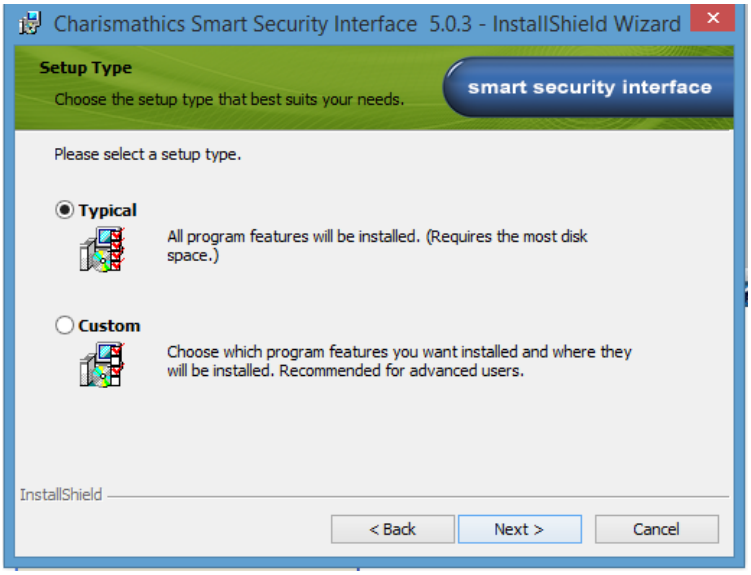
Charismathic 32 bit lub Charismathic 64 bit.

- Widok instalatora programu Charismathics – naciśnij przycisk „Next”

- przejść dalej – potwierdź umowę licencyjną przypisaną do karty lub tokena USB – zaznacz opcję „ I accept the terms in the license agreement” – naciśnij przycisk „Next”



- Wybierz rodzaj instalacji – „Typical" – naciśnij przycisk „Next"

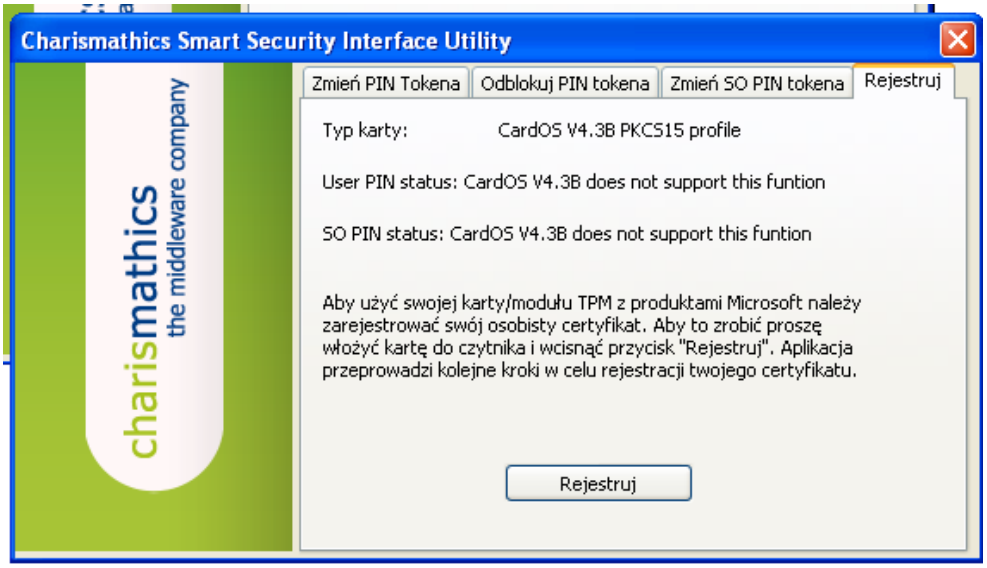


Po zakończeniu instalacji naciśnij przycisk zakończ – „Finisch"

