



proCertum  
**SecureSign**



WERSJA 2.3

# PODRĘCZNIK UŻYTKOWNIKA

Styczeń 2006

# SPIS TREŚCI

<b>WAŻNE INFORMACJE .....</b>	<b>3</b>
<b>WSTĘP .....</b>	<b>4</b>
<b>JAK KORZYSTAĆ Z DOKUMENTACJI .....</b>	<b>5</b>
<b>WYMAGANIA SPRZĘTOWE I SYSTEMOWE .....</b>	<b>6</b>
<b>1. KONFIGURACJA APLIKACJI.....</b>	<b>7</b>
1.1.    MAGAZYN.....	7
1.2.    SECURESIGN .....	8
1.3.    PROXY .....	10
1.4.    JĘZYK .....	10
<b>2. USTAWIENIA PLIKU MAGAZYNU.....</b>	<b>11</b>
2.1.    ZAUFANE PUNKTY.....	11
2.2.    ZAUFANE POLITYKI CERTYFIKACJI.....	11
2.3.    LISTY UNIEWAŻNIEŃ (CRL).....	12
2.4.    OCSP .....	12
2.5.    ZNACZNIK CZASU .....	13
<b>3. SKŁADANIE PODPISU ELEKTRONICZNEGO.....</b>	<b>14</b>
3.1.    URUCHOMIENIE PROGRAMU proCERTUM SECURESIGN .....	14
3.2.    PROCES SKŁADANIA PODPISU ELEKTRONICZNEGO .....	15
3.2.1. <i>Wybór dokumentu do podpisu .....</i>	<i>15</i>
3.2.2. <i>Dodawanie opisu dokumentu do podpisu.....</i>	<i>16</i>
3.2.3. <i>Przeglądanie dokumentu przygotowanego do podpisu .....</i>	<i>17</i>
3.2.4. <i>Wybór typu podpisu (wewnętrzny lub zewnętrzny).....</i>	<i>18</i>
3.2.5. <i>Weryfikacja poprawności przygotowania dokumentu do podpisu .....</i>	<i>19</i>
3.2.6. <i>Wybór certyfikatu.....</i>	<i>20</i>
3.2.7. <i>Złożenie podpisu.....</i>	<i>21</i>
3.2.8. <i>Przegląd zawartości podpisu .....</i>	<i>23</i>
3.2.9. <i>Podpisanie kolejnego dokumentu.....</i>	<i>24</i>
3.2.10. <i>Zakończenie pracy programu proCertum SecureSign.....</i>	<i>24</i>
<b>4. SKUTKI PRAWNE PODPISU ELEKTRONICZNEGO .....</b>	<b>25</b>
<b>5. PODSTAWOWE DEFINICJE I SKRÓTY .....</b>	<b>27</b>

## Ważne informacje

### ***Tryb bezpieczny***

Aplikacja proCertum SecureSign pracuje w trybie bezpiecznym wtedy, gdy w aplikacji służącej do konfiguracji ustawień – proCertum ClientSettings w zakładce „Podpis” włączona jest opcja „Kwalifikowany podpis”. Oprogramowanie proCertum SecureSign jest wtedy częścią bezpiecznego urządzenia do składania podpisu elektronicznego i złożony nim podpis elektroniczny zgodnie z ustawą z dnia 18 września 2001r. o podpisie elektronicznym będzie wywoływać skutki prawne równoważne podpisowi własnoręcznemu.

#### **UWAGA**

Oprogramowanie w trybie bezpiecznym współpracuje tylko z dedykowanymi kartami kryptograficznymi, które chronią klucz prywatny w profilu bezpiecznym. Użycie tego klucza oprócz podania PIN, wymaga również uwierzytelniania oprogramowania podpisującego.

#### **OSTRZEŻENIE**

Osoba składająca podpis powinna być pewna, że stanowisko komputerowe jest pod wyłączną jej kontrolą, to znaczy, że podczas działania niniejszego oprogramowania osoba postronna nie ma żadnej możliwości (np. poprzez sieć lub zainfekowanie wirusem) oddziaływania na pracę komputera.

### **Tryb zwykły**

Aplikacja proCertum SecureSign pracuje w trybie zwykłym wtedy, gdy w aplikacji służącej do konfiguracji ustawień – proCertum ClientSettings w zakładce „Podpis” wyłączona jest opcja „Kwalifikowany podpis”.

#### **UWAGA**

Oprogramowanie w trybie zwykłym współpracuje z wieloma popularnymi na rynku kartami, które nie zabezpieczają w sposób szczególny przed użyciem klucza prywatnego przez nieuwierzytelnione oprogramowanie podpisujące (po podaniu kodu PIN może dojść do użycia klucza - zrealizowania podpisu - poza kontrolą osoby podpisującej).

#### **OSTRZEŻENIE**

Osoba składająca podpis powinna być pewna, że stanowisko komputerowe jest pod wyłączną jej kontrolą, to znaczy, że podczas działania niniejszego oprogramowania osoba postronna nie ma żadnej możliwości (np. poprzez sieć lub zainfekowanie wirusem) oddziaływać na pracę komputera.

## WSTĘP

Aplikacja **proCertum SecureSign** służy do składania podpisu elektronicznego i może być elementem **bezpiecznego urządzenia do składania podpisu elektronicznego** w myśl Ustawy o podpisie elektronicznym z dnia 18 września 2001r.

Aplikacja **proCertum SecureSign** jest częścią **Bezpiecznego urządzenia do składania podpisu elektronicznego Suscriptor Q 01** wtedy, gdy współpracuje z kartą kryptograficzną **cryptoCertum**, która jest komponentem technicznym spełniającym wymagania normy ITSEC E4 High.

Dodatkowo aplikacja **proCertum SecureSign** może wykorzystywać w procesie składania kwalifikowanego podpisu elektronicznego moduł uwierzytelniający SAM (Secure Application Module).

Aplikacja **proCertum SecureSign** działająca w trybie bezpiecznym służy do składania bezpiecznego podpisu elektronicznego w środowisku niepublicznym, takim jak dom, biuro, etc., w którym dostęp do oprogramowania podpisującego w normalnych warunkach eksploatacji ma ściśle określona grupa użytkowników.

**W momencie składania bezpiecznego podpisu  
całość bezpiecznego urządzenia do składania podpisu elektronicznego  
(oprogramowanie i komponent techniczny)  
musi być pod wyłączną kontrolą podpisującego  
(zgodnie z Art.3, Ust.2, pkt. b Ustawy o podpisie elektronicznym).**

Aplikacja **proCertum SecureSign**:

- tworzy podpisy elektroniczne w formacie ETSI – (Electronic Signature Format, określony przez European Telecommunications Standards Institute),
- tworzy podpisy zgodnie z polityką podpisu,
- spełnia wymogi stawiane programowi podpisującemu, określone w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128 poz.1094 z dnia 12 sierpnia 2002 r.).

## Jak korzystać z dokumentacji

Konsekwentne stosowanie w dokumencie różnego rodzaju oznaczeń, jak wyróżnienia w tekście, sposoby zapisu klawiszy, elementy graficzne, a także jednolita terminologia ułatwiają poszukiwanie i zrozumienie potrzebnych informacji. Poniżej przedstawiono stosowane oznaczenia, symbole graficzne i przyjęte konwencje opisu klawiszy oraz wyjaśniono ich znaczenie.


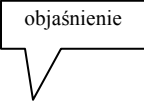
### Stosowane style czcionek

Nazwy poszczególnych elementów aplikacji (takich jak okna, przyciski, komunikaty) są wyróżniane stylem czcionki:

Styl czcionki	Znaczenie
<i>Rejestracja listy CRL</i>	Oznaczenie nazwy okna.
<b>Start</b>	Oznaczenie polecenia w menu oraz przycisków na pasku narzędzi.
<b>Zapisz</b>	Oznaczenie przycisku.
Czy podpisać istniejący katalog?	Tekst komunikatu aplikacji.

