Sigillum POLSKIE CENTRUM CERTYFIKACJI ELEKTRONICZNEJ

SignOnViewer

Instrukcja Użytkownika

Wersja 1.00

SPIS TREŚCI

1. SŁOWNICZEK

bezpieczny podpis elektroniczny (wg UoPE)
podpis elektroniczny, który:
- jest przyporządkowany wyłącznie do osoby składającej ten podpis
- jest sporządzany za pomocą bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny
- jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna

CA (ang., certification authority)
centrum certyfikacji wystawiające certyfikaty kwalifikowane

certyfikacja (ang. certification)
- wydawanie certyfikatu klucza publicznego przez urząd certyfikacji
- wydawanie certyfikatu zgodności z obowiązującymi kryteriami oceny zabezpieczeń przez jednostkę certyfikującą działającą w ramach krajowego systemu certyfikacji zabezpieczeń

certyfikat (wg UoPE)
elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby

certyfikat klucza publicznego (ang. public key certificate)
informacja o kluczu publicznym - poświadczenie wydane przez urząd certyfikacji, stwierdzające, że klucz publiczny należy do konkretnego podmiotu; podpisane cyfrowo kluczem prywatnym CA, zawierające dane identyfikujące podmiot i klucz publiczny podmiotu, określające okres ważności certyfikatu

certyfikat ROOT- certyfikat główny
certyfikat głównego urzędu certyfikacji, będącego najwyżej w hierarchii urzędów. Certyfikat ten stanowi punkt zaufania dla wszystkich certyfikatów wydanych przez centra certyfikacji znajdujące się w Infrastrukturze Klucza Publicznego (PKI)

kwalifikowany certyfikat (wg UoPE)
certyfikat spełniający warunki określone w Ustawie, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w Ustawie

kwalifikowany podmiot świadczący usługi certyfikacyjne (wg UoPE)
podmiot świadczący usługi certyfikacyjne, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne

klucz prywatny
klucz służący do wykonywania zastrzeżonej czynności, którego rozpowszechnienie zagraża bezpieczeństwu systemu. Klucz prywatny jest w wyłącznym posiadaniu adresata informacji. Najczęściej służy do odszyfrowywania i podpisywania informacji.

lista CRL
podpisane przez Urząd Certyfikacji chronologiczne zestawienie zawierające listę wszystkich certyfikatów unieważnionych bądź zawieszonych przez Urząd Certyfikacji

odwołanie certyfikatu
proces polegający na usunięciu certyfikatu z systemu zarządzania urzędem certyfikacji. Jego zadaniem jest wskazanie, że klucz publiczny zawarty w odpowiednim certyfikacie nie może być dłużej używany

PKI (ang. Public Key Infrastructure) - Infrastruktura Klucza Publicznego

ogół zagadnień technicznych, operacyjnych i organizacyjnych umożliwiających realizację różnych usług ochrony informacji przy zastosowaniu kryptografii klucza publicznego i certyfikatów klucza publicznego;

podpis elektroniczny (wg UoPE)

dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny

polityka certyfikacji (ang. certificate policy (CP))

nazwany zbiór reguł, określający stosowalność certyfikatu dla konkretnej społeczności użytkowników i / lub klasy aplikacji ze wspólnymi wymaganiami w zakresie bezpieczeństwa

Root CA

urząd certyfikacji posługujący się certyfikatem samo-podpisanym

ścieżka certyfikacji

łańcuch różnorodnych certyfikatów niezbędnych do stwierdzenia ważności danego certyfikatu klucza publicznego. Ścieżka certyfikacyjna powinna zawierać certyfikat użytkownika końcowego podpisany przez urząd certyfikacji, oraz certyfikaty wszystkich nadrzędnych certyfikatów urzędów certyfikacji występujących w danej architekturze klucza publicznego

Urząd Certyfikacji, Urząd ds. Certyfikacji (ang. Certification Authority (CA))

urząd realizujący usługę wydawania i zarządzania certyfikatami; potoczna nazwa najbardziej typowego urzędu certyfikacyjnego realizującego podstawową usługę certyfikacyjną w ramach PKI - certyfikację kluczy publicznych

Urząd Rejestracji, Urząd ds. Rejestracji (ang. Registration Authority (RA))

organ odpowiedzialny za weryfikację tożsamości subskrybenta oraz przekazanie odpowiednich informacji do urzędu certyfikacji zgodnie z procedurą rejestracji stosowaną w celu wydania certyfikatu

urządzenie służące do składania podpisu elektronicznego (wg UoPE)
sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający złożenie podpisu lub poświadczenia elektronicznego przy wykorzystaniu danych służących do składania podpisu lub poświadczenia elektronicznego

urządzenie służące do weryfikacji podpisu elektronicznego (wg UoPE)
sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający identyfikację osoby fizycznej, która złożyła podpis elektroniczny, przy wykorzystaniu danych służących do weryfikacji podpisu elektronicznego lub w sposób umożliwiający identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne, przy wykorzystaniu danych służących do weryfikacji poświadczenia elektronicznego

usługi certyfikacyjne
szeroka klasa usług dotyczących TTP obejmująca działania polegające na poświadczeniu wybranych informacji przez wygenerowanie podpisanego elektronicznie zaświadczenia certyfikacyjnego, jak certyfikacja kluczy publicznych, certyfikacja istnienia danych elektronicznych w określonym czasie, certyfikacja przedstawienia danych elektronicznych przez określonych użytkowników w określonym czasie

usługi certyfikacyjne (wg UoPE)
wydawanie certyfikatów, znakowanie czasem lub inne usługi związane z podpisem elektronicznym

Ustawa
ustawa z dnia 18 września 2001 r. o podpisie elektronicznym określająca warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych oraz zasady nadzoru nad podmiotami świadczącymi te usługi

uwierzytelnienie (ang. authentication)
sprawdzenie tożsamości jednostki; proces polegający na sprawdzeniu, czy przedstawiająca się osoba (także komputer, urządzenie lub usługa) jest tą, za którą się podaje

UZC (ang. Time Stamping Authority (TSA)) - Urząd Znacznika Czasu
urząd realizujący usługę certyfikacyjną oznaczania czasem przedstawionego skrótu dokumentu elektronicznego

znakowanie czasem (wg UoPE)
usługa polegająca na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę

zaświadczenie certyfikacyjne
elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu- kwalifikowanego podmiotu świadczącego usługi certyfikacyjne, i które umożliwiają identyfikację tego podmiotu lub organu

2. PODSTAWY PODPISU ELEKTRONICZNEGO

Upowszechnianie się elektronicznych form przekazu informacji wiąże się z przesyłaniem ich w sieciach publicznych. Dokumenty przesyłane w ten sposób wymagają zapewnienia im wysokiego poziomu bezpieczeństwa. Zastosowanie metod kryptograficznych pozwala na zagwarantowanie ochrony na o wiele wyższym poziomie niż w przypadku dokumentów tradycyjnych. Metody te umożliwiają:

- zapewnienie poufności poprzez szyfrowanie danych, dzięki czemu dokument taki staje się nieprzydatny dla osób niepowołanych,
- utrzymanie i weryfikację integralności dokumentu - można mieć pewność, że nikt nic nie zmienił podczas transmisji,
- uwierzytelnienie podmiotu uczestniczącego w wymianie informacji,
- niezaprzeczalność - zapobieganie próbom wyparcia się uczestnictwa w procesie wymiany informacji.