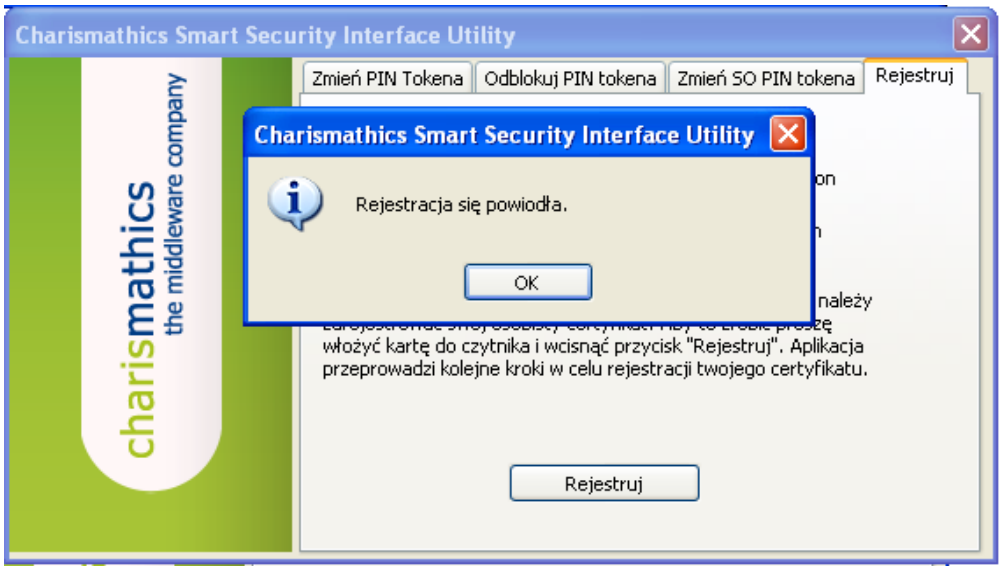
Funkcje

Do uruchomienia karty nie ma potrzeby podawania kodu PIN (znajduje się w bezpiecznej kopercie)

W celu aktywowania podpisu należy umieścić kartę w czytniku oraz podpiąć czytnik (token USB) do komputera, następnie w zakładce „Rejestruj" dokonać rejestracji podpisu.

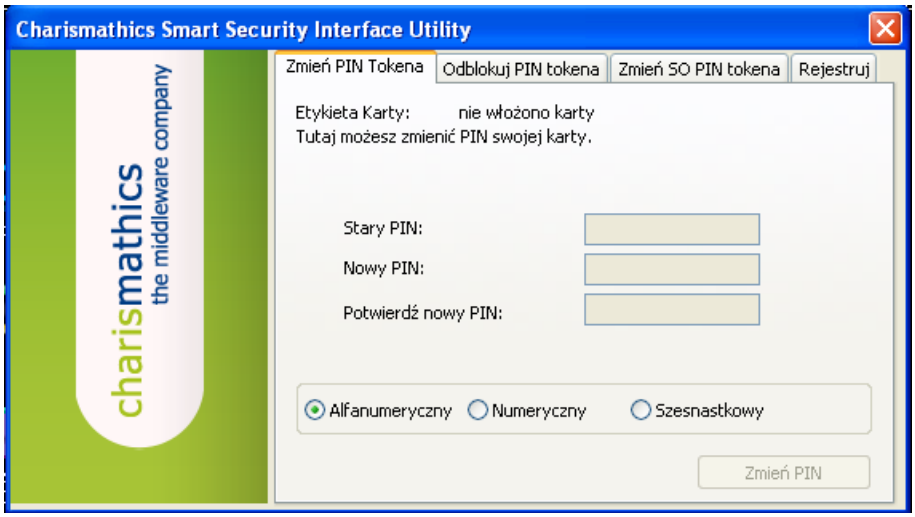


Naciśnij przycisk „Rejestruj”



Certyfikat został poprawnie zarejestrowany w systemie. Można zamknąć oprogramowanie.

Oprogramowanie służy również do zarządzania kartą jak na przykład zmiana kodu PIN



Zakładkę „Odblokuj PIN tokena” używa się w momencie zablokowania kodu PIN.

Do odblokowania PIN-u służy kod PUK umieszczony z kodem PIN w bezpiecznej kopercie.

Instalacja certyfikatów NBP NCCERT oraz EuroCert

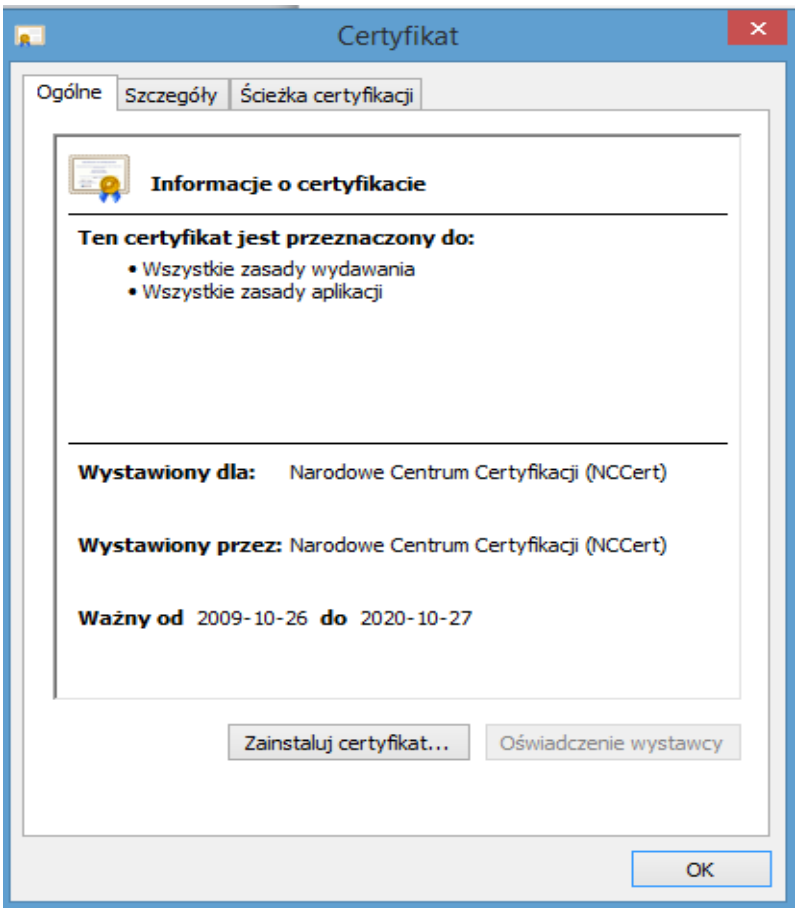
Aby prawidłowo korzystać z podpisu elektronicznego należy zainstalować w magazynie certyfikatów systemu Windows certyfikat Narodowego Banku Polskiego oraz certyfikat EuroCert.