### Stosowane symbole

W dokumencie stosowane są też następujące symbole graficzne:

Symbol	Znaczenie
	Uwaga bardzo ważna dla realizacji zadania z punktu widzenia aplikacji lub z przyczyn merytorycznych.
	Objaśnienie wskazanego elementu

## WYMAGANIA SPRZĘTOWE I SYSTEMOWE


Minimalne wymagania sprzętowo-systemowe umożliwiające prawidłową i bezpieczną pracę z aplikacją do składania bezpiecznego podpisu elektronicznego **proCertum SecureSign**, to:

- procesor Pentium© 100 Mhz,
- 64 MB pamięci operacyjnej,
- minimum 25 MB wolnej przestrzeni dyskowej przed instalacją aplikacji,
- przeglądarka Internet Explorer 5.5x (siła szyfrowania 128 bitowa),
- skonfigurowane połączenie internetowe - wymagane jest tylko w przypadku wykorzystywania polityk podpisu oznaczających dodatkowo dokument czasem przed podpisaniem,
- monitor i karta graficzna o rozdzielczości min. 800 x 600 pikseli,
- system operacyjny Microsoft Windows NT/2000/XP,
- czytnik kart kryptograficznych,
- karta z kryptoprocesorem,
- moduł uwierzytelniający SAM (opcjonalnie),
- oprogramowanie sterujące pracą czytnika.

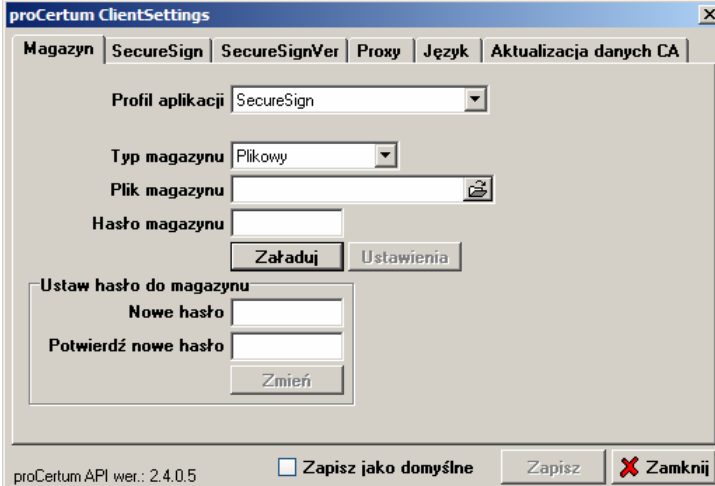
## 1. Konfiguracja aplikacji

Dla zapewnienia poprawnego działania aplikacji **proCertum SecureSign** należy przed rozpoczęciem procesu składania podpisu odpowiednio zdefiniować parametry pracy aplikacji. Do konfigurowania używana jest dodatkowa aplikacja **proCertum ClientSettings**, która jest instalowana razem z aplikacją **proCertum SecureSign**.

Aplikacja **proCertum Client Settings** jest narzędziem umożliwiającym skonfigurowanie kilku aplikacji linii „proCertum”. Dlatego też nie zawsze konieczne jest definiowanie parametrów zawartych we wszystkich zakładkach. Poniżej opisano zawartość zakładek, których odpowiednie skonfigurowanie jest niezbędne do poprawnego działania aplikacji **proCertum SecureSign**.

	<p>Ustawienia zawarte w zakładkach, które nie zostały opisane nie są wykorzystywane przez aplikację <b>proCertum SecureSign</b>.</p> <p>Kliknięcie „<b>Zamknij</b>” powoduje wyjście z aplikacji <b>proCertum ClientSettings</b> bez zmian w pokazanych ustawieniach i zakończenie procedury ustawień, natomiast jeżeli wprowadzone zostały jakieś zmiany to kliknij przycisk „<b>Zapisz</b>”, żeby aplikacja je zapamiętała.</p>
---	---


### 1.1. Magazyn



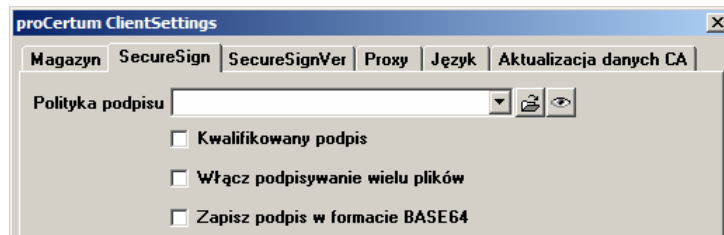
The screenshot shows the 'proCertum ClientSettings' window with the 'Magazyn' tab selected. The interface includes the following elements:

- Navigation tabs: Magazyn, SecureSign, SecureSignVer, Proxy, Język, Aktualizacja danych CA.
- Profil aplikacji: SecureSign (dropdown menu).
- Typ magazynu: Plikowy (dropdown menu).
- Plik magazynu: [empty text field] with a file selection icon.
- Hasło magazynu: [empty password field].
- Buttons: Załaduj, Ustawienia.
- Section: Ustaw hasło do magazynu.
  - Nowe hasło: [empty password field].
  - Potwierdź nowe hasło: [empty password field].
  - Button: Zmień.
- Footer: proCertum API ver.: 2.4.0.5,  Zapisz jako domyślne, Zapisz, Zamknij.

W tej zakładce można zdefiniować z jakiego typu magazynu korzysta wybrana aplikacja, jaki jest plik magazynu oraz zmienić hasło i wewnętrzne ustawienia pliku magazynu.


	<p>Należy pamiętać, że ustawienia magazynu przechowywane są osobno dla każdej obsługiwanej aplikacji. Z tegoż powodu, ażeby skonfigurować ustawienia dla <b>proCertum SecureSign</b>, należy wybrać profil aplikacji „SecureSign”.</p>
---	--

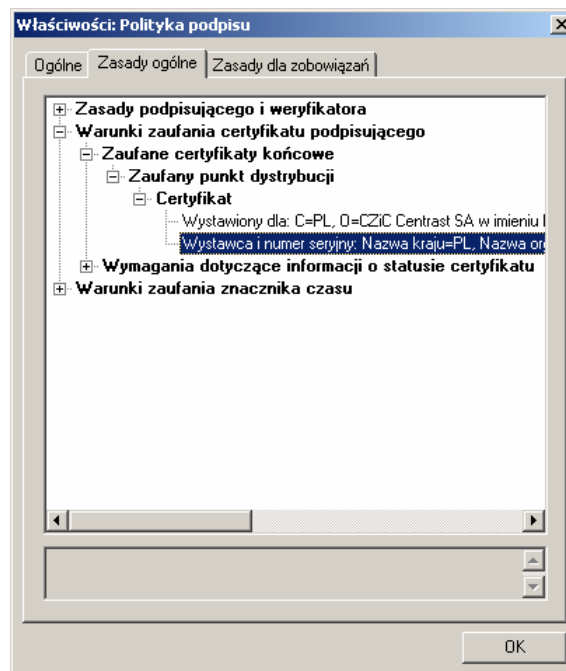
## 1.2. SecureSign




Zakładka – „Podpis”, zawiera następujące ustawienia:

- **Polityka podpisu,**

W tym polu można zapoznać się z aktualną lub zdefiniować nową lokalizację polityki podpisu. W celu przeglądnięcia szczegółowych informacji opisujących wybraną politykę podpisu należy kliknąć na przycisk . Okno zawierające informacje o polityce podpisu wygląda następująco:



Należy sprawdzić, na jakie zaświadczenie certyfikacyjne wskazuje wybrane w powyższym oknie pole „Wystawca i numer seryjny”. Następnie należy zdecydować, czy ufamy temu punktowi zaufania.