Powyższe cechy można zagwarantować stosując podpis elektroniczny. Podpis elektroniczny zgodnie z definicją ustawową (Art. 3 Ustawy z dnia 18 września 2001r. o podpisie elektronicznym, Dz. U. Nr 130, Poz. 1450, z dnia 15.11.2001r.) to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane służą do identyfikacji osoby składającej podpis elektroniczny.

Wyróżnia się dwa rodzaje podpisów elektronicznych: zwykły i bezpieczny. Bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu jest przyporządkowany wyłącznie do osoby składającej ten podpis oraz jest sporządzony za pomocą bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny. Zgodnie z ustawą został on zrównany pod względem prawnym z podpisem odręcznym.

Koncepcja podpisu elektronicznego jest ściśle związana z kryptografią asymetryczną oraz infrastrukturą klucza publicznego. Wymiana informacji pomiędzy dwoma podmiotami powinna opierać się na zaufaniu tzn. odbiorca powinien mieć pewność, że nadawca jest tym, za kogo się podaje. Natomiast nadawca może zakładać, że odbiorca jest tym, dla kogo informacja była przeznaczona. Do takiej formy wymiany informacji służą pary kluczy stosowanych w szyfrowaniu: prywatny i publiczny.

Klucz prywatny (ang. private key) służy do deszyfrowania wiadomości (zaszyfrowanej kluczem publicznym) oraz bierze udział w procesie tworzenia podpisu cyfrowego. Klucz prywatny zna jedynie jego właściciel i powinien być chroniony ze szczególną starannością. Nośnikiem dla klucza prywatnego jest karta kryptograficzna (mikroprocesorowa).

Klucz publiczny (ang. public key) służy do zaszyfrowania wiadomości. Osoba, która chce zaszyfrować wiadomość używa do tego celu klucza publicznego odbiorcy wiadomości. Tylko właściciel klucza prywatnego może odszyfrować taką wiadomość. W ten sposób osoba wysyłająca wiadomość ma pewność, że treść wiadomości zostanie odczytana tylko przez odbiorcę.

Zgodnie z aktualnym stanem prawnym, wykorzystując podpisy elektroniczne możliwe jest podpisywanie faktur, transakcji elektronicznych, umów cywilno-prawnych, deklaracji ZUS, oraz wielu innych dokumentów.

3. ZAWARTOŚĆ ZESTAWU DO PODPISU ELEKTRONICZNEGO SIGILLUM

Pełny zestaw do podpisu elektronicznego udostępniany przez PCCE Sigillum przy zakupie certyfikatu zawiera:

1. Czytnik kart mikroprocesorowych
2. Kartę mikroprocesorową z certyfikatami
3. Płytę instalacyjną, umożliwiającą automatyczną instalację następujących komponentów:
    a. CryptoCardSuite –oprogramowania obsługującego karty mikroprocesorowe
    b. aplikacji SignOnViewer
    c. zaświadczeń certyfikacyjnych Głównego Urzędu Certyfikacji (ROOT) i Pośrednich Centrów Certyfikacji

Przeznaczenie aplikacji

Aplikacja SignOnViewer :

- weryfikuje plik z podpisem S-MIME
- weryfikuje pliki z podpisem CMS (Unizeto) i PKCS#7 (KIR)
- weryfikuje standardy podpisu: ETSI TS 101 733 i ETSI 101 903 XML-XAdES

SignOnViewer sprawdza fakt zainstalowania zaświadczeń certyfikacyjnych Sigillum na komputerze, na którym są instalowane.

Zgodność z innymi standardami podpisu

W poniższej tabeli wymieniono, wraz z krótkim opisem standardy weryfikowane przez aplikację SignOnViewer.

Nazwa standardu	**Rozszerzenie pliku**	**Przykładowa aplikacja / producent**
PKCS#7	*.sdoc	-
S/MIME	*.signpro	-
S/MIME	*.pem	Pemheart, Enigma
CMS	*.sig	Safe Device- KIR, ProCertumCombiLite, ProCertumSecureSign-Unizeto
XadES – BES	*.xml	-
PKCS#7	*.p7	-

4. INSTALACJA

Wymagania sprzętowo- systemowe

Aplikacja SignOnViewer może być uruchamiana w systemach:

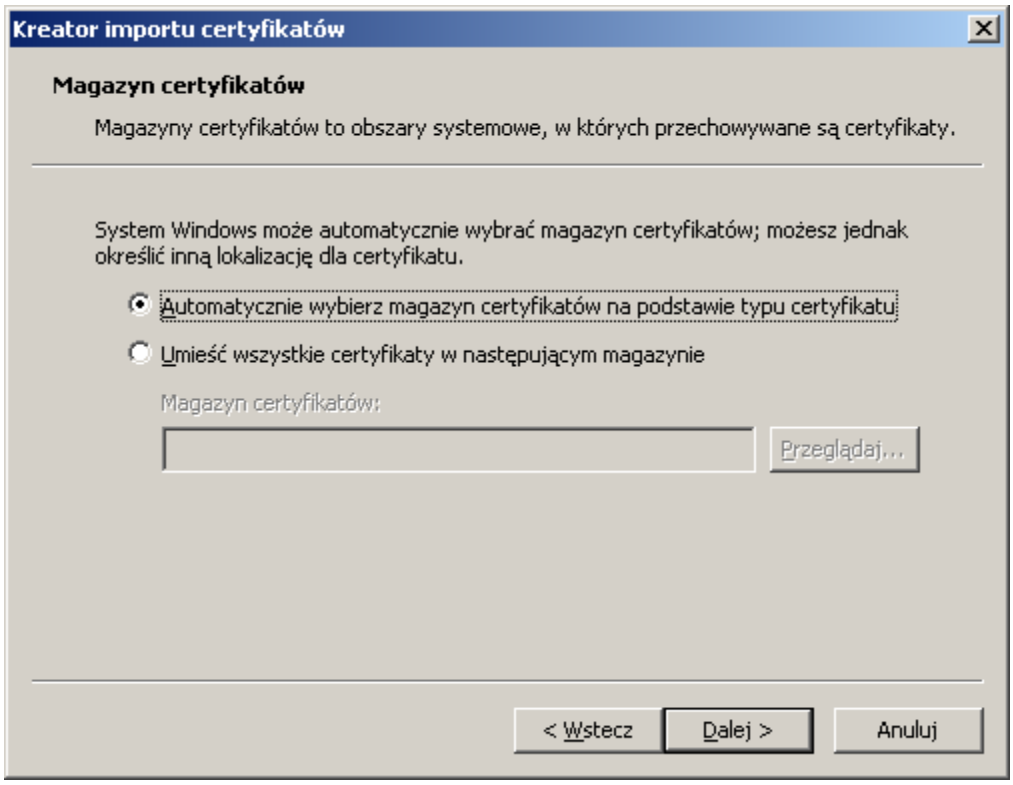
- Windows 98 SE (w systemie Win98 SE wspierane są sdoc, signPro, pem, p7 natomiast CMS i XAdES nie są wspierane w Win98 SE)
- Windows 2000 SP4
- Windows XP z SP2
- Windows 2003.
- Windows Vista 32