W tym celu z płyty zawierającej oprogramowanie należy wybrać plik z katalogu głównego:

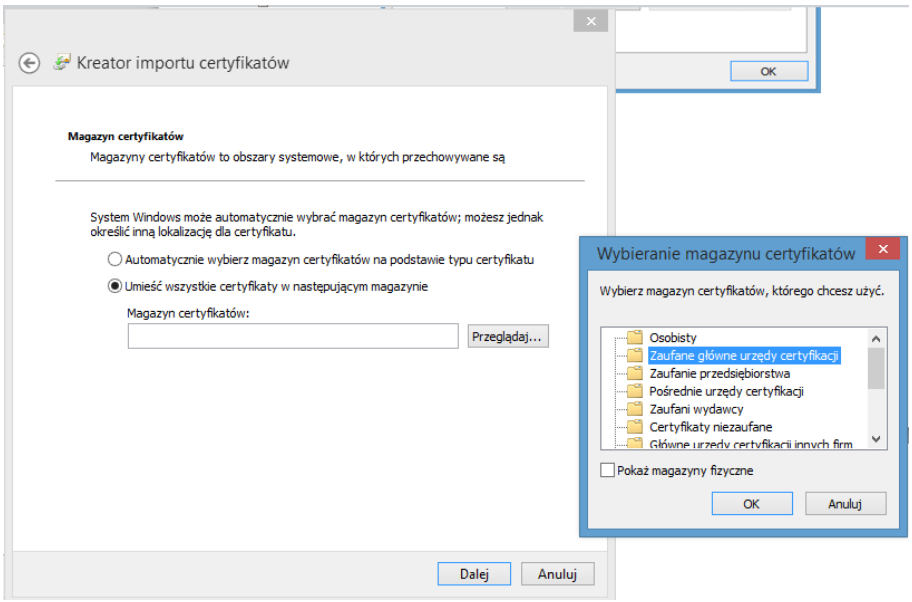
Plik: **certyfikat nccert.crt**

Kreator importu certyfikatów systemu Windows uruchomi się automatycznie.

Naciśnij przycisk „Zainstaluj Certyfikat”



Następnie w ekranie „Magazyn certyfikatów” wskaż opcję „Umieść wszystkie certyfikaty w następującym magazynie”. Wyświetli się okno „Wybieranie magazynu certyfikatów” wskaż „zaufane główne urzędy certyfikacji” i zatwierdź „OK”



Postępuj zgodnie z poleceniami instalatora systemu Windows. Po zakończeniu wyświetli się komunikat o pomyślnym zainstalowaniu certyfikatu w systemie.

Instalacja certyfikatu EuroCert

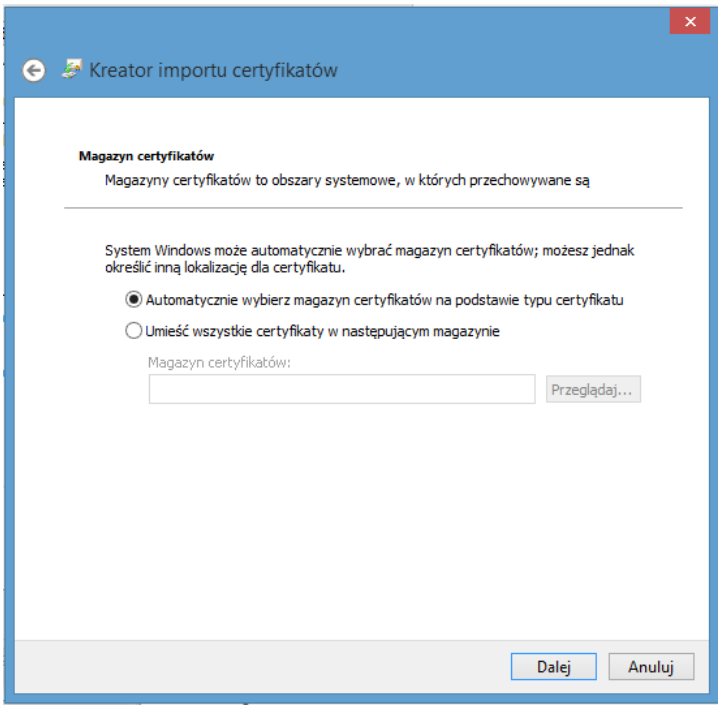
Instalacja certyfikatu EuroCert przebiega podobnie jak instalacja certyfikatu NBP NCCERT.