	<p>W przypadku podpisu kwalifikowanego należy sprawdzić, czy wybrane w powyższym oknie pole: „Wystawca i numer seryjny” wskazuje na zaświadczenie certyfikacyjne kwalifikowanego podmiotu świadczącego usługi certyfikacyjne. W warunkach polskich jest to: Narodowe Centrum Certyfikacji (zaświadczenie certyfikacyjne dostępne jest pod adresem URL: <a href="http://www.centrast.pl/ncc/lista_wydanych/lista_wyd.aspx">http://www.centrast.pl/ncc/lista_wydanych/lista_wyd.aspx</a>). Posiadając certyfikat kwalifikowany wystawiony przez Narodowe Centrum Certyfikacji można składać podpisy kwalifikowane w myśl art. 5. Ustawy o podpisie elektronicznym z dnia 18 września 2001 r. (Dz.U. z 2001 r. Nr 130).</p>
---	--

Użytkownik ma do dyspozycji następujące polityki podpisu instalowane wraz z aplikacją:

- cck002.spol – umożliwia złożenie podpisu bezpiecznego,
- cck0021.spol – umożliwia złożenie podpisu bezpiecznego wraz z dodatkowym opisem,
- cck006.spol – umożliwia złożenie podpisu przy wykorzystaniu certyfikatu powszechnego CERTUM.
- cck010.spol – umożliwia oznaczenie dokumentu czasem przed złożeniem podpisu bezpiecznego przy wykorzystaniu serwera znacznika czasu - <http://time.certum.pl>.

Szczegółowy opis każdej z polityk dostępny jest w oknie „**Właściwości: Polityka podpisu**”.

- skonfigurowane połączenie internetowe - wymagane jest tylko w przypadku wykorzystywania polityk podpisu oznaczających dodatkowo dokument czasem przed podpisaniem.

- **Kwalifikowany podpis,**

Zaznaczenie tej opcji spowoduje uruchomienie aplikacji w trybie bezpiecznym. W aplikacji wyświetlane będą tylko te certyfikaty, które znajdują się na karcie kryptograficznej w tzw. profilu dedykowanym (bezpiecznym).

Gdy opcja „**Kwalifikowany podpis**” zostanie wyłączona, aplikacja przejdzie w tryb zwykły i będzie umożliwiać użytkownikowi skorzystanie z certyfikatów zawartych na karcie w profilu powszechnym oraz znajdujących się w magazynach systemowych.

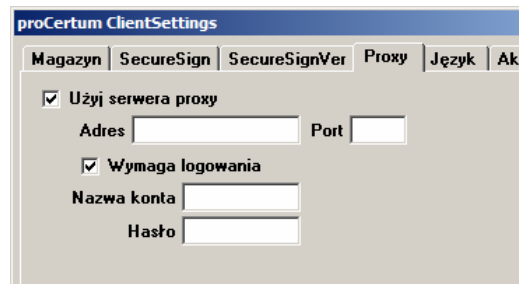
- **Włącz podpisywanie wielu plików,**

Przez włączenie tej opcji użytkownik będzie miał możliwość podpisania wielu plików w jednej sesji. Jednak w przypadku, gdy aplikacja będzie pracować w profilu bezpiecznym, użytkownik ze względów bezpieczeństwa będzie musiał podawać PIN do karty podczas podpisywania każdego pliku.

- **Zapisz podpis w formacie BASE64.**

**Konwersja BASE64**, technika kodowania polegająca na przekształcaniu dowolnych danych dwójkowych na dane złożone z 65 znaków (w tym jeden znak służący do dopełniania) nadających się do wydrukowania, stosowana w systemach PEM i PGP. Kod radix-64 jest powszechnie stosowany w załącznikach pocztowych jako tzw. format BASE 64.

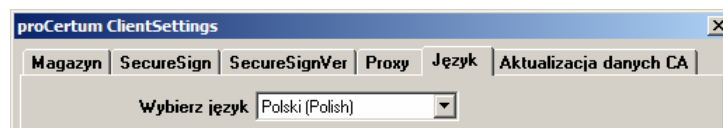
### 1.3. Proxy



W celu skonfigurowania serwera proxy należy zaznaczyć opcję **Użyj serwera proxy** głównym oknie aplikacji **proCertum ClientSettings**, a następnie podać adres IP oraz numer portu. Jeżeli obsługa proxy wymaga indywidualnego logowania to należy podać nazwę konta a następnie hasło

### 1.4. Język

Aplikacja **proCertum SecureSign** można pracować w wielu językach. Lista języków widoczna w ustawieniach zależy jest od plików językowych dostarczanych razem z aplikacją.

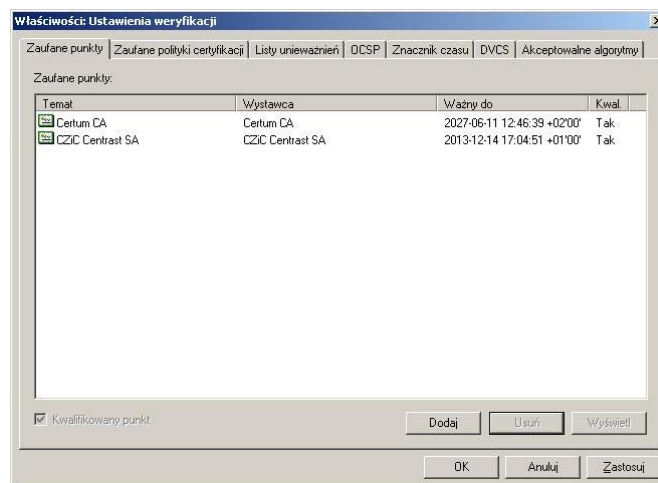


## 2. Ustawienia pliku magazynu

W zakładce „Magazyn” jest możliwość otworzenia okna ustawień pliku magazynu poprzez naciśnięcie przycisku „Ustawienia” załadowawszy magazyn. Są to ustawienia bibliotek **proCertum API**, które wykonują proces weryfikowania.

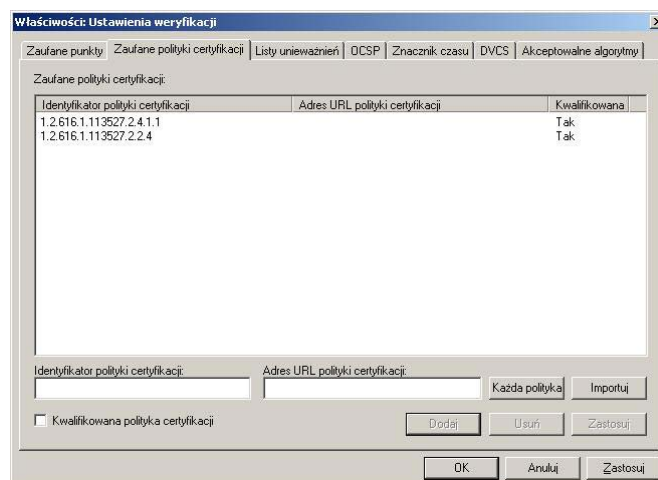
### 2.1. Zaufane punkty

Lista certyfikatów zaufanych wydawców. Jeśli wydawca nie znajduje się na tej liście, wtedy nie ma możliwości pomyślnego zweryfikowania podpisu w trybie weryfikacji kwalifikowanej. Domyślne ustawienie to Narodowe Centrum Certyfikacji oraz Unizeto Technologies SA.



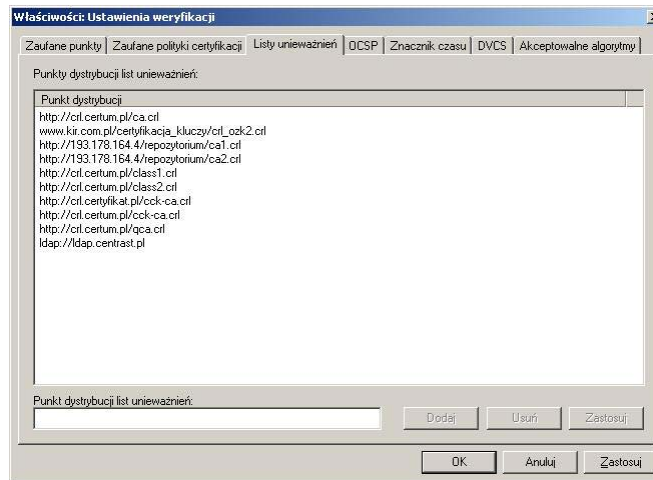
### 2.2. Zaufane polityki certyfikacji

Są to identyfikatory dozwolonych polityk, które mogły zostać użyte podczas wystawiania certyfikatu kwalifikowanego. Aby dany certyfikat mógł być zweryfikowany w trybie kwalifikowanym, identyfikator polityki musi znajdować się na tej liście.