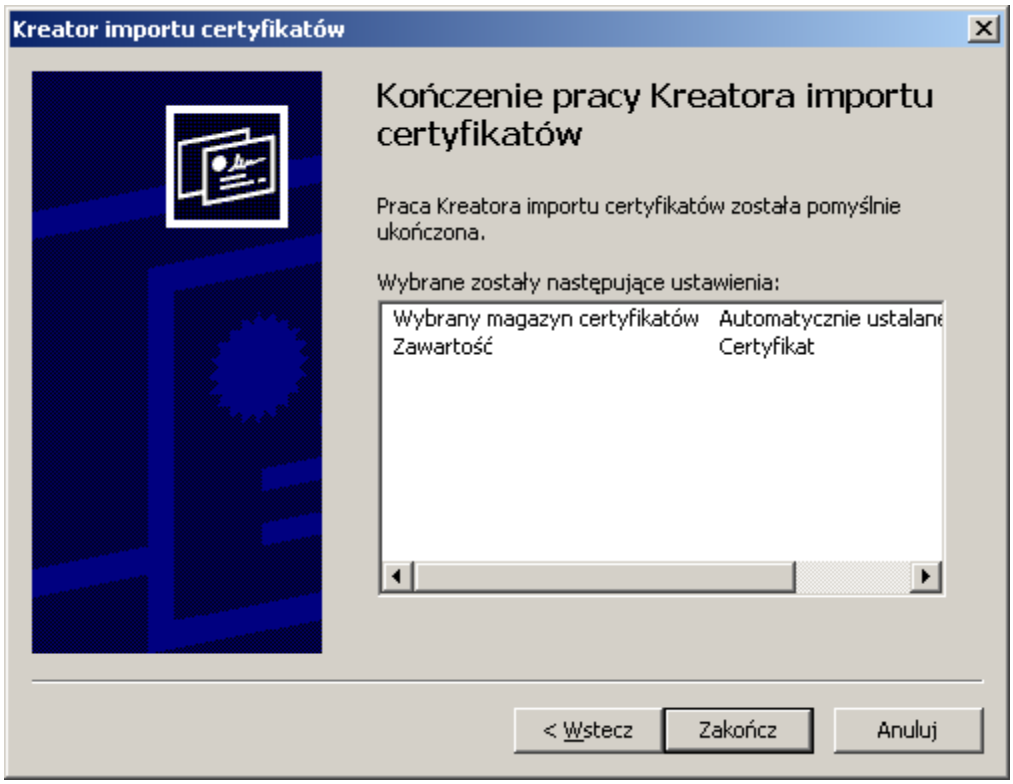
Do poprawnej pracy wymagana jest przeglądarka Internet Explorer w wersji 5.5 lub nowszej.

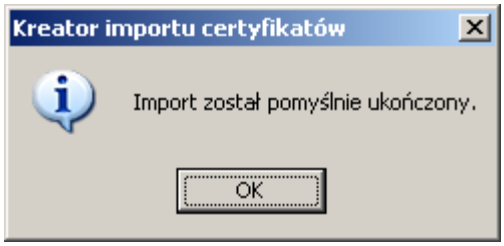
Instalacja

Umieszczenie aplikacji SignOnViewer.exe w dowolnym miejscu systemu.

Przy pierwszym uruchomieniu pojawi się kreator importu zaświadczeń certyfikacyjnych. Każde z zaświadczeń certyfikacyjnych należy zatwierdzić.

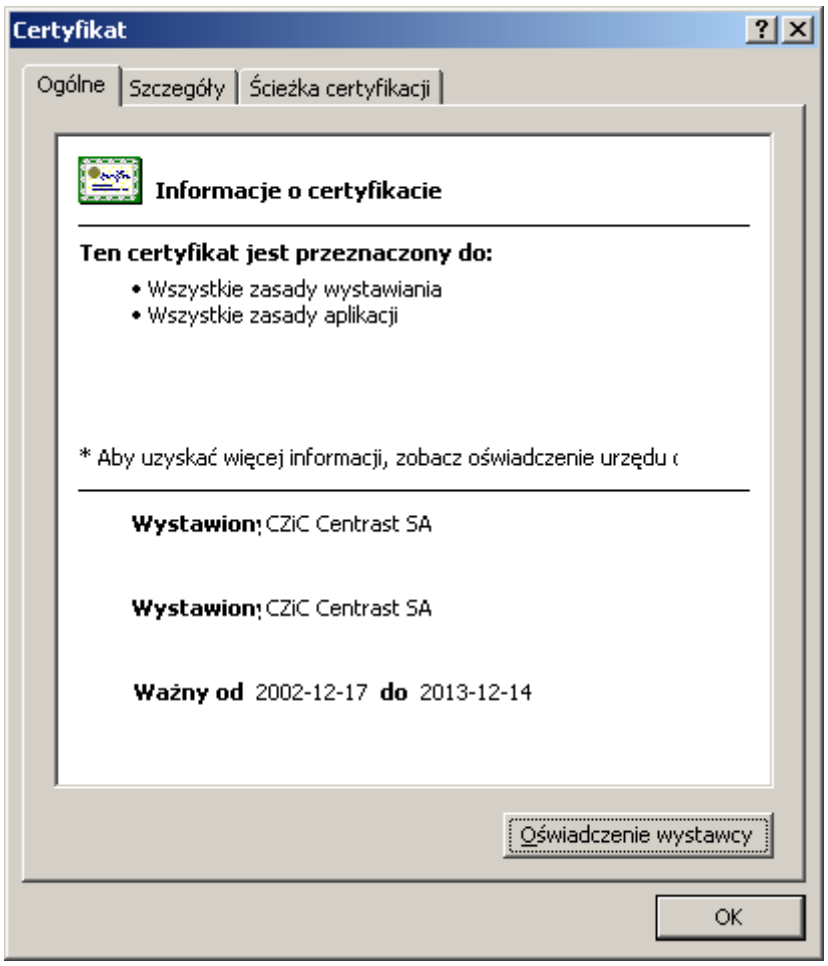

Kreator importu certyfikatów
Magazyn certyfikatów
Magazyny certyfikatów to obszary systemowe, w których przechowywane są certyfikaty.
System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.
Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu
Umieść wszystkie certyfikaty w następującym magazynie
Magazyn certyfikatów:
Przeglądaj...
< Wstecz
Dalej >
Anuluj

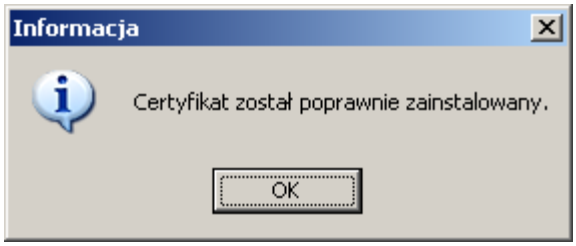

Kreator importu certyfikatów
Kończenie pracy Kreatora importu certyfikatów
Praca Kreatora importu certyfikatów została pomyślnie ukończona.
Wybrane zostały następujące ustawienia:
Wybrany magazyn certyfikatów
Automatycznie ustalane
Zawartość
Certyfikat
< Wstecz
Zakończ
Anuluj



Po wyborze miejsca przechowywania certyfikatów Kreator importu certyfikatów zakończy działanie.

Przykładowy ekran zaimportowanego zaświadczenia certyfikacyjnego do systemu. [CZiC Centrast S.A.]:




Informacja
Certyfikat został poprawnie zainstalowany.
OK

5. KORZYSTANIE Z APLIKACJI

Zainstalowane komponenty

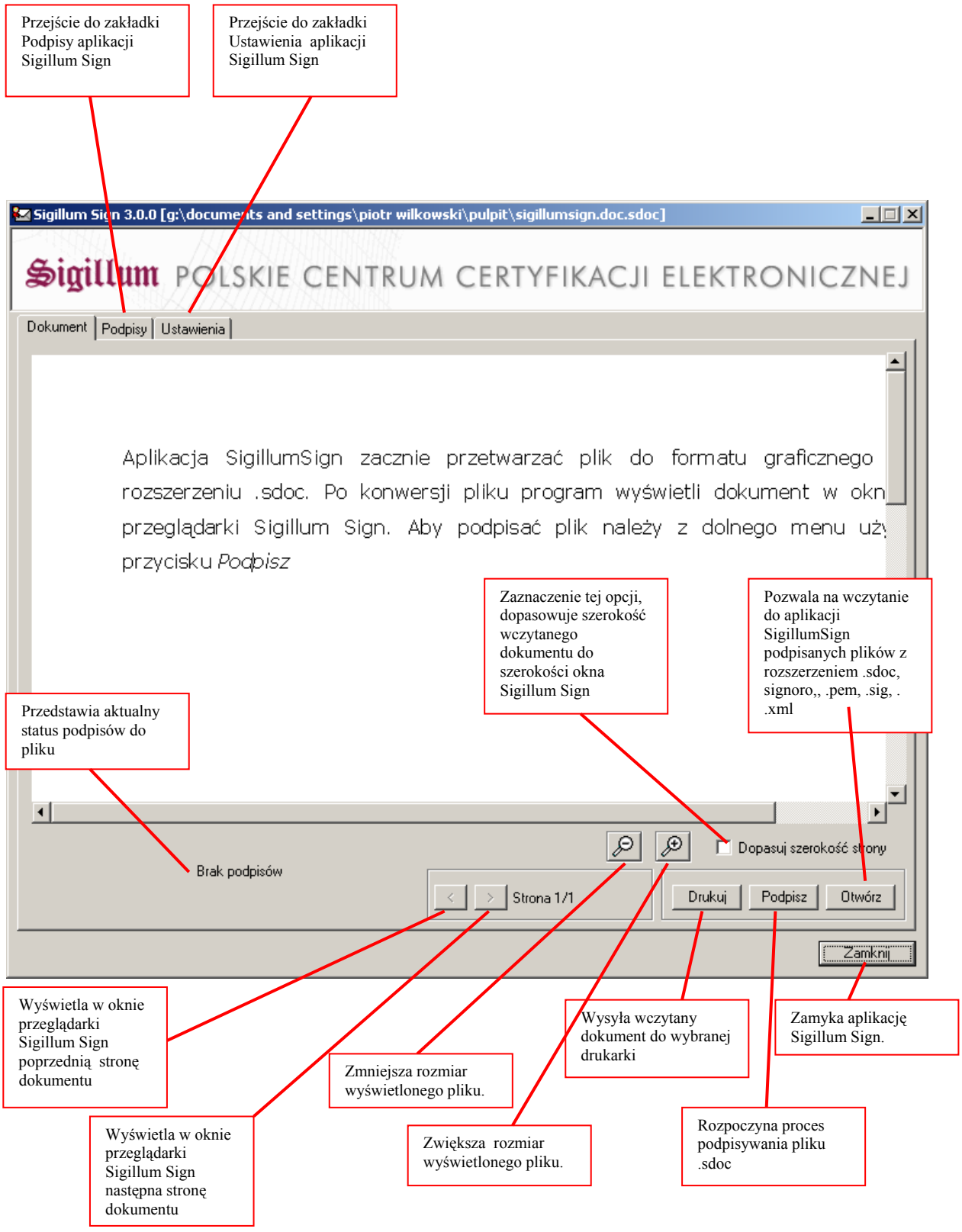
Do poprawnego działania aplikacji SignOnViewer wymaga się zainstalowania odpowiednich komponentów:

a. zainstalowanie w systemie zaświadczeń certyfikacyjnych Głównego Urzędu Certyfikacji oraz Pośrednich Centrów Certyfikacji
b. aplikacja SignOnViewer
c. zgoda na pobranie zaświadczeń certyfikacyjnych przy pierwszym uruchomieniu aplikacji SignOnViewer – wymagane jest połączenie do sieci Internet

Aby sprawdzić czy poszczególne komponenty zainstalowały się prawidłowo należy:

- w przypadku rejestracji zaświadczeń certyfikacyjnych w systemie jednym ze sposobów jest wyświetlenie magazynu certyfikatów wykorzystując do tego przeglądarkę Microsoft Internet Explorer. Z paska opcji wybieramy Narzędzia – Opcje Internetowe, przechodzimy do zakładki Zawartość w polu Certyfikaty. W nowo otwartym oknie należy wybrać zakładkę Pośrednie Urzędy Certyfikacji i odszukać żądany certyfikat.

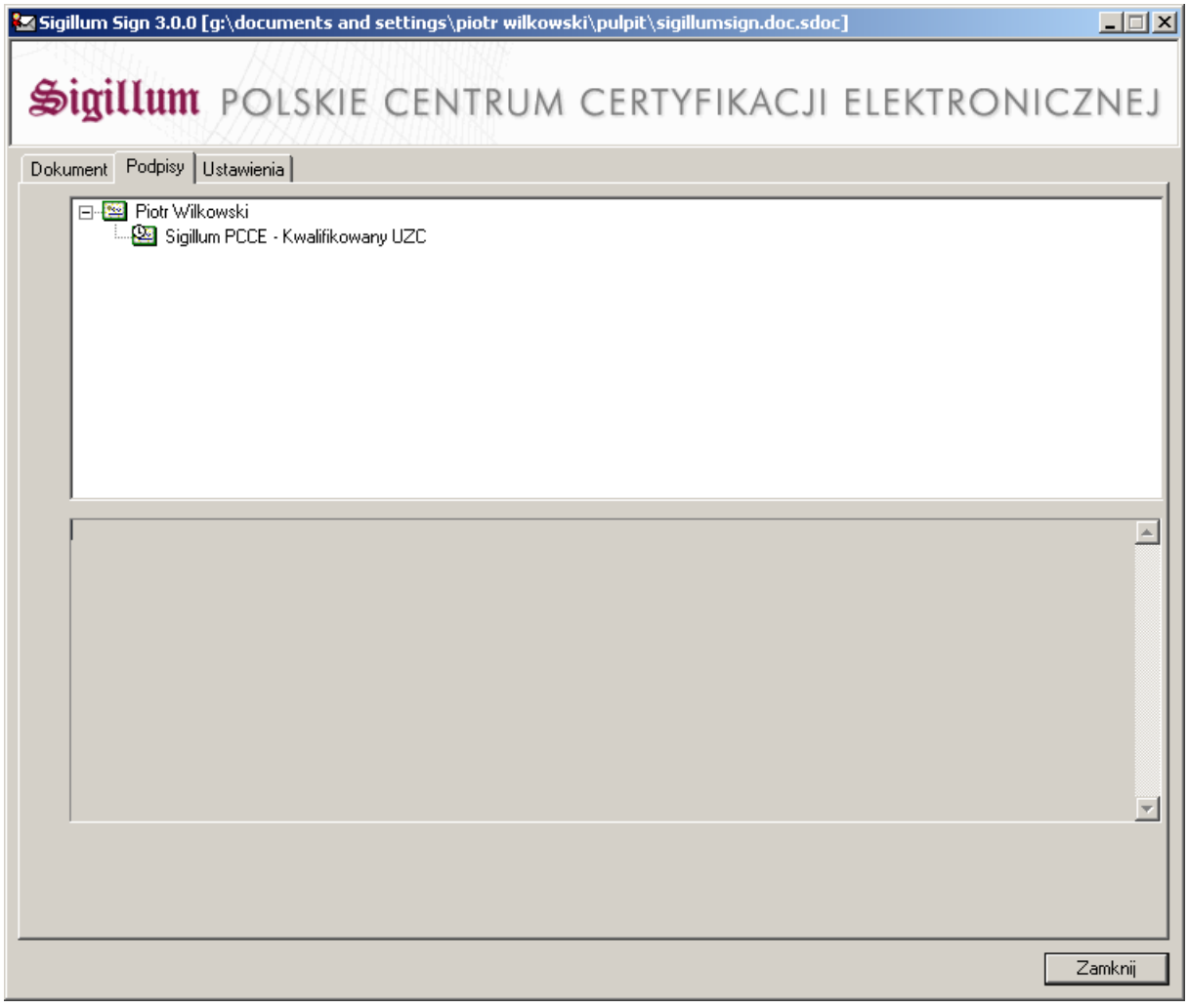
Opcje aplikacji



Jeśli wybrano przycisk *Podpisz*, program otworzy okno wyboru certyfikatu, którego klucz prywatny posłuży do złożenia podpisu. Użycie tej opcji nie jest polecane, ze względu na tworzenie pliku podpisu w formacie .sdoc

Do wykonania oisywanych poniżej operacji konieczne jest doinstalowanie CryptoCard Suit firmy Crypto-Tech.

Po kliknięciu przycisku *OK*, program przejdzie do zakładki Podpisy, w którym wyświetli informację o podpisach i znacznikach czasu.



5.1. Weryfikacja podpisanych plików

Aplikacja SignOnViewer pozwala na weryfikację podpisanego pliku. Można w tym celu dwukrotnie kliknąć na plik podpisu i zweryfikować status podpisu znajdujący się w zakładce *Podpisy.*

Po uruchomieniu programu wybrać przycisk *Otwórz* i wskazać ścieżkę do pliku, który ma być zweryfikowany.
W oknie wyświetlane są informacje o błędach podpisu i znaczniku czasu, oraz lista podpisów, znaczników czasu do podpisu i kontrasygnat wraz ze statusami. Informacja o błędach może zawierać następujące komunikaty:

- „Brak podpisów". Jeżeli nie został złożony żaden podpis,
- „Podpis zweryfikowany poprawnie", jeżeli wszystkie podpisy złożone pod dokumentami są poprawne,
- „Podpis zweryfikowany niekompletnie", jeśli program nie był w stanie określić, czy podpisy złożone pod dokumentem są prawidłowe (może tak się stać, jeśli nie jest możliwe pobranie aktualnej listy CRL, lub, jeżeli certyfikaty główne nie zostały zaimportowane do systemu),
- „Podpis zweryfikowany negatywnie", jeżeli wygenerowany podpis nie jest poprawny ze względu na zmianę w dokumencie lub podpisie, lub cofnięcie poświadczenia certyfikatu przez Wystawce),

A także odpowiedni komunikat błędu jeżeli nie udało się odczytać podpisów.

Wśród informacji znajdujących się na liście podpisów status wyświetlany jest w postaci graficznej (ikony), oraz za pomocą komunikatu określającego problem.

Możliwe statusy podpisu:


Podpis zweryfikowany poprawnie


Podpis zweryfikowany niekompletnie


Podpis zweryfikowany negatywnie


Znacznik czasu zweryfikowany poprawnie

Znacznik czasu zweryfikowany niekompletnie

Znacznik czasu zweryfikowany negatywnie

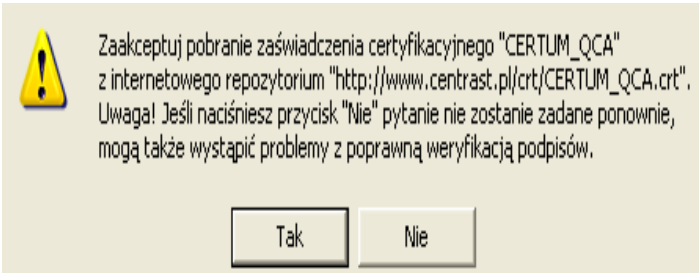
Pobieranie zaświadczeń certyfikacyjnych

Aby program mógł poprawnie zweryfikować podpisy, należy:

- uruchomić odpowiednią opcję pobrania zaświadczeń certyfikacyjnych w dodatkowych zadaniach instalatora lub
- przy pierwszej weryfikacji zabezpieczonego pliku automatycznie zostaną pobrane zaświadczenia certyfikacyjne Głównego Urzędu Certyfikacji oraz pośrednich centrów certyfikacji.

Przy każdym zaświadczeniu pojawi się okno z informacją – jak poniżej. Należy każdorazowo zaakceptować pobranie zaświadczenia.

UWAGA! Jeżeli użytkownik zrezygnuje z pobrania zaświadczeń mogą wystąpić problemy z weryfikacją podpisów.



Zgodność z innymi standardami podpisu elektronicznego

Aplikacja SignOnViewerjest w stanie zweryfikować dokumenty podpisane przez aplikację Sigillum Sign i Sigillum Sign Pro. Ponadto Aplikacja wspiera weryfikację

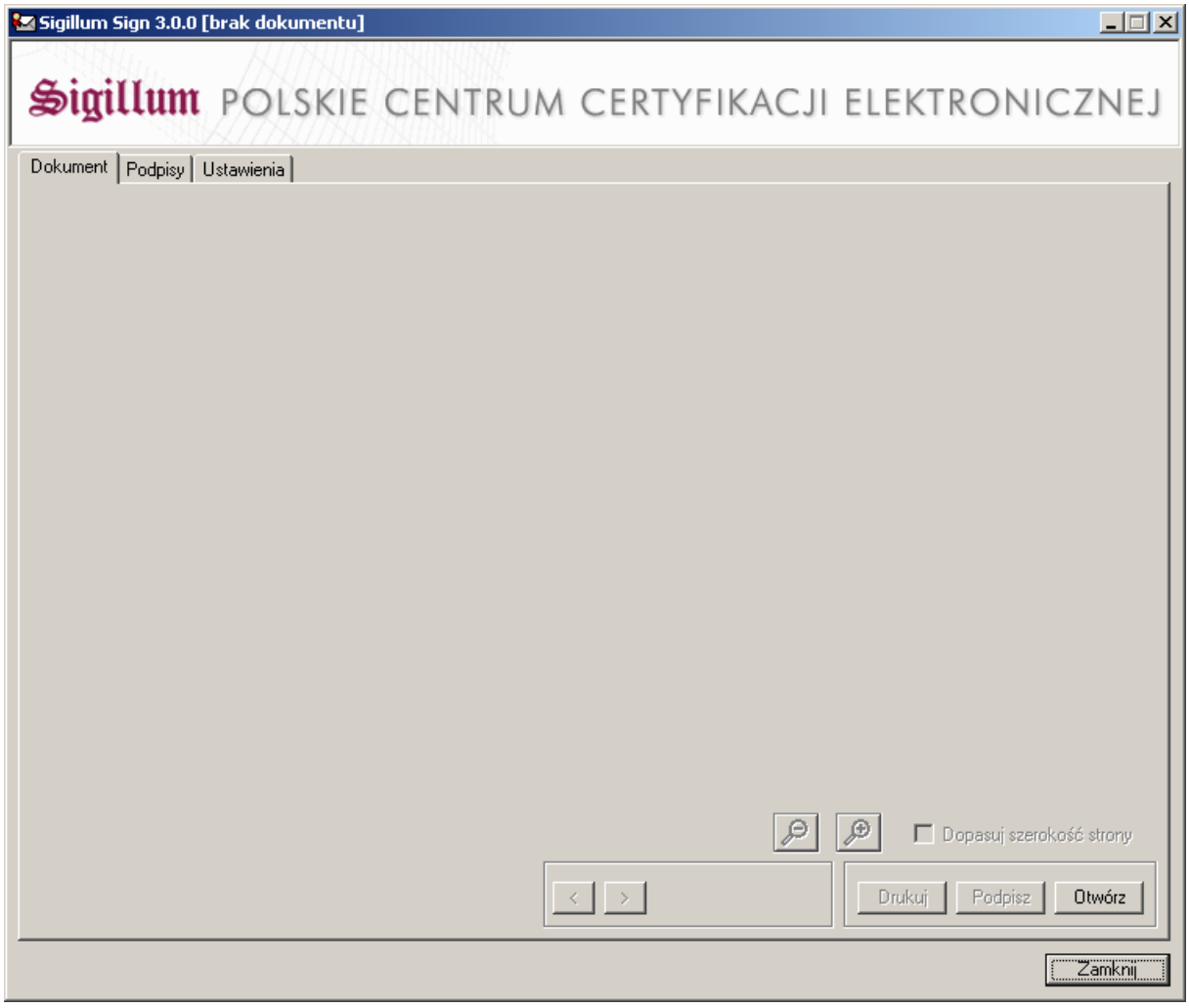
plików podpisanych w standardach używanych przez inne krajowe Pośrednie Centra Certyfikacji (Szafir KIR, Certum Unizeto) standardów PKCS#7, CMS.
Aplikacja pozwala na pełną weryfikację plików podpisanych z wykorzystaniem infrastruktury Polskiego Centrum Certyfikacji Elektronicznej Sigillum PWPW S.A. –weryfikacja podpisu, weryfikacja wielu podpisów i znaczników czasu, weryfikacja kontrasygnaty, weryfikacja znacznika czasu do kontrasygnaty.
W obecnej wersji oprogramowanie pozwala między innymi na:

- Weryfikację plików w standardzie CMS zgodnym z aplikacjami innych centrów certyfikacji (w chwili obecnej są to: KIR i Unizeto)
- Weryfikację standardów podpisu: ETSI TS 101 733 i ETSI 101 903 XML-XadES
- Sprawdzanie przez SignOnViewer faktu zainstalowania zaświadczeń certyfikacyjnych Sigillum na komputerze na którym są instalowane.

Ustawienia aplikacji SignOnViewer

5.2. Zakładka Dokument

Aby uruchomić program SignOnViewer na zakładce *Dokument* należy kliknąć na *Start → Programy → SignOnViewer→ Przeglądarka SignOnViewer*. Aplikacja domyślnie otworzy się na zakładce *Dokument.*

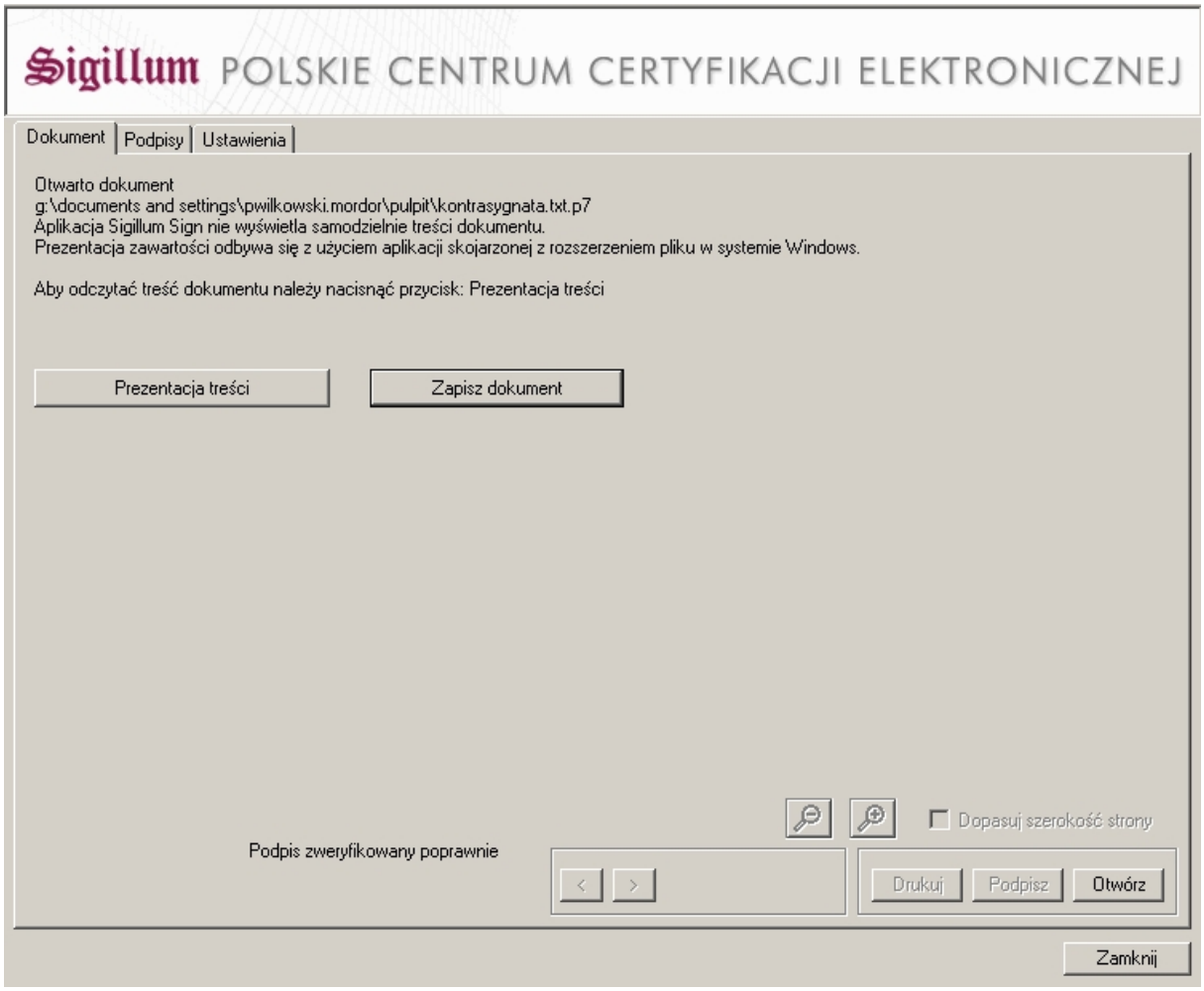


Zakładka ta pozwala na ustawienia podglądu pliku .sdoc. Istnieje możliwość powiększenia i pomniejszenia wyświetlanego pliku oraz przejście do następnej lub poprzedniej strony, jeśli plik zawiera więcej niż jedną stronę. Zaznaczanie opcji Dopasuj szerokość strony, automatycznie zmieni rozmiar wyświetlanego dokumentu, aby mieścił się w szerokości okna przeglądarki SignOnViewer. Przycisk *Drukuj*, służy do wydrukowania wczytanego pliku w oknie aplikacji SignOnViewer. Przycisk *Otwórz* pozwala na otworzenie podpisanego pliku .sdoc, .signpro, .sig, .xml, .pem, .p7 w celu zweryfikowania podpisu pliku. Użycie przycisku *Zamknij* spowoduje wyjście z aplikacji SignOnViewer

W przypadku gdy wczytany został plik podpisany z rozszerzeniem innym niż .sdoc czyli .signpro, .pem, .sig, .p7, .xml w oknie przeglądarki pojawią się dodatkowe dwa przyciski:

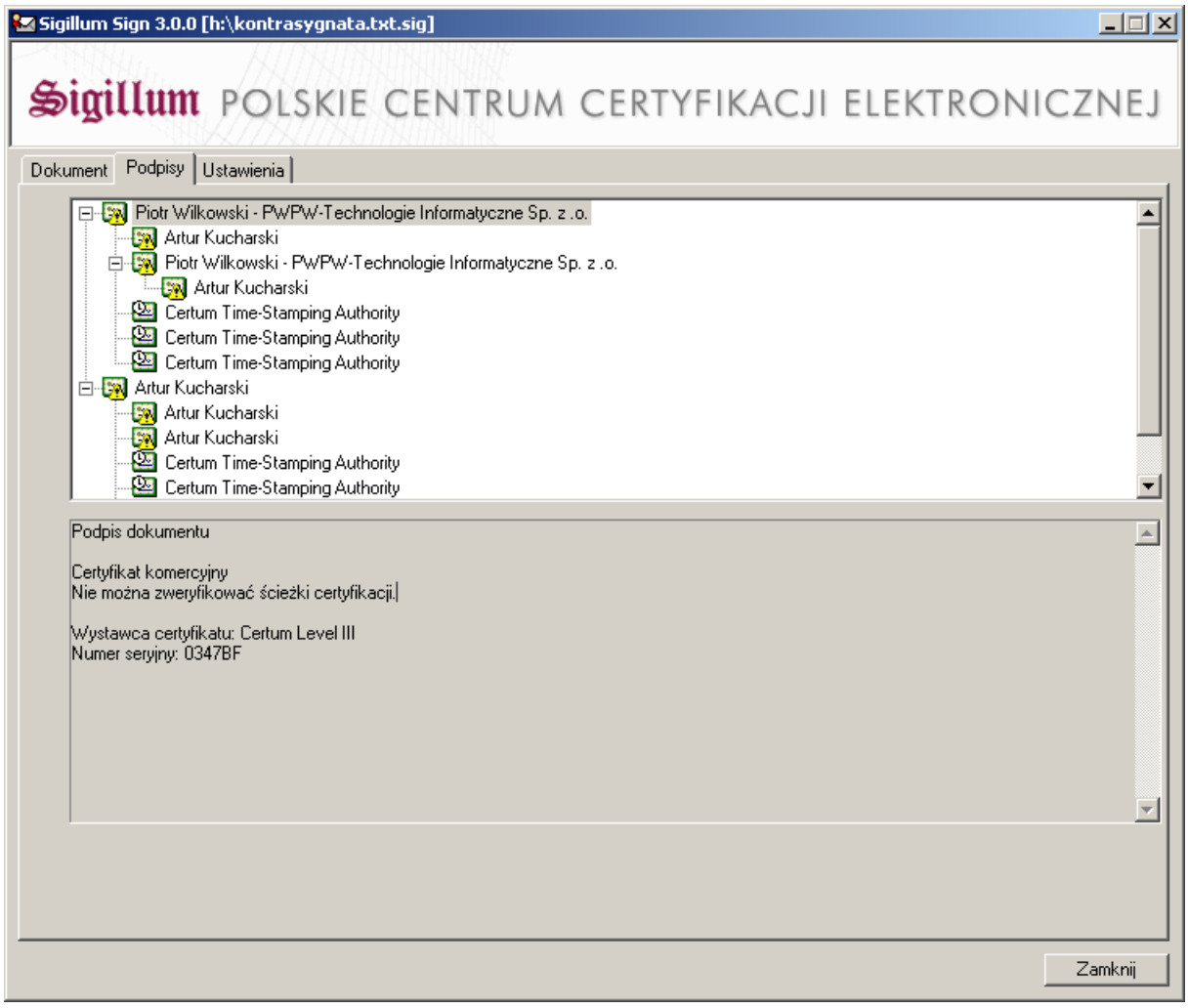
Prezentacja treści – służy do uruchomienia podpisanego pliku przy pomocy skojarzonej aplikacji

Zapisz dokument – służy do zapisania pliku źródłowego we wskazanym miejscu na dysku.



5.3. Zakładka Podpisy

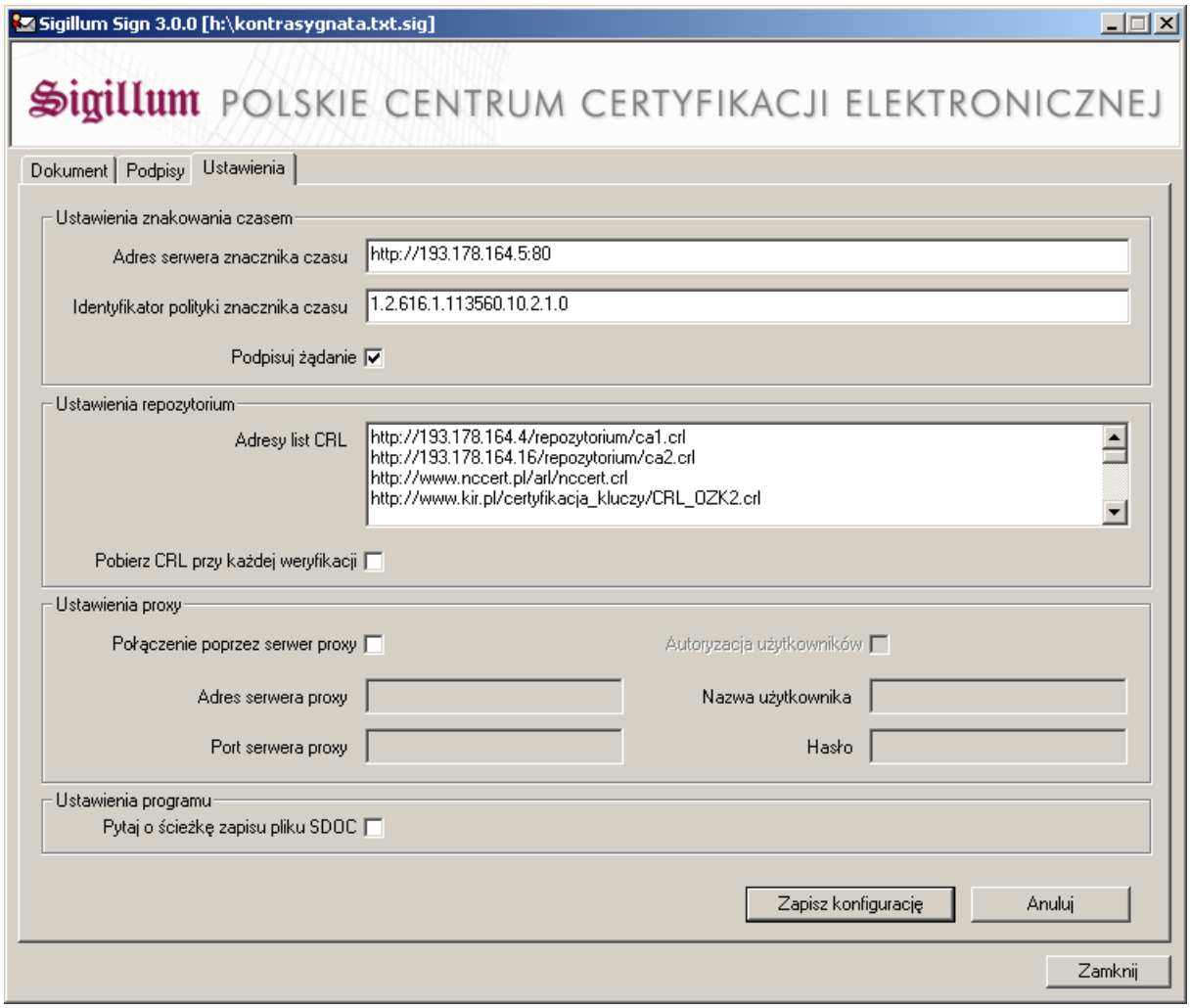
Zakładka podpisy prezentuje w formie graficznej i opisowej statusy podpisów, znaczników czasu i kontrasygnat do pliku w postaci drzewa. Dodatkowo wyświetlane są opcje o osobie dla której certyfikat został wystawiony, informacje o wystawcy certyfikatu, rodzaju podpisu i numerze seryjnym certyfikatu. Aby obejrzeć szczegóły certyfikatu, należy dwukrotnie kliknąć na certyfikat osoby znajdujący się na białym polu.



5.4. Zakładka Ustawienia

W zakładce ustawienia znajduje się główny panel zarządzania aplikacją SignOnViewer. W sekcji *Ustawienia znakowania czasem* znajdują się pola do konfiguracji adresu serwera znacznika czasu i identyfikatora polityki znacznika czasu. Aby aplikacja miała możliwość znakowania czasem opcja *Podpisuj żądanie* musi być zaznaczona. W następnej sekcji Ustawienia repozytorium, istnieje możliwość dodawania, usuwania i edycji list certyfikatów unieważnionych CRL. Poniżej znajduję się opcja *Pobierz CRL przy każdej weryfikacji.* Zaznaczenie spowoduje, każdorazowe pobranie aktualnych list CRL przy weryfikacji pliku.
Kolejna sekcja *Ustawienia proxy* pozwala na dodatkowe ustawienia sieci. W przypadku korzystania z serwera Proxy należy zaznaczyć *Połączenie poprzez serwer Proxy* i wprowadzić dane dotyczące adresu i portu serwera Proxy. Jeżeli

serwer Proxy wymaga autoryzacji, należy zaznaczyć opcję *Autoryzacja użytkowników* i uzupełnić dane do zalogowania się na serwerze Proxy.
Istnieje możliwość wymuszenia na aplikacji SignOnViewer wyświetlenia okna z zapytaniem o ścieżkę pliku dla .sdoc, w tym celu należy zaznaczyć opcję *Pytaj o ścieżkę zapisu pliku SDOC*.



5.5. Zachowanie konfiguracji

Aby wszelkie wprowadzone zmiany w konfiguracji zostały zapamiętane, należy wcisnąć przycisk „Zapisz konfigurację” a następnie „Zamknij”. Zmiany zostaną uwzględnione przy następnym uruchomieniu aplikacji.

6. PROBLEMY I BŁĘDY

Najczęściej występujące problemy

Brak podłączenia stacji roboczej do sieci Internet – pobieranie list CRL