Aby zainstalować certyfikat Centrum Certyfikacji EuroCert z płyty zawierającej oprogramowanie należy wybrać Certyfikat EuroCert. Plik **Certyfikat Eurocert_QCA_2014.crt**

Kreator instalacji certyfikatów systemu Windows uruchomi się automatycznie.

Naciśnij przycisk „Zainstaluj Certyfikat”

Następnie w ekranie „Magazyn certyfikatów” wskaż opcję „Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu” i naciśnij „Dalej”.



Postępuj zgodnie z poleceniami instalatora systemu Windows. Po zakończeniu wyświetli się komunikat o pomyślnym zainstalowaniu certyfikatu w systemie.

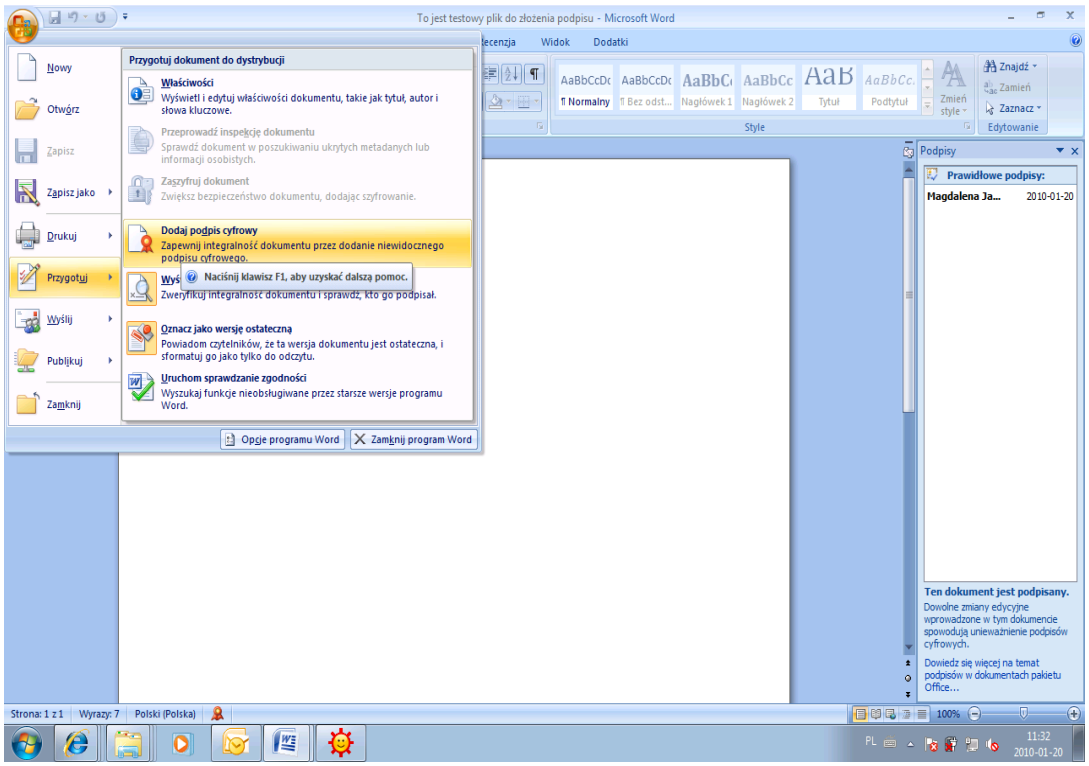
Korzystanie z certyfikatu kwalifikowanego

Po zainstalowaniu oprogramowania AuthentIC Manager można składać podpis elektroniczny pod dokumentami. Na Twoim komputerze został zainstalowany certyfikat kwalifikowany. Aplikacje takie

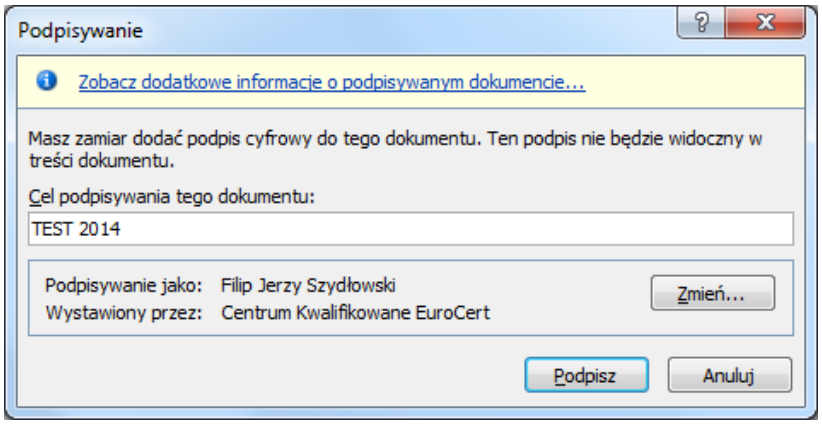
jak Płatnik wywołują zainstalowany certyfikat podczas złożenia podpisu elektronicznego. Proces podpisu wygląda następująco:

1. Otwieramy dokument, który chcemy podpisać certyfikatem kwalifikowanym.

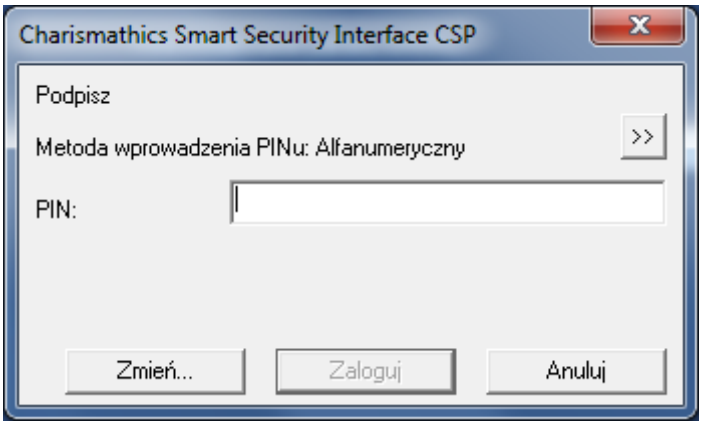
2. Wybieramy opcje „Przygotuj”-> „Dodaj podpis cyfrowy”



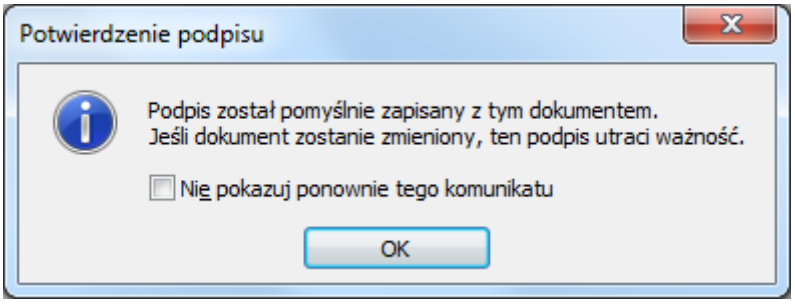
3. Pojawia się okno, w którym możemy wybrać certyfikat w celu podpisania.



4. Program poprosi nas o podanie hasła (PIN)



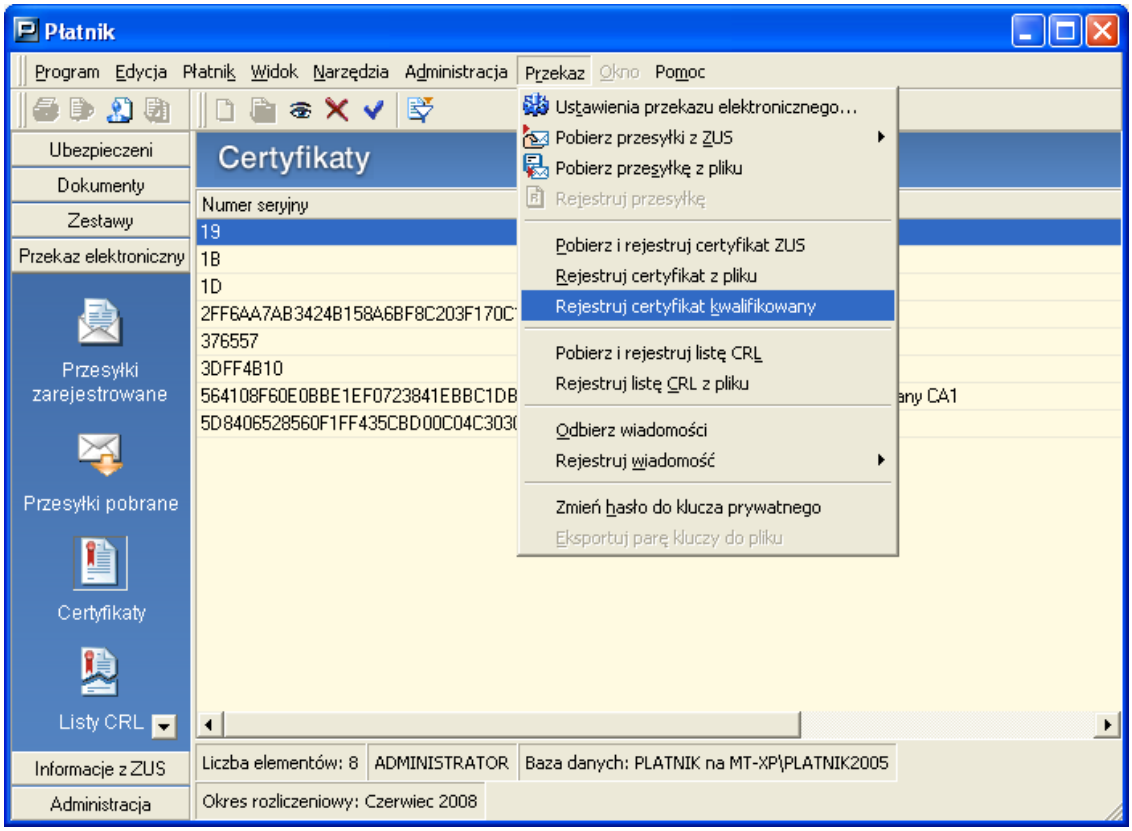
5. Po wprowadzeniu PIN do klucza prywatnego na karcie na ekranie wyświetla się komunikat o złożeniu podpisu elektronicznego



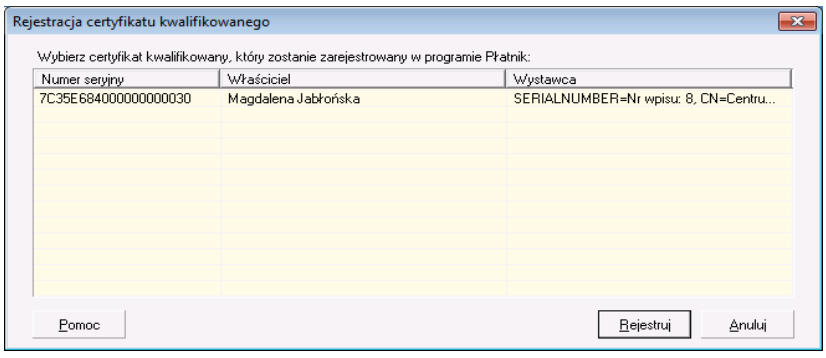
Konfiguracja programu Płatnik

Mobilny ePodpis może być wykorzystywany w programie Płatnik do komunikacji z ZUSem. W celu skonfigurowania tego programu należy wykonać następujące kroki:

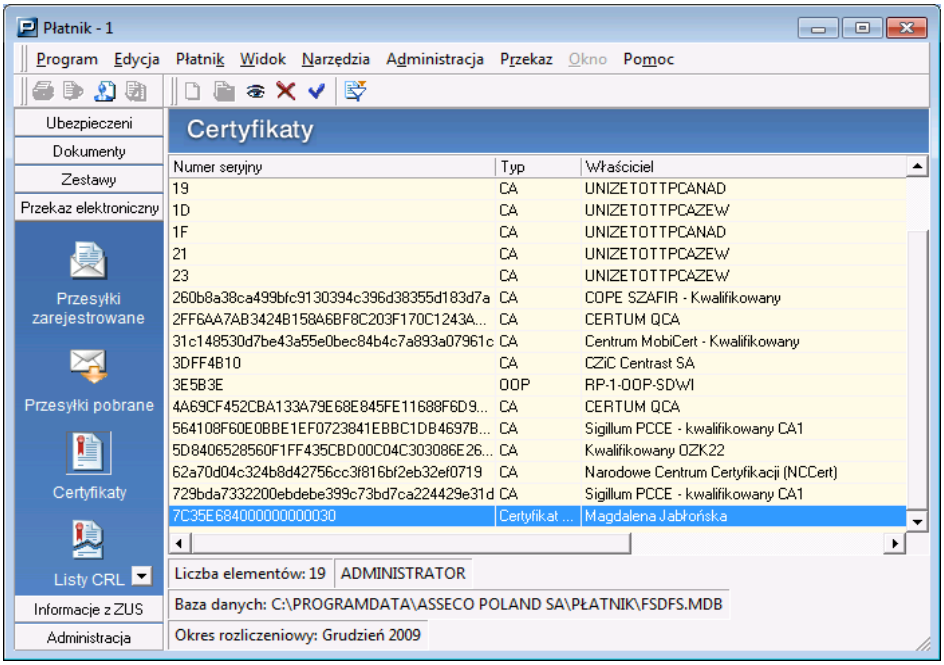
1. Po uruchomieniu programu należy wybrać z menu **Przekaz** > **Rejestruj certyfikat kwalifikowany**.



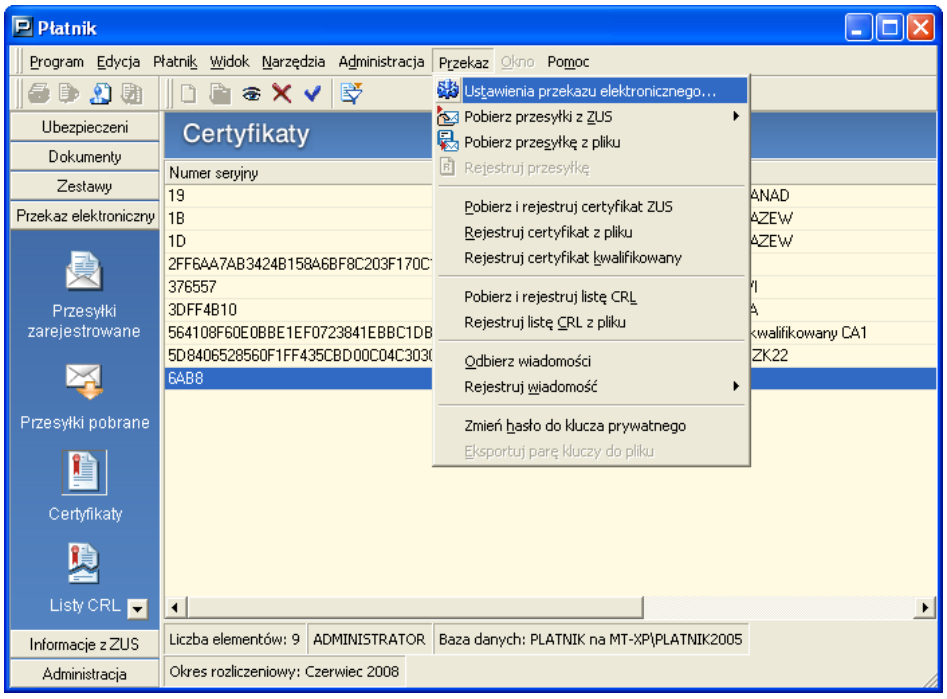
2. Wybieramy kwalifikowany certyfikat użytkownika, a następnie **Rejestruj**.



3. Zarejestrowany certyfikat możemy obejrzeć w zakładce **Przekaz elektroniczny** > **Certyfikaty.**

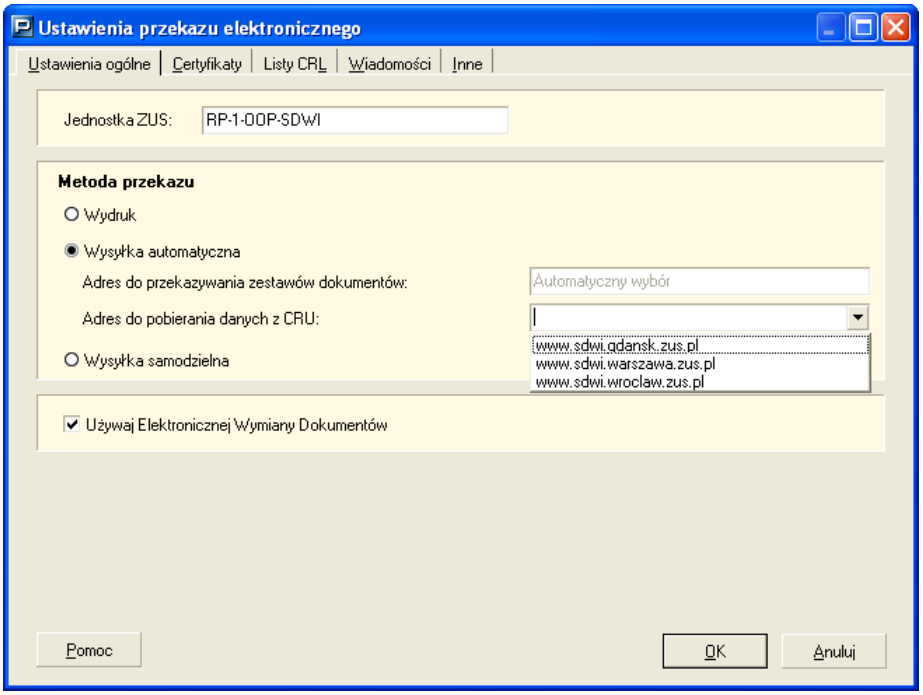


4. Następnie w menu wybieramy **Przekaz** > **Ustawienia przekazu elektronicznego...**

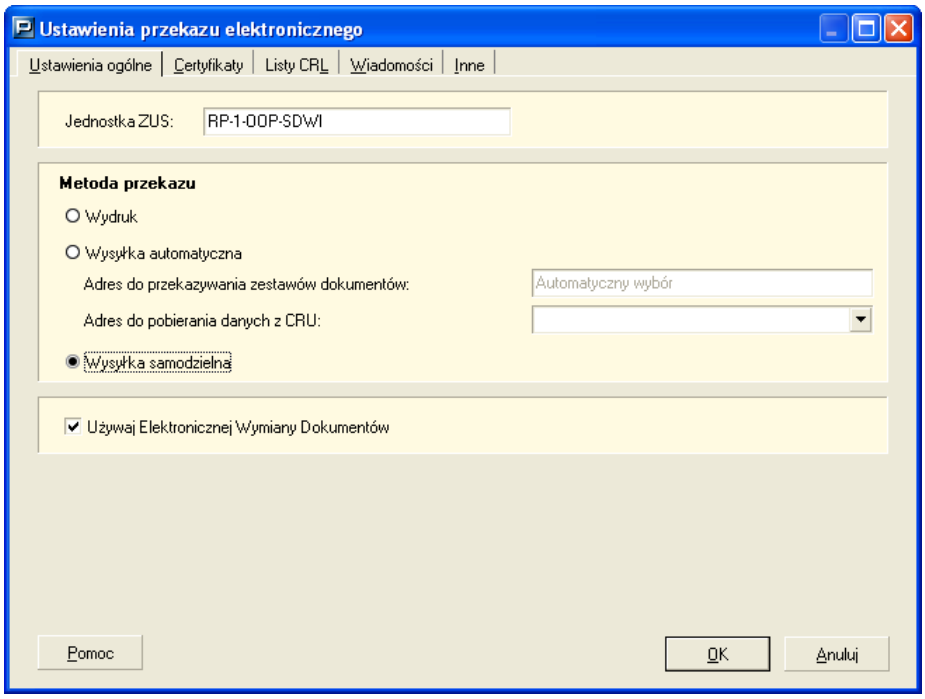


5. Wybieramy zakładkę **Ustawienia ogólne.** W okienku **Metoda przekazu** wybieramy:

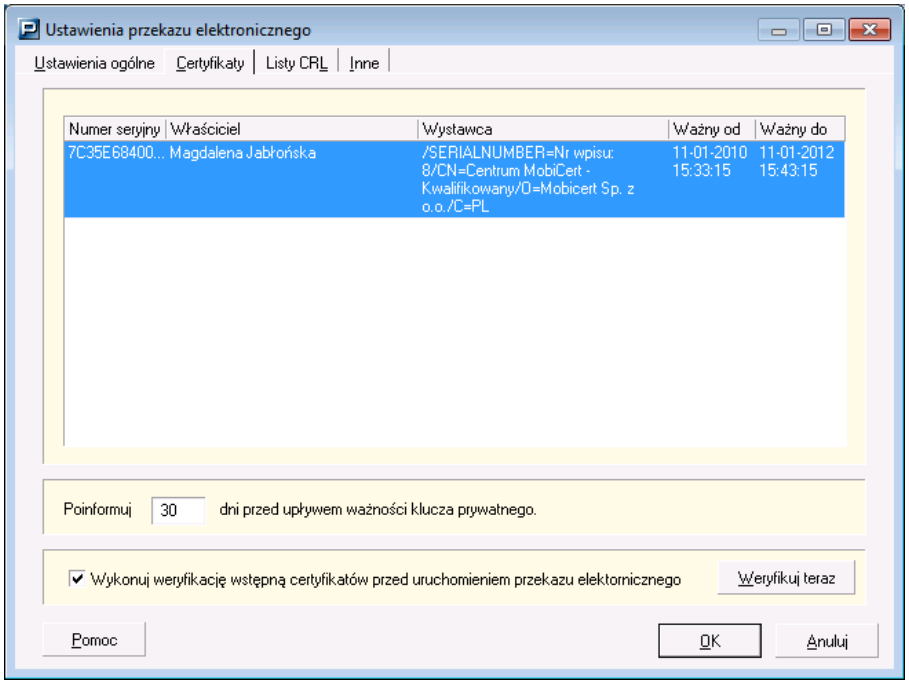
a) **Wysyłka automatyczna**, oraz właściwy oddział ZUSu.



b) lub **Wysyłka samodzielna**.



6. Na koniec wybieramy zakładkę **Certyfikaty** i zaznaczamy opcję **Do elektronicznej komunikacji z ZUS w zakresie przekazywania dokumentów ubezpieczeniowych wykorzystywany będzie wskazany certyfikat kwalifikowany (dwukrotne kliknięcie otwiera okno certyfikatu).**
   Aby zapisać ustawienia wybieramy **OK.**



Zagadnienia prawne

- Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. nr 130, poz. 1450), jeżeli został złożony w okresie ważności tego certyfikatu.
- Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi,
- Bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie, jako osobę składającą podpis.
- Zasady wydawania, zawieszania i unieważniania certyfikatów kwalifikowanych i niekwalifikowanych oraz zakres i ograniczenia stosowania certyfikatów określone są szczegółowo w dokumentach „Polityka certyfikacji dla certyfikatów kwalifikowanych” udostępnianych w Internecie pod adresem http://www.mobicert.pl/dokumenty/KW_02_Polityka_Certyfikacji.pdf