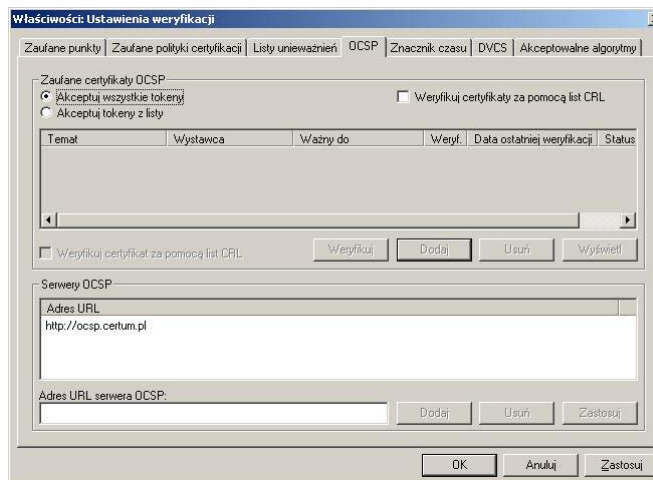
## 2.3. Listy unieważnień (CRL)

Definiowanie adresów URL list unieważnionych certyfikatów.



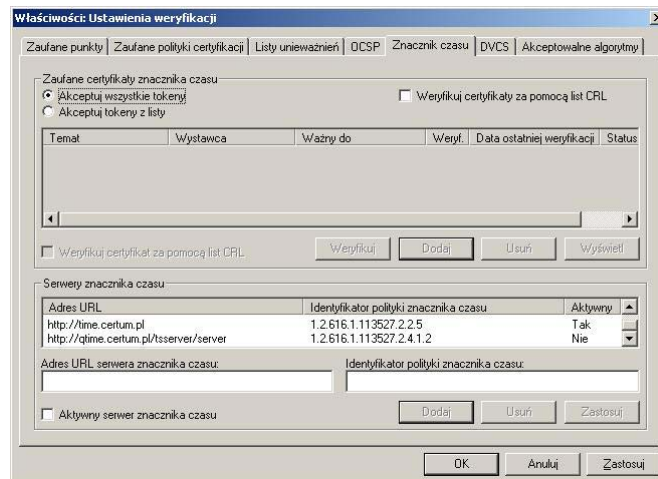
## 2.4. OCSP

Zakładka umożliwia definiowanie adresów serwerów OCSP (Online Certificate Status Protocol).



## 2.5. Znacznik Czasu

Zakładka ta zawiera pola, w których można zdefiniować adres serwera znacznika czasu oraz identyfikator polityki znacznika czasu, do której się odwołujesz.



### 3. SKŁADANIE PODPISU ELEKTRONICZNEGO


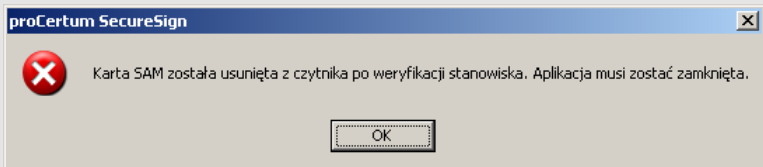
#### 3.1. URUCHOMIENIE PROGRAMU proCertum SecureSign

Jeżeli komunikacja z kartą przebiegła prawidłowo i znajduje się na niej certyfikat kwalifikowany, to można wówczas przystąpić do składania bezpiecznego podpisu elektronicznego na dokumencie.

W tym celu uruchomić należy aplikację poprzez wybranie **proCertum SecureSign** z menu **Programy** ⇒ **Unizeto** ⇒ **proCertum SecureSign**. Aplikację można także uruchomić poprzez skrót **proCertum SecureSign** znajdujący się na pulpicie.

W wyniku uwierzytelnienia pomiędzy oprogramowaniem a komponentem technicznym zostaje ustanowiony klucz sesyjny, wykorzystywany później do zbudowania bezpiecznego kanału.

#### UWAGA!

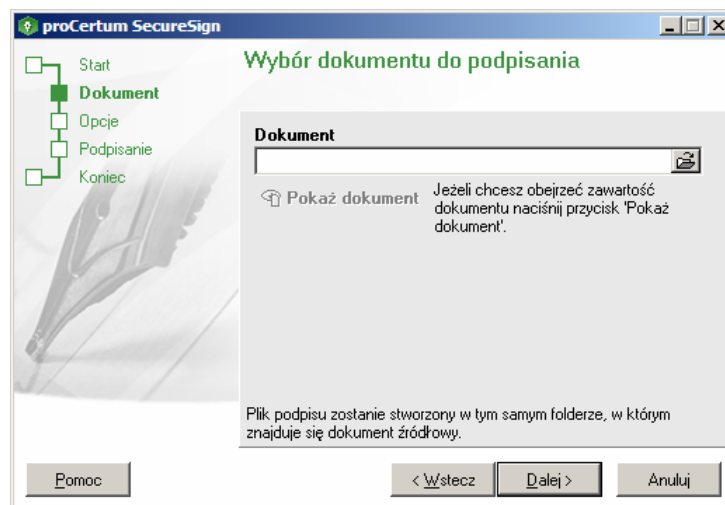
	<p>Jeżeli aplikacja proCertum SecureSign pracuje w trybie bezpiecznym i używamy wersji karty kryptograficznej z modułem uwierzytelniającym SAM, to ten moduł po włożeniu do portu USB musi pozostać tam aż do końca procesu składania podpisu elektronicznego. Jeżeli moduł ten zostanie usunięty z portu USB w trakcie procesu, złożenie podpisu będzie niemożliwe i nastąpi zamknięcie procesu składania podpisu. Należy wtedy ponownie umieścić moduł uwierzytelniający SAM w porcie USB i uruchomić oprogramowanie proCertum SecureSign.</p> <div style="text-align: center;">  </div> <p>W przypadku używania karty bez modułu uwierzytelniającego, po weryfikacji aplikacji przejdziemy od razu do ekranu początkowego aplikacji.</p>
---	---

Po weryfikacji stanowiska do bezpiecznego składania podpisu elektronicznego pojawi się ekran powitalny programu. W zależności od ustawień aplikacji interfejs początkowy będzie się różnić. Interfejs początkowy zależy od tego czy w ustawieniach aplikacji zostało nadane hasło dostępu do magazynu.

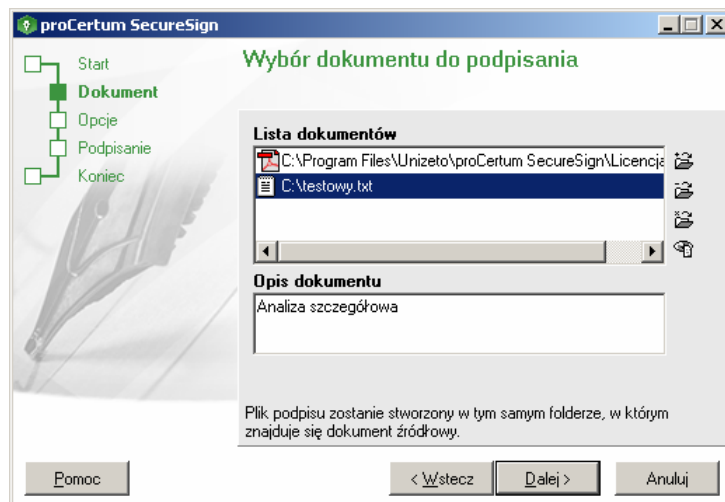
## 3.2. PROCES SKŁADANIA PODPISU ELEKTRONICZNEGO



### 3.2.1. Wybór dokumentu do podpisu



W zależności od zdefiniowanych wcześniej ustawień w aplikacji **proCertum Client Settings** (zakładka *Podpisy* opcja *Włącz podpisywanie wielu plików*) możliwe jest podpisanie tylko jednej lub wielu wskazanych wiadomości.



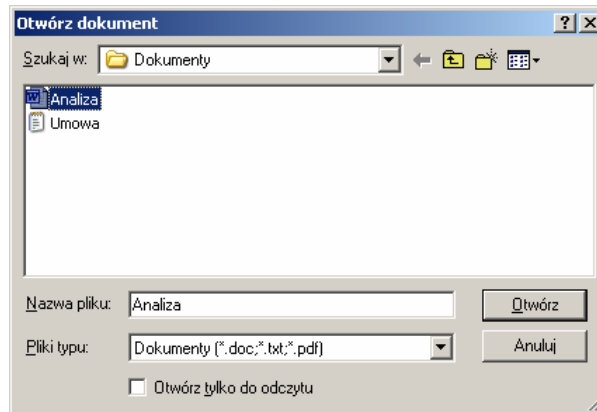
Możliwe jest także dołączenie do podpisu dodatkowych informacji opisujących podpisywany dokument. Możliwość taka jest jednak zależna od używanej polityki podpisu. Dlatego też pole, w którym opisuje się plik wiadomości nie zawsze jest widoczne.



Kolejnym krokiem jest wyszukanie i wskazanie dokumentu, który ma zostać podpisany poprzez kliknięcie na ikonie  lub  (włączone podpisywanie wielu plików), po czym wybrać należy dokument klikając na przycisku „*Otwórz*”. W przypadku podpisywania wielu plików, obok okna „**Lista dokumentów**” dostępne będą

dotatkowe przyciski umożliwiające usuwanie plików z listy  oraz czyszczenie całej listy .

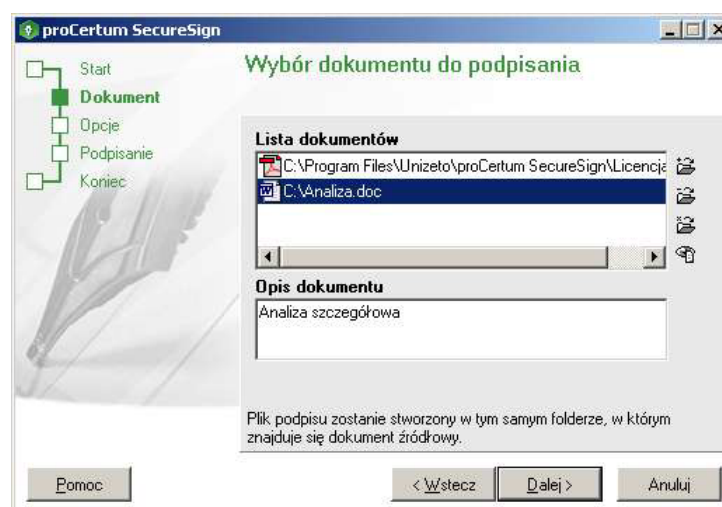
W wyniku procesu podpisywania, pliki podpisane zapisane zostaną w tym samym folderze, w którym znajdują się pliki z wiadomościami.




W procesie składania podpisu dokument ulegnie zabezpieczeniu przed dalszymi modyfikacjami poprzez ustawienie pliku w tryb „tylko do odczytu”. Ma to na celu zapewnienie integralności przeglądanego dokumentu w trakcie procesu składania podpisu.

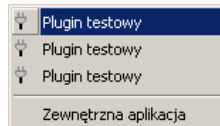
### 3.2.2. Dodawanie opisu dokumentu do podpisu

W celu dodania opisu dokumentu należy w polu **Opis dokumentu** wprowadzić wybrany tekst. W przypadku podpisywania wielu plików zaznaczyć należy najpierw dany dokument na liście, ponieważ dla każdego pliku opis dokumentu wprowadza się oddzielnie.



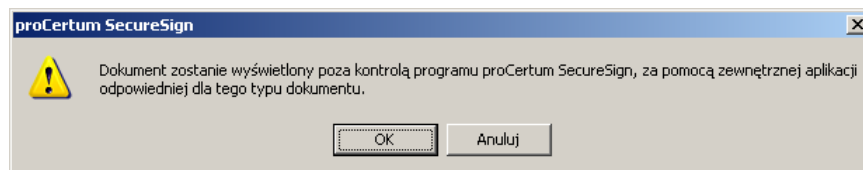
### 3.2.3. Przeglądanie dokumentu przygotowanego do podpisu

Jeżeli chcesz przejrzeć przed podpisaniem dokument, to w tym celu należy kliknąć przycisk oznaczony ikoną . Jeżeli w aplikacji **proCertum ClientSettings** zdefiniowane zostały wtyczki (pluginy) służące do otwierania plików o określonych rozszerzeniach, to użytkownik ma dodatkowo możliwość wyboru wtyczki, za pomocą której otworzony ma zostać podpisywany dokument.



Jeżeli nie zostały zdefiniowane żadne wtyczki lub jeżeli użytkownik wybrał pozycję „**Zewnętrzna aplikacja**”, to dokument otworzony zostanie za pomocą właściwego (zdefiniowanego w systemie) programu, przystosowanego do przeglądania zawartości dokumentu w danym formacie.

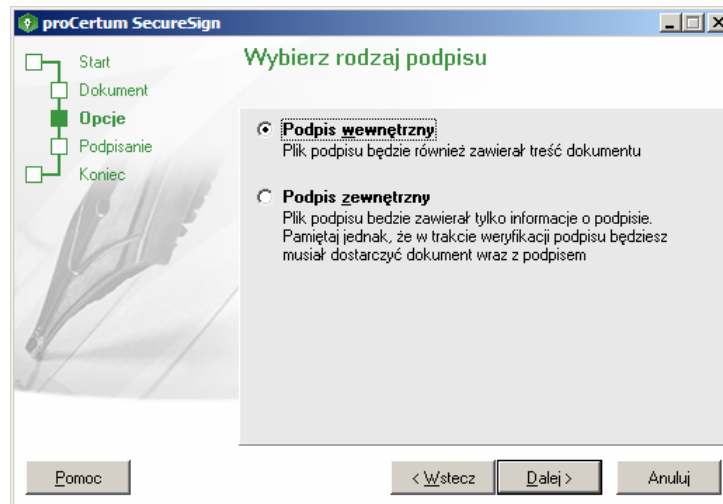
Aplikacja poinformuje nas stosownym komunikatem o fakcie otwierania dokumentu przez mechanizm spoza samej aplikacji.



Dokumenty w formacie \*.txt oraz \*.rtf są otwierane automatycznie przez wewnętrzną przeglądarkę aplikacji.

### 3.2.4. Wybór typu podpisu (wewnętrzny lub zewnętrzny)

Na tym etapie wybrać należy typ podpisu, jaki złożyć chce użytkownik

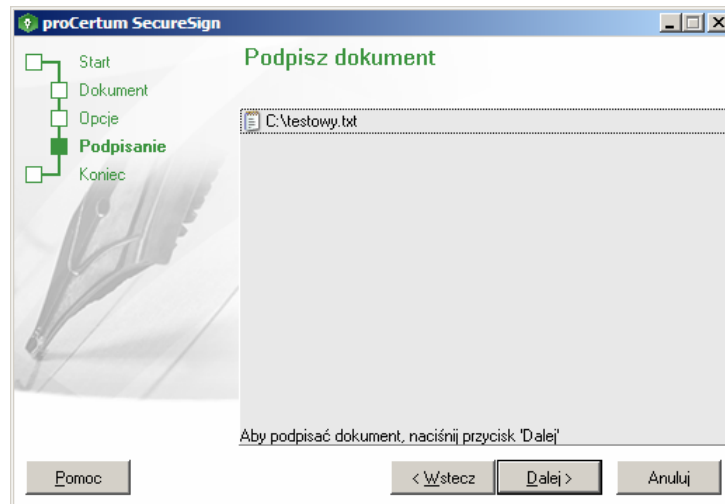


- **podpis wewnętrzny:** utworzony plik (\*.sig) będzie zawierał zarówno podpis i plik podpisywany. Do późniejszej weryfikacji potrzebny będzie tylko ten plik.
- **podpis zewnętrzny:** utworzony plik (\*.sig) będzie zawierał podpis, a podpisywany plik nie jest do niego dołączany. Do weryfikacji takiego podpisu wymagane więc będzie posiadanie i wskazanie zarówno pliku z podpisem, jak i pliku podpisywanego.

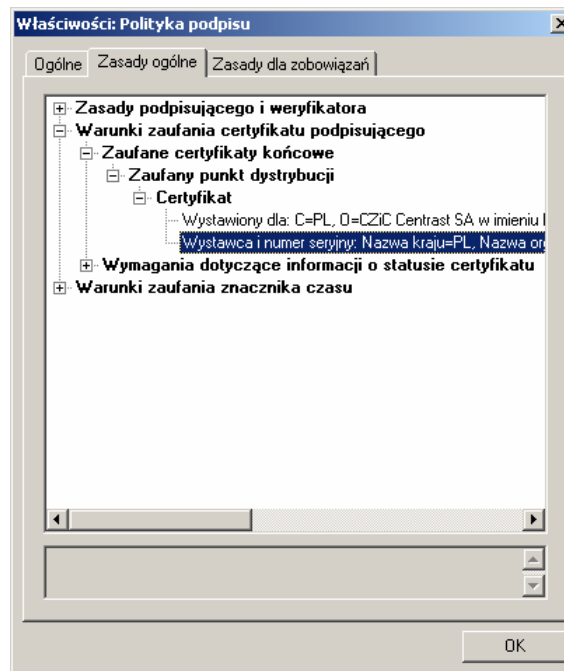
i kliknąć na przycisku „**Dalej**”.

### 3.2.5. Weryfikacja poprawności przygotowania dokumentu do podpisu

Na tym etapie stwierdzić można, czy do podpisania przygotowane zostały odpowiednie pliki.



Jeżeli przed podpisaniem użytkownik chce dla pewności jeszcze raz zapoznać się z polityką podpisu, to może tego dokonać klikając na przycisku „*Pokaż politykę podpisu*”.



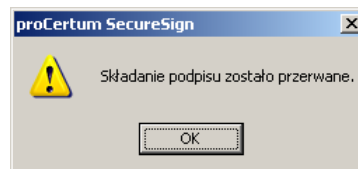
Aby wskazać inne pliki do podpisania kliknąć należy na „*Wstecz*”, Jeżeli zaś lista plików sporządzona jest odpowiednio to należy wówczas:

- włożyć kartę do czytnika, i
- po ostatecznym zweryfikowaniu listy plików do podpisania, kliknąć na „**Dalej**”.

Gdy do czytnika nie zostanie włożona karta z certyfikatem kwalifikowanym, to wyświetlony zostanie poniższy komunikat:



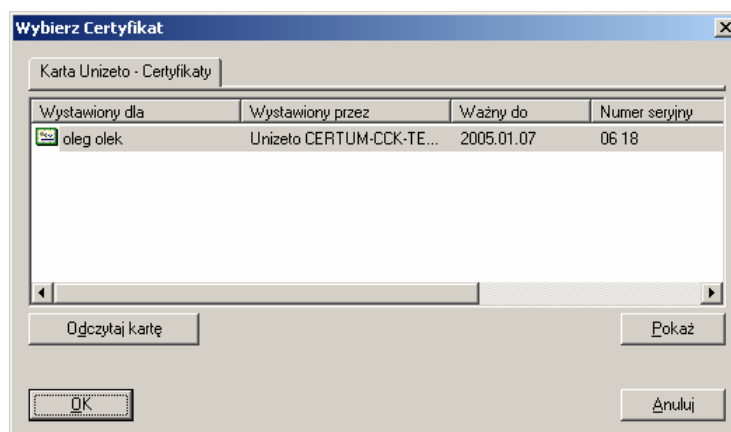
W przypadku, gdy użytkownik przerwać będzie chciał proces składania podpisu, to kliknąć należy na przycisku „**Anuluj**”. Proces zostanie przerwany, aplikacja wyświetli odpowiedni komunikat i wróci do poprzedniego okna.



Jeżeli zaś użytkownik kontynuować chce procedurę i złożyć podpis pod wybranym dokumentem, to po włożeniu karty do czytnika, kliknąć powinien na przycisku „**OK**” w oknie „*Wybór certyfikatu*”. Pojawi się wówczas okno umożliwiające wybór certyfikatu.

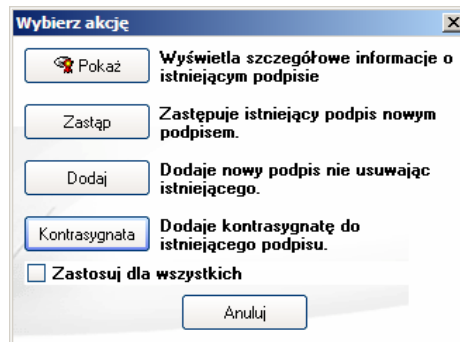
### 3.2.6. Wybór certyfikatu

Wskaż certyfikat z listy i kliknij przycisk „**OK**”.

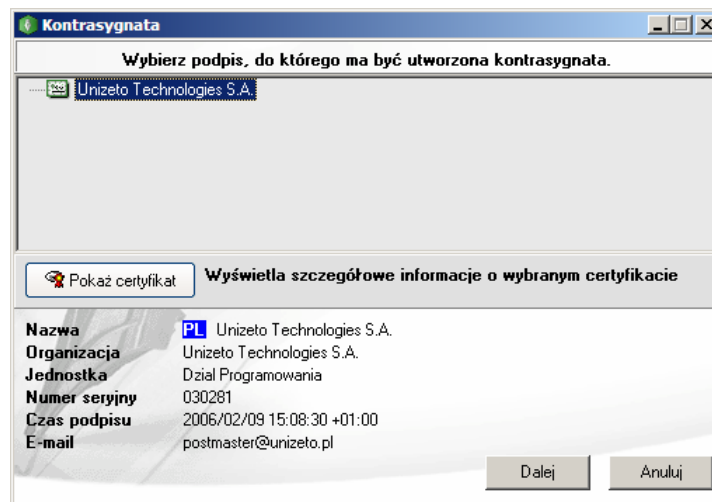


### 3.2.7. Złożenie podpisu

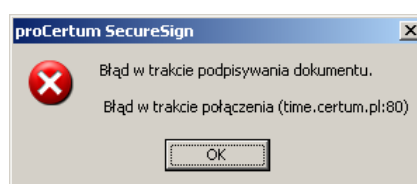
Aplikacja **proCertum SecureSign** daje użytkownikowi możliwość wielokrotnego podpisania tego samego dokumentu. Jeżeli oprogramowanie wykryje, że wskazany dokument został już wcześniej podpisany to użytkownik będzie miał w poniższym oknie następujący wybór:



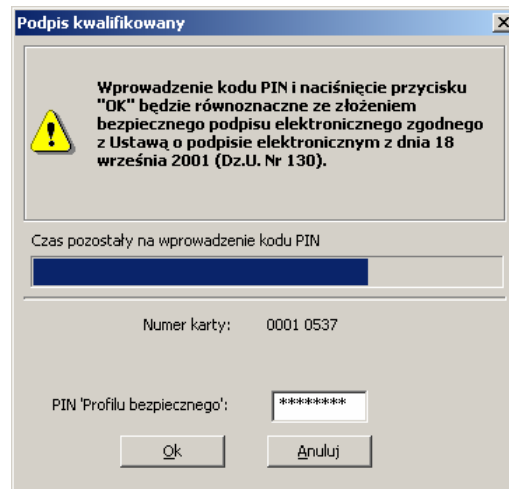
- dodanie kolejnego podpisu do już istniejących,
- utworzenie nowego pliku podpisu (poprzednie podpisy zostaną zastąpione)
- kontrasygnowanie:



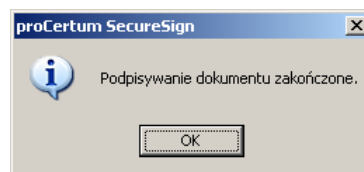
W momencie wystąpienia problemów z połączeniem internetowym w przypadku wykorzystywania polityki podpisu, która oznacza dokument czasem przed złożeniem podpisu pojawi się następujący komunikat:



Program **proCertum SecureSign** informuje o fakcie składania bezpiecznego podpisu elektronicznego zgodnie z wymaganiami przedstawionymi przez Ustawę o podpisie elektronicznym z dnia 18 września 2001 (Dz.U. z 2001 r. Nr 130 poz. 1450).

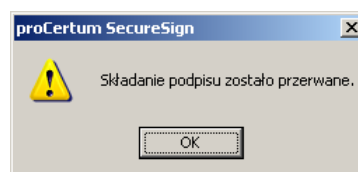


- Jeżeli użytkownik przerwać będzie chciał proces składania podpisu, wówczas kliknąć powinien na przycisku „**Anuluj**”.
- Jeżeli użytkownik chciał zaś będzie złożyć podpis, to podać musi kod PIN do karty i kliknąć przycisk „**OK**” przed upływem czasu, pokazanego w formie wydłużającego się paska. Poprawne wykonanie tego kroku spowoduje pojawienie się następującego komunikatu.



W przypadku podpisywania wielu plików, użytkownik proszony będzie o podanie kodu PIN przy podpisywaniu każdego kolejnego pliku. Kliknięcie przycisku „**Anuluj**” spowoduje przerwanie podpisywania tylko aktualnie podpisywanego pliku.

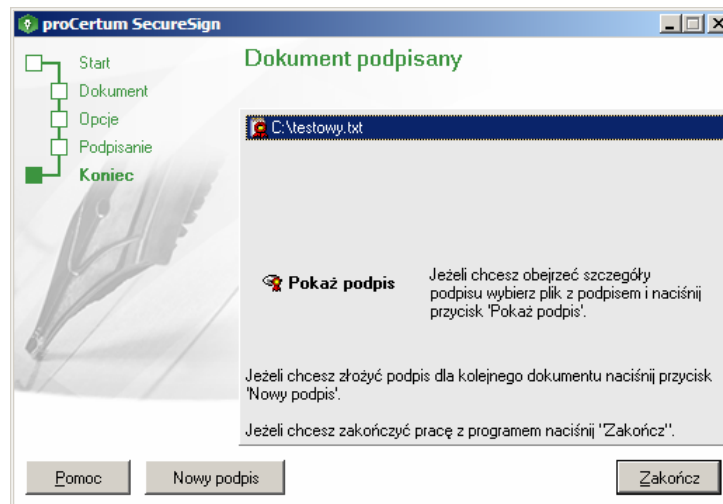
Jeżeli użytkownik nie zdąży złożyć podpisu (tzn. wprowadzić kod PIN i kliknąć „**OK**”) w trakcie przewidzianego na to okresu czasu, wówczas proces składania podpisu zostanie przerwany. Podpis nie zostanie złożony i pojawi się następujący komunikat:



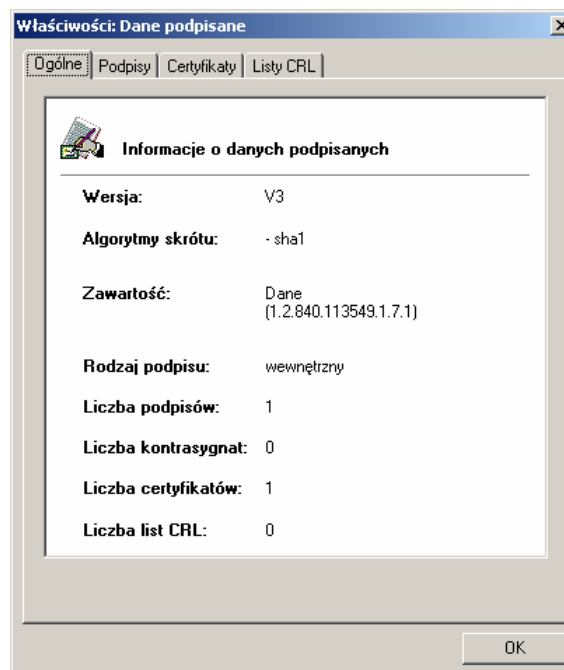
Aplikacja powraca w takim przypadku do kroku „*Podpisz dokument*”.

### 3.2.8. Przegląd zawartości podpisu

Jeśli proces podpisania dokumentu zakończony został pomyślnie, to wyświetlone zostanie okno umożliwiające podgląd zawartości podpisu. Górna jego część zawiera ścieżkę dostępu do podpisanego pliku, dolna zaś przycisk „**Pokaż podpis**”, po kliknięciu na którym, użytkownik przejrzeć może zawartość pliku podpisu danego dokumentu. W przypadku podpisywania wielu plików okno to będzie zawierać listę wszystkich plików podpisanych plików, użytkownik zaś po wyborze dowolnego z nich postępuje analogicznie, jak zostało to opisane w poprzednim zdaniu.



Informacja o podpisie zawarta jest w oknie „*Właściwości: Dane podpisane*”.



**KONIEC PROCEDURY SKŁADANIA PODPISU**

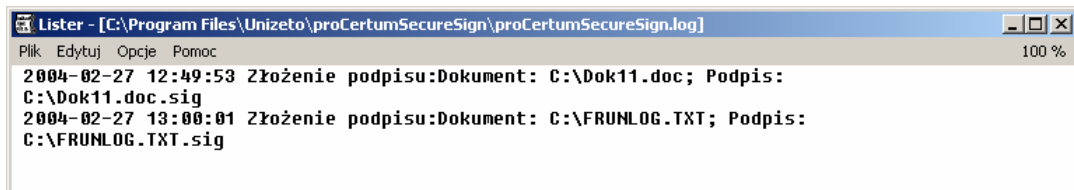
### 3.2.9. Podpisanie kolejnego dokumentu

Kliknij „*Nowy Podpis*” w oknie „*Dokument podpisany*”. Program gotowy jest do rozpoczęcia nowego procesu składania podpisu.

### 3.2.10. Zakończenie pracy programu proCertum SecureSign

Kliknij „*Zakończ*” w oknie „*Dokument podpisany*”.

Wszystkie czynności wykonywane w trakcie procedury podpisywania dokumentu rejestrowane przez aplikację **proCertum SecureSign** w dzienniku zdarzeń, tworzonym przez system – plik o nazwie „proCertumSecureSign.log” znajduje się w katalogu, w którym zainstalowana jest aplikacja. (Domyślnie będzie to więc: c:\Program Files\Unizeto\proCertumSecureSign\)



```
Lister - [C:\Program Files\Unizeto\proCertumSecureSign\proCertumSecureSign.log]
Plik  Edytuj  Opcje  Pomoc  100 %
2004-02-27 12:49:53 Złożenie podpisu:Dokument: C:\Dok11.doc; Podpis:
C:\Dok11.doc.sig
2004-02-27 13:00:01 Złożenie podpisu:Dokument: C:\FRUNLOG.TXT; Podpis:
C:\FRUNLOG.TXT.sig
```

## 4. SKUTKI PRAWNE PODPISU ELEKTRONICZNEGO

Ustawa z dnia 18 września 2001r. (Dz. U. z dnia Nr 130 poz.1450 15 listopada 2001 r.) precyzuje skutki prawne złożonego podpisu elektronicznego. Poniżej przedstawiono fragment ustawy dotyczący skutków prawnych podpisu elektronicznego.

*„Art. 5. 1. Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu. Bezpieczny podpis elektroniczny złożony w okresie zawieszenia kwalifikowanego certyfikatu wykorzystywanego do jego weryfikacji wywołuje skutki prawne z chwilą uchylecia tego zawieszenia.*

*2. Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba, że przepisy odrębne stanowią inaczej.*

*3. Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu zapewnia integralność danych opatrzonych tym podpisem i jednoznacznie wskazuje kwalifikowanego certyfikatu, w ten sposób, że rozpoznawalne są wszelkie zmiany tych danych oraz zmiany wskazania kwalifikowanego certyfikatu wykorzystywanego do weryfikacji tego podpisu, dokonane po złożeniu podpisu.*

*Art. 6. 1. Bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny.*

*2. Przepis ust. 1 nie odnosi się do certyfikatu po upływie terminu jego ważności lub od dnia jego unieważnienia oraz w okresie jego zawieszenia, chyba, że zostanie udowodnione, że podpis został złożony przed upływem terminu ważności certyfikatu lub przed jego unieważnieniem albo zawieszeniem.*

*3. Nie można powoływać się, że podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu nie został złożony za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny.*

*Art. 7. 1. Podpis elektroniczny może być znakowany czasem.*

*2. Znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego.*

*3. Uważa się, że podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usługi. Domniemanie to istnieje do dnia utraty ważności zaświadczenia certyfikacyjnego wykorzystywanego do weryfikacji tego znakowania. Przedłużenie istnienia domniemania wymaga kolejnego znakowania czasem podpisu elektronicznego wraz z danymi służącymi do poprzedniej weryfikacji przez kwalifikowany podmiot świadczący tę usługę.*

*Art. 8. Nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego.*

Postanowienia ustawy doprecyzowuje również kodeks cywilny

## **Kodeks Cywilny**

*Art. 78.*

*§2. Oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne z oświadczeniem woli złożonym w formie pisemnej.*

## 5. PODSTAWOWE DEFINICJE I SKRÓTY

### **Algorytm kryptograficzny**

Algorytm służący do szyfrowania i deszyfrowania informacji używanych w programach komunikacji sieciowej. Do podstawowych algorytmów kryptograficznych należą: DES, RSA, MD5, SHA, IDEA.

### **Centrum Certyfikacji**

Jednostka organizacyjna, będąca elementem składowym zaufanej trzeciej strony, obdarzonej zaufaniem w zakresie tworzenia i wydawania użytkownikom certyfikatów klucza publicznego.

### **Certyfikat klucza publicznego**

Informacja o kluczu publicznym użytkownika, która dzięki podpisaniu przez urząd certyfikacji (np. Centrum Certyfikacji) jest niemożliwa do podrobienia.

### **CRL**

Lista certyfikatów unieważnionych, publikowana zwykle przez wystawcę tych certyfikatów (ang. *Certificate Revocation List*).

### **GUR**

Główny Urząd Rejestracji.

### **Integralność**

Zapewnia możliwość sprawdzenia, czy przesyłane dane nie zostały w żaden sposób zmodyfikowane podczas transmisji. Dzieje się tak dzięki dołączeniu do wiadomości znacznika integralności wiadomości, czyli ciągu bitów obliczonego na podstawie wiadomości.

### **Kryptografia**

Dziedzina kryptologii zajmująca się projektowaniem algorytmów szyfrowania i deszyfrowania. Do zadań algorytmów należy zapewnienie tajności lub autentyczności komunikatów.

### **Kwalifikowany podpis elektroniczny**

podpis elektroniczny, który:

- jest przyporządkowany wyłącznie do osoby składającej ten podpis,
- jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna,
- jest weryfikowany za pomocą ważnego kwalifikowanego certyfikatu.

### **LUR**

Lokalny Urząd Rejestracji.

### **Niezaprzeczalność**

Zapobieganie odmowie poprzednich uzgodnień lub wykonania działań.

### **OCSP**

Protokół serwera weryfikacji statusu certyfikatów, pracującego w trybie *on-line* (ang. *Online Certificate Status Protocol*).

### **PEM**

Standard bezpiecznej poczty elektronicznej. Ulepszony pod względem bezpieczeństwa schemat poczty elektronicznej, zwiększający prywatność korespondencji w sieci Internet. Wykorzystywany jest on zarówno do szyfrowania z jednym, jak i z parą kluczy (ang. *Privacy Enhanced Mail*).

### **PKCS # 12**

Standard składni osobistej wymiany informacji specyfikujący przenośny format dla składowanych i przesyłanych kluczy prywatnych, certyfikatów i innych sekretów użytkownika.

**PKCS # 7**

Standard składni wiadomości szyfrowanej w sposób ogólny definiujący wiadomość kryptograficzną wzmocnioną przez podpis cyfrowy i szyfrowanie.

**PKI**

Infrastruktura Klucza Publicznego (ang. *Public Key Infrastructure*).

**Podpis elektroniczny**

Przekształcenie kryptograficzne jednostki danych, umożliwiające odbiorcy danych sprawdzenie pochodzenia i integralności jednostki danych oraz ochronę nadawcy i odbiorcy jednostki danych przed sfałszowaniem przez odbiorcę; asymetryczne podpisy elektroniczne mogą być generowane przez jeden podmiot przy zastosowaniu klucza prywatnego i algorytmu asymetrycznego, np. RSA.

**Poświadczenie**

Weryfikacja utworzenia lub istnienia informacji przez podmiot inny niż twórca tej informacji. Uniemożliwia nadawcy lub odbiorcy komunikatu zaprzeczenie faktu jego przesłania.

**Poufność**

Utrzymywanie informacji w sekrecie dla wszystkich podmiotów, które nie są uprawnione do jej znajomości.

**Poufność**

Zagwarantowanie, że przesyłane lub przechowywane dane będą dostępne (możliwe do odczytania) jedynie dla uprawnionych osób, np.: odbiorcy wiadomości pocztowej. W szczególności chodzi o drukowanie, wyświetlanie i inne formy ujawniania, w tym ujawnianie istnienia jakiegoś obiektu.

**PSE**

Osobiste bezpieczne środowisko (ang. *personal security environment*) jest to lokalny bezpieczny nośnik klucza prywatnego podmiotu, klucza publicznego (zwykle w postaci autocertyfikatu); w zależności od polityki bezpieczeństwa nośnik ten może mieć postać kryptograficznie zabezpieczonego pliku (np. zgodnie z PKCS#12) lub odporny na penetrację sprzętowy token (np. identyfikacyjna karta elektroniczna).

**RSA**

Kryptograficzny algorytm asymetryczny (nazwa pochodzi od pierwszych liter jego twórców Rivesta, Shamira i Adlemana), w których jedno przekształcenie prywatne wystarcza zarówno do podpisywania jak i deszyfrowania wiadomości, zaś jedno przekształcenie publiczne wystarcza zarówno do weryfikacji jak i szyfrowania wiadomości.

**Szyfrowanie**

Kryptograficzne przekształcenie danych, którego wynikiem jest zaszyfrowany tekst (szyfrogram). Tekst taki dla osób trzecich stanowi jedynie przypadkowy ciąg znaków, na podstawie którego nie jest możliwe odtworzenie żadnej użytecznej informacji. Otrzymany w wyniku szyfrowania ciąg znaków nosi nazwę tekstu zaszyfrowanego (szyfrogramu).

**TTP**

Zaufana trzecia strona, instytucja lub jej przedstawiciel mający zaufanie innych podmiotów w zakresie działań związanych z zabezpieczeniem, działań związanych z uwierzytelnianiem, mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego (wg PN 2000) (ang. *Trusted Third Party*).

**Znacznik Czasu**

Jednostka danych oznaczająca moment, w którym zaszło określone zdarzenie względem wspólnego czasu odniesienia (np.: jednoznacznie określa moment podpisania wiadomości, co pozwala na stwierdzenie, czy podpis został złożony w okresie ważności certyfikatu).

\* \* \*