



Podręcznik użytkownika

proCertum SmartSign 9.3

Wersja dokumentacji 1.38

Autorskie prawa majątkowe do tej dokumentacji oraz opisywanego przez nią oprogramowania przysługują **Asseco Data Systems S.A.** z siedzibą w Gdańsku, ul. Jana z Kolna 11. Powyższe prawa są chronione ustawą o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24, poz. 83 z dnia 4 lutego 1994 roku z późniejszymi zmianami).

Poniższa dokumentacja jest rozpowszechniana na podstawie udzielonej licencji.

Spis treści

1. WSTĘP	4
2. WYMAGANIA SPRZĘTOWE I PROGRAMOWE	5
3. AKTUALIZACJA APLIKACJI	6
3.1. Aktualizacja pakietu EXE	6
3.2. Aktualizacja pakietu MSI	8
4. INSTALACJA APLIKACJI	9
5. OBSŁUGA APLIKACJI	14
5.1. Pomoc	16
5.2. Ustawienia	18
5.2.1. Ustawienia – Ogólne	18
5.2.2. Ustawienia – Podpis	19
5.2.3. Ustawienia – Weryfikacja	25
5.2.3.1. Podstawowe opcje weryfikacji	25
5.2.3.2. Dodatkowe opcje weryfikacji	26
5.2.4. Ustawienia – Znacznik czasu	26
5.3. Podpisywanie plików	27
5.3.1. Dodawanie elementów do listy	28
5.3.2. Operacja podpisu	28
5.3.3. Podpis wielokrotny	34
5.3.4. Kontrasygnata	36
5.3.5. Podpisywanie plików PDF	39
5.3.5.1. Dodawanie graficznego symbolu podpisu	39
5.3.6. Menu kontekstowe	42
5.4. Weryfikowanie podpisów	43
5.4.1. Dodawanie elementów do listy	44
5.4.2. Informacje o podpisie i weryfikowanym dokumencie	44
5.4.3. Operacja weryfikacji	46
5.4.4. Status weryfikacji	48
5.4.5. Menu kontekstowe	50
5.5. Systemowe menu kontekstowe	51
5.6. Uruchamianie z linii poleceń	52
5.6.1. Przykłady	52
5.6.1.1. Podpisywanie plików	52
5.6.1.2. Weryfikowanie podpisów	54
5.6.1.3. Wyświetlenie informacji o podpisie	55
5.7. Powiadamianie o aktualizacji	56
6. SPIS RYSUNKÓW	58

1. Wstęp

proCertum SmartSign to aplikacja umożliwiająca składanie i weryfikację podpisu elektronicznego na pliku.

Uwaga: Zalecane jest używanie aktualnej wersji oprogramowania **proCertum SmartSign** do pobrania ze strony:

<https://pomoc.certum.pl/pl/oprogramowanie/procertum-smartsign/>

Aplikacja **proCertum SmartSign**:

- obsługuje certyfikaty kwalifikowane wydane zarówno przez Asseco Data Systems S.A. jak i KIR, PWPW, Enigma oraz Eurocert. Karty KIR Graphite, PWPW Dark, Enigma oraz Eurocert obsługiwane są wyłącznie przez interfejs CSP.
- obsługuje certyfikaty niekwalifikowane wydane przez Asseco Data Systems S.A.
- tworzy podpisy elektroniczne w formacie **XAdES**, **CAdES/ETSI**, **PAdES**. W przypadku podpisu **XAdES** lub **CAdES/ETSI** utworzony podpis może być **podpisem wewnętrznym** (plik podpisu będzie zawierał treść dokumentu), lub **podpisem zewnętrznym** (plik podpisu będzie zawierał tylko informacje o podpisie).
- oznacza dokumenty **kwalifikowanym lub niekwalifikowanym znacznikiem czasu**, gdy wymagane jest odniesienie do wiarygodnego czasu i stwierdzenie, że dokument lub podpis istniał w danej chwili.

UWAGA!!!

Zgodnie z artykułem 137 Ustawy o usługach zaufania oraz identyfikacji elektronicznej od dnia 1 lipca 2018 r. algorytm funkcji skrótu SHA-1 stosowany przy składaniu kwalifikowanych podpisów elektronicznego, zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych powinien być zastąpiony algorytmem funkcji skrótu SHA-2. W związku z tym aplikacja **proCertum SmartSign** umożliwia składanie podpisów tylko przy użyciu algorytmu SHA-2.

Niezależnie od posiadanej wersji oprogramowania jedyną rekomendowaną funkcją skrótu jest funkcja skrótu SHA2.

2. Wymagania sprzętowe i programowe

Poniżej podano minimalne wymagania sprzętowo-programowe umożliwiające prawidłową pracę programu **proCertum SmartSign**:

- komputer klasy PC/Laptop;
- system operacyjny (architektura x86-64): Windows 10, Windows 11;
- skonfigurowane połączenie internetowe;
- czytnik kart kryptograficznych*;
- karta z kryptoprocesorem*;
- oprogramowanie sterujące pracą czytników*;

***Uwaga!**

Czytnik kart kryptograficznych, karta z kryptoprocesorem oraz oprogramowanie sterujące pracą czytników są wymagane tylko w przypadku operacji składania podpisu przy użyciu karty kryptograficznej.

Ponadto, do poprawnej pracy aplikacji, wymagane jest aby aplikacja miała dostęp do następujących adresów:

213.222.201.0 - 213.222.201.255

213.222.198.0 - 213.222.198.255

<http://time.certum.pl>

<http://public-qlts.certum.pl>

<http://public-qlts.certum.pl/qts-17>

<http://qts10.clide.certum.pl>

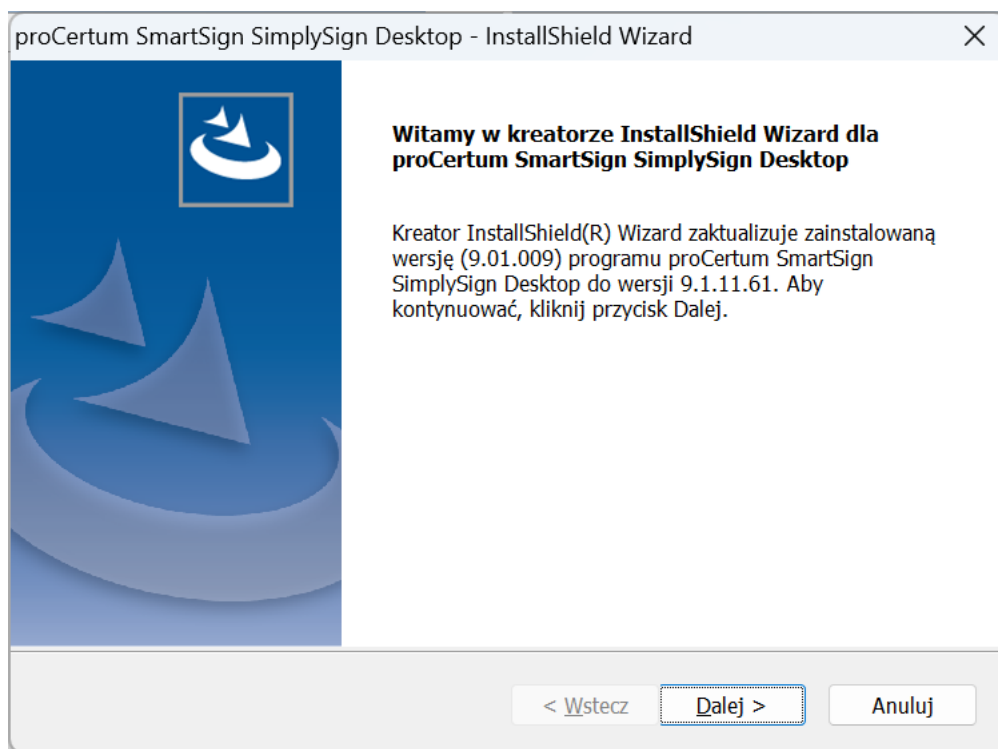
<http://qts.certum.pl/default/clide>

<http://ocsp.certum.pl/>

3. Aktualizacja aplikacji

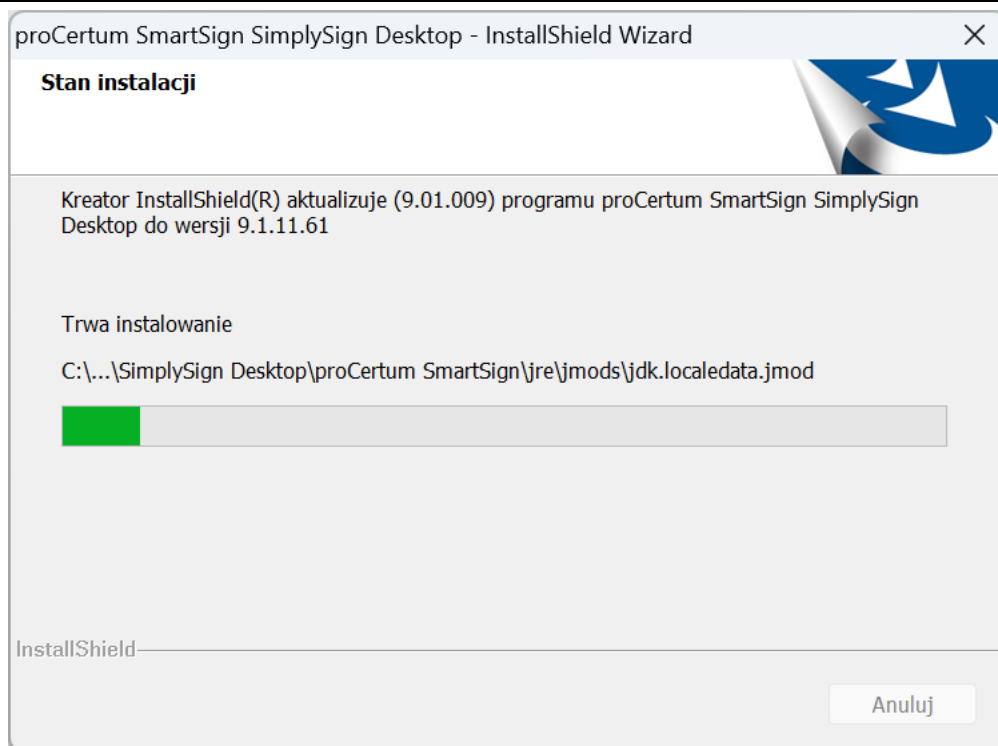
3.1. Aktualizacja pakietu EXE

W celu aktualizacji aplikacji zainstalowanej z pakietu EXE, należy pobrać odpowiedni nowy pakiet EXE, **wyłączyć** aplikację **proCertum SmartSign** i **SimplySign Desktop** i następnie uruchomić pobrany pakiet EXE. Włączone zostanie okno instalatora z informacją, o tym, że przeprowadzona zostanie aktualizacja.



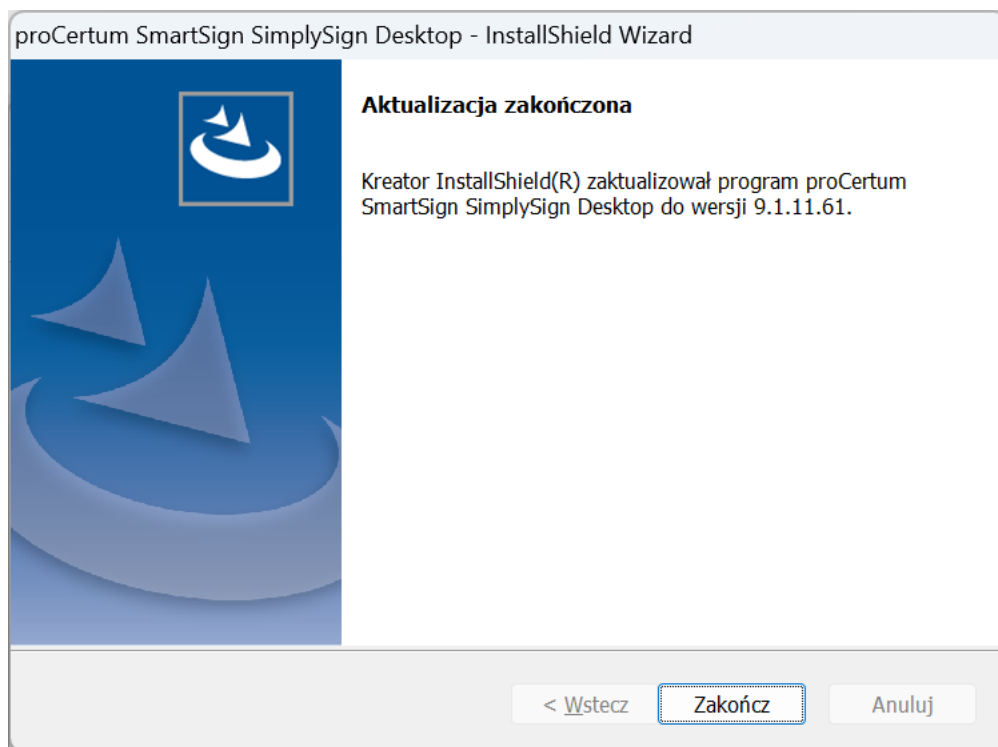
Rysunek 1: Informacja o aktualizacji

Po naciśnięciu przycisku **Dalej** rozpocznie się aktualizacja aplikacji.



Rysunek 2: Przebieg procesu aktualizacji

Po przeprowadzonej aktualizacji instalator wyświetli okno z informacją o jej zakończeniu.



Rysunek 3: Informacja o zakończeniu aktualizacji

3.2. Aktualizacja pakietu MSI

W celu aktualizacji aplikacji zainstalowanej z pakietu MSI, należy pobrać odpowiedni nowy pakiet MSI, **wyłączyć** aplikacje **proCertum SmartSign** i **SimplySign Desktop** i następnie uruchomić pobrany pakiet MSI poleceniem:

msiexec /i pobrany_pakiet.msi

i postępować zgodnie z kreatorem instalacji.

Można również dokonać aktualizacji w tzw. **trybie cichym** wydając polecenie:

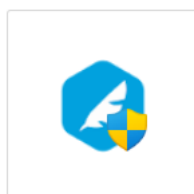
msiexec /i pobrany_pakiet.msi /q

Wtedy aktualizacja zostanie wykonana bez pokazywania okien instalatora.

4. Instalacja aplikacji

Aby rozpocząć pracę z aplikacją **proCertum SmartSign** należy ją poprawnie zainstalować w systemie. W tym celu należy dwukrotnie nacisnąć ikonę pliku **SimplySignDesktop-win.exe**

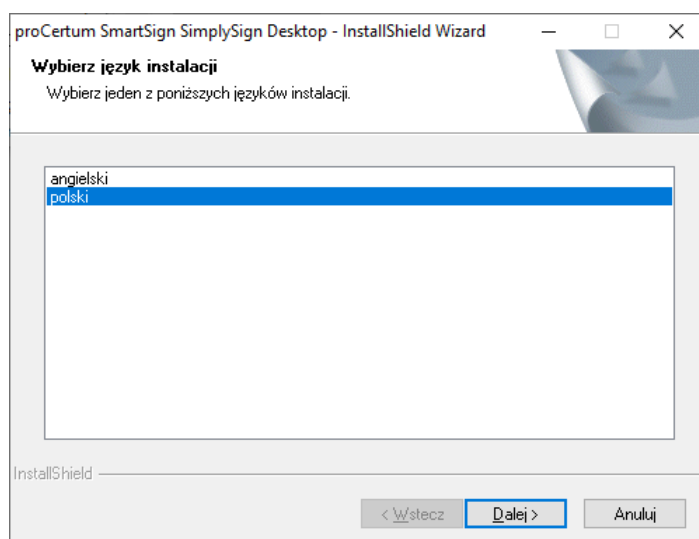
Uwaga! Jeśli w systemie była zainstalowana wcześniejsza wersja oprogramowania, zaleca się uprzednie odinstalowanie jej.



SimplySignDeskt
op-9.3.2.66-win-
64-bit.exe

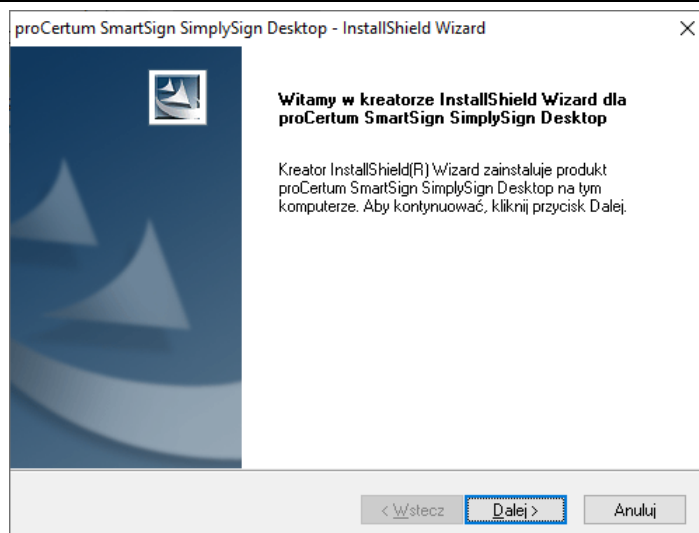
Rysunek 4: Ikona instalatora

Po uruchomieniu instalacji pokaże się następujące okno:



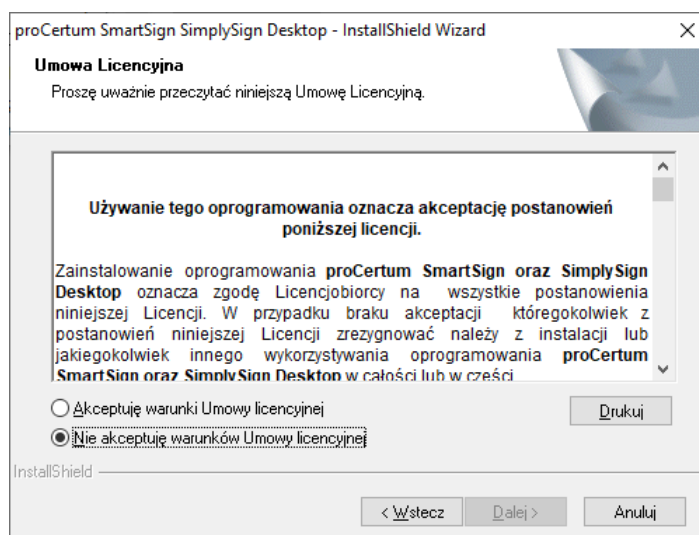
Rysunek 5: Wybór języka oprogramowania

Należy wybrać język, w którym przeprowadzona zostanie instalacja i w którym będzie działała aplikacja. Następnie należy nacisnąć przycisk **Dalej** – pojawi się okno powitalne kreatora instalacji.



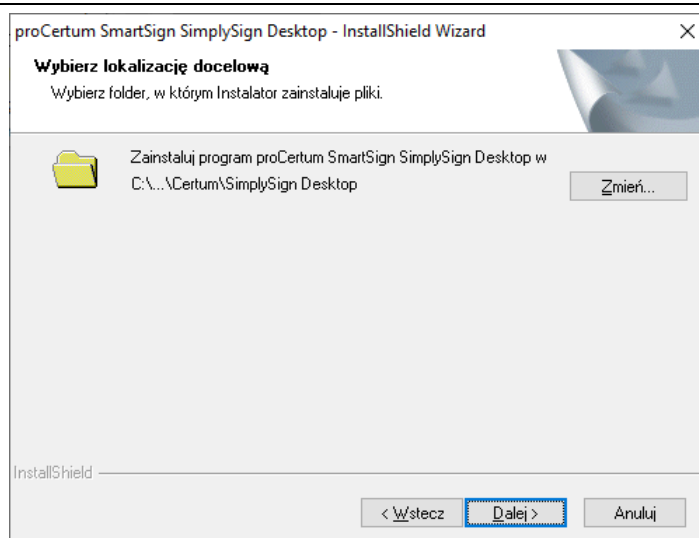
Rysunek 6: Okno powitalne kreatora instalacji

Po naciśnięciu przycisku **Dalej >** w oknie pojawi się Umowa licencyjna. Należy zapoznać się z jej treścią. Po jej zaakceptowaniu należy zaznaczyć opcję **Akceptuję warunki Umowy Licencyjnej** i nacisnąć przycisk **Dalej >**. W przeciwnym wypadku (po zaznaczeniu opcji **Nie akceptuję warunków Umowy Licencyjnej**) odrzucimy zapisy umowy licencyjnej i dalsza instalacja nie będzie możliwa.



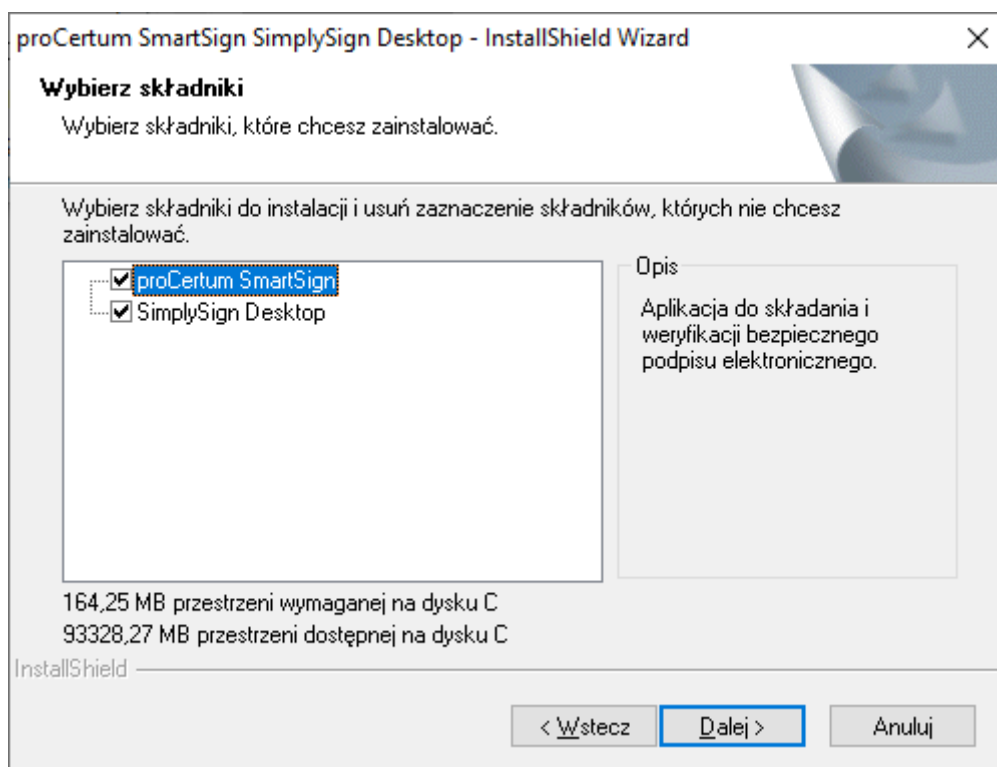
Rysunek 7: Umowa licencyjna

Następnym etapem będzie wybór miejsca, w którym zostaną zainstalowane pliki aplikacji **proCertum SmartSign**.



Rysunek 8: Wybór katalogu docelowego aplikacji

Domyślnie jest to: **C:\Program Files\Certum\SimplySign Desktop\proCertum SmartSign**. Jeśli chcemy zmienić miejsce docelowe należy kliknąć przycisk **Zmień...** i ustawić nowe miejsce docelowe. Po wybraniu miejsca docelowego należy kliknąć przycisk **Dalej >**. Wyświetlone zostaną komponenty, które można zainstalować.



Rysunek 9: Wybór komponentów, które zostaną zainstalowane

Komponenty, które można zainstalować to:

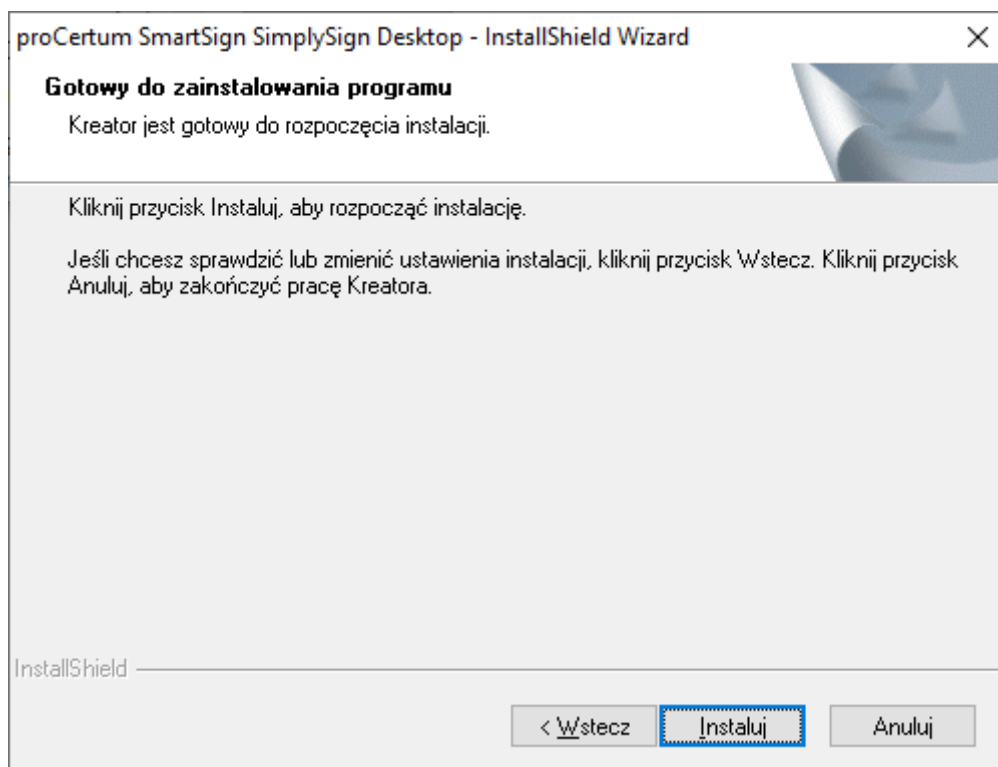
- **proCertum SmartSign** – aplikacja proCertum SmartSign;
- **SimplySign Desktop** – aplikacja SimplySign Desktop;

Osoby posiadające tylko fizyczną kartę kryptograficzną powinny odznaczyć komponent **SimplySign**

i pozostawić zaznaczony tylko komponent **proCertum SmartSign**.

Osoby posiadające certyfikat na karcie wirtualnej **SimplySign** powinny pozostawić zaznaczone obydwa komponenty.

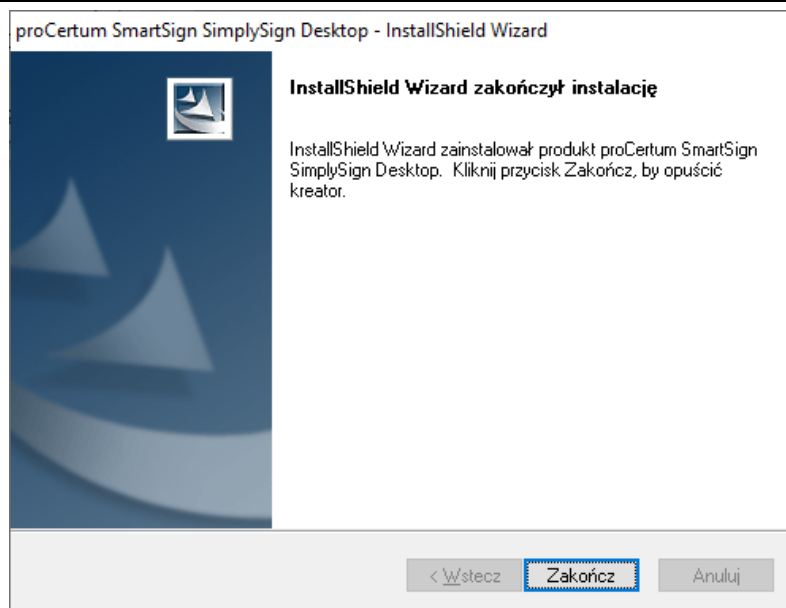
Po zaznaczeniu odpowiednich komponentów należy nacisnąć przycisk **Dalej**. Wyświetlone zostanie okno informujące o gotowości do instalacji.



Rysunek 10: Instalator jest gotowy do rozpoczęcia procesu instalacji

Po naciśnięciu przycisku **Instaluj** rozpocznie się instalowanie wybranych komponentów.

Jeśli komponenty zostaną poprawnie zainstalowane to pojawi się następujący komunikat:



Rysunek 11: Zakończenie procesu instalacji

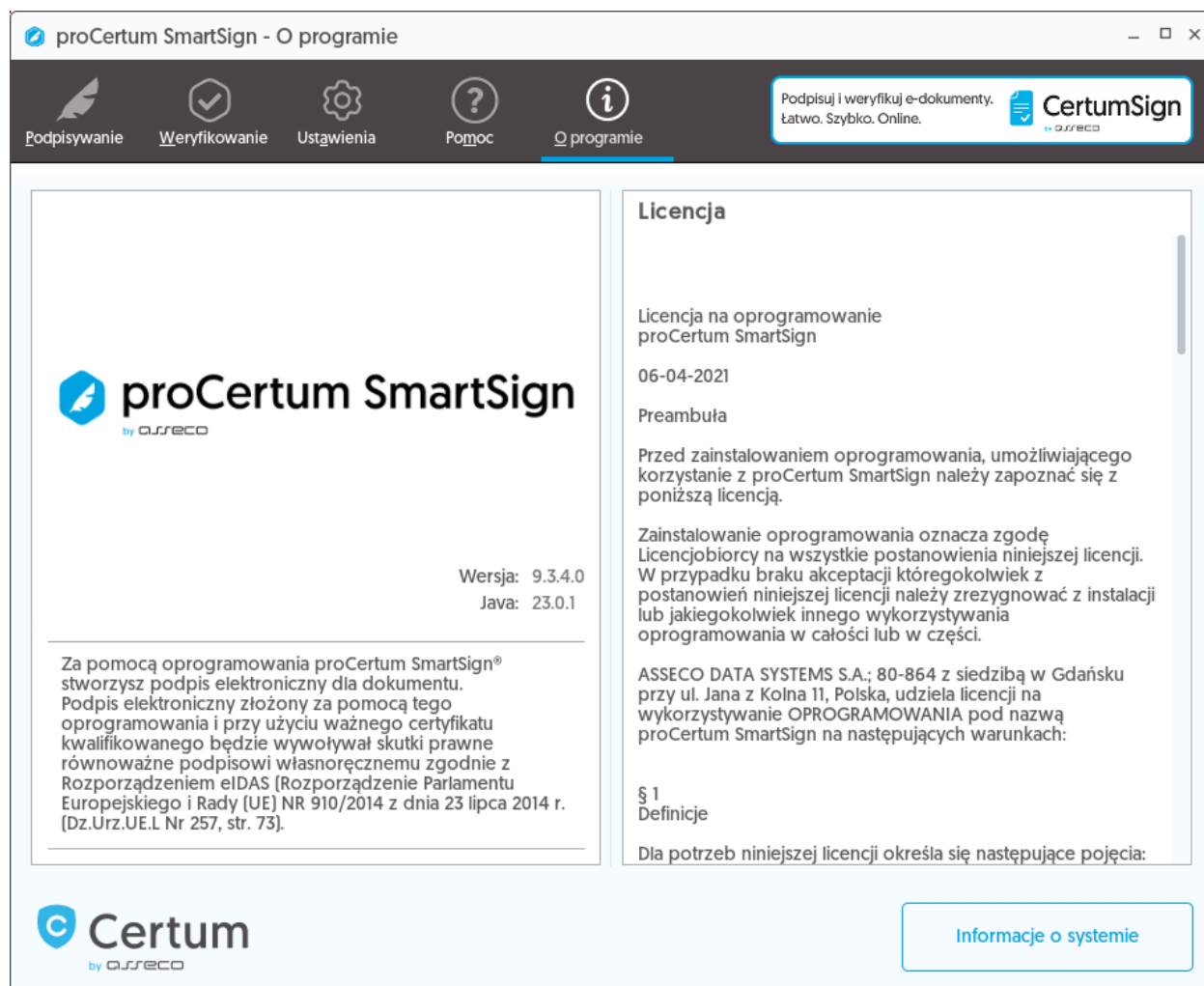
Naciśnięcie przycisku **Zakończ** zamyka kreatora instalacji aplikacji.

Aby uruchomić aplikację należy nacisnąć ikonę **proCertum SmartSign** dostępną na pulpicie lub w menu Start > Programy > Certum > proCertum SmartSign.

Aby uruchomić aplikację należy nacisnąć ikonę **SimplySign Desktop** dostępną na pulpicie lub w menu Start > Programy > Certum > SimplySign Desktop.

5. Obsługa aplikacji

Aplikacja **proCertum SmartSign** służy do składania i weryfikacji podpisu cyfrowego.

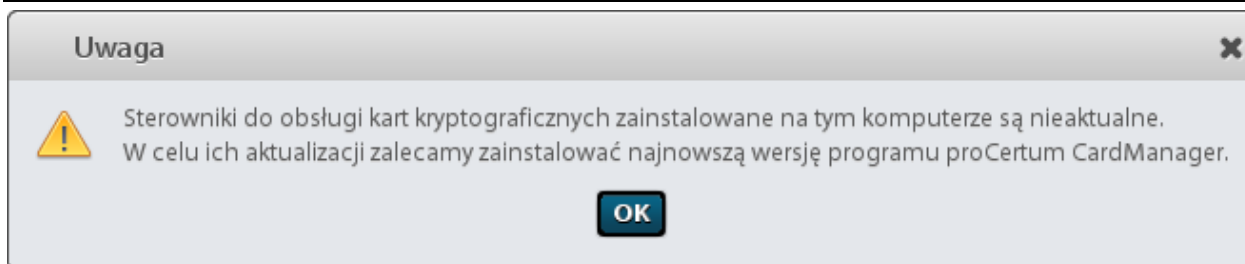


Rysunek 12: Okno główne aplikacji proCertum SmartSign

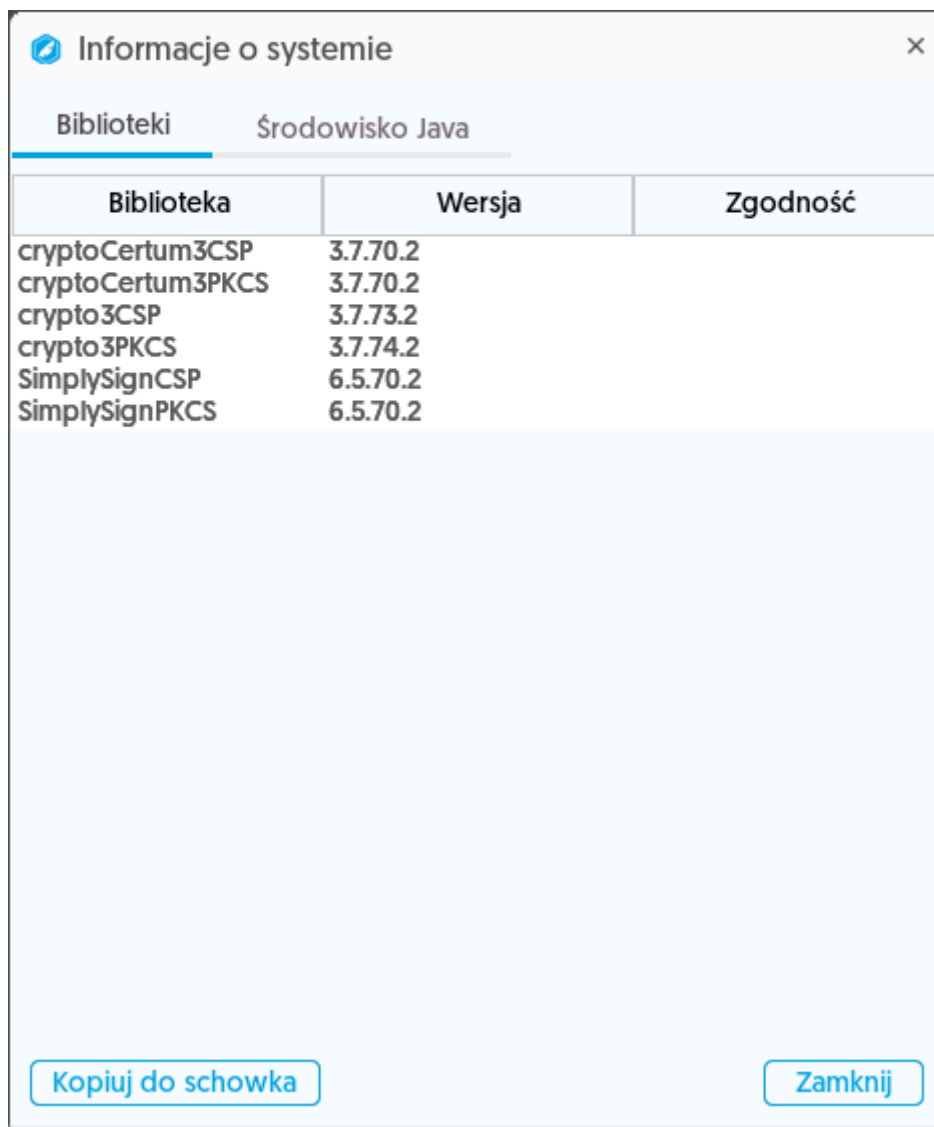
W aplikacji **proCertum SmartSign** możemy wyróżnić pięć zakładek:

- **Podpisywanie** – umożliwia realizację operacji złożenia podpisu elektronicznego, umożliwia także złożenie podpisu wielokrotnego i kontrasygnaty pod istniejącym podpisem;
- **Weryfikowanie** – umożliwia realizację operacji weryfikacji podpisu elektronicznego;
- **Ustawienia** – umożliwia konfigurację usługi podpisywania i weryfikacji oraz ustawień ogólnych;
- **Pomoc** – wyświetla dokumentację aplikacji;
- **O programie** – wyświetla informacje na temat wersji oprogramowania oraz licencji, a także daje możliwość wglądu w **Informacje o systemie**.

W oknie powitalnym oraz w oknie **O programie** znajduje się przycisk **Informacje o systemie**. Jego naciśnięcie powoduje wyświetlenie okna zawierającego informacje o środowisku, w którym uruchomiona została aplikacja. W oknie tym, w zakładce **Biblioteki** prezentowana jest lista bibliotek służących do obsługi kart kryptograficznych. Aplikacja posiada wbudowany mechanizm weryfikacji tych bibliotek i w przypadku stwierdzenia niezgodności, w kolumnie **Zgodność** wyświetla stosowną informację na ten temat. Weryfikacja bibliotek odbywa się również podczas każdego uruchamiania aplikacji. W przypadku stwierdzenia niezgodności jakiegokolwiek biblioteki pojawia się informacja o tym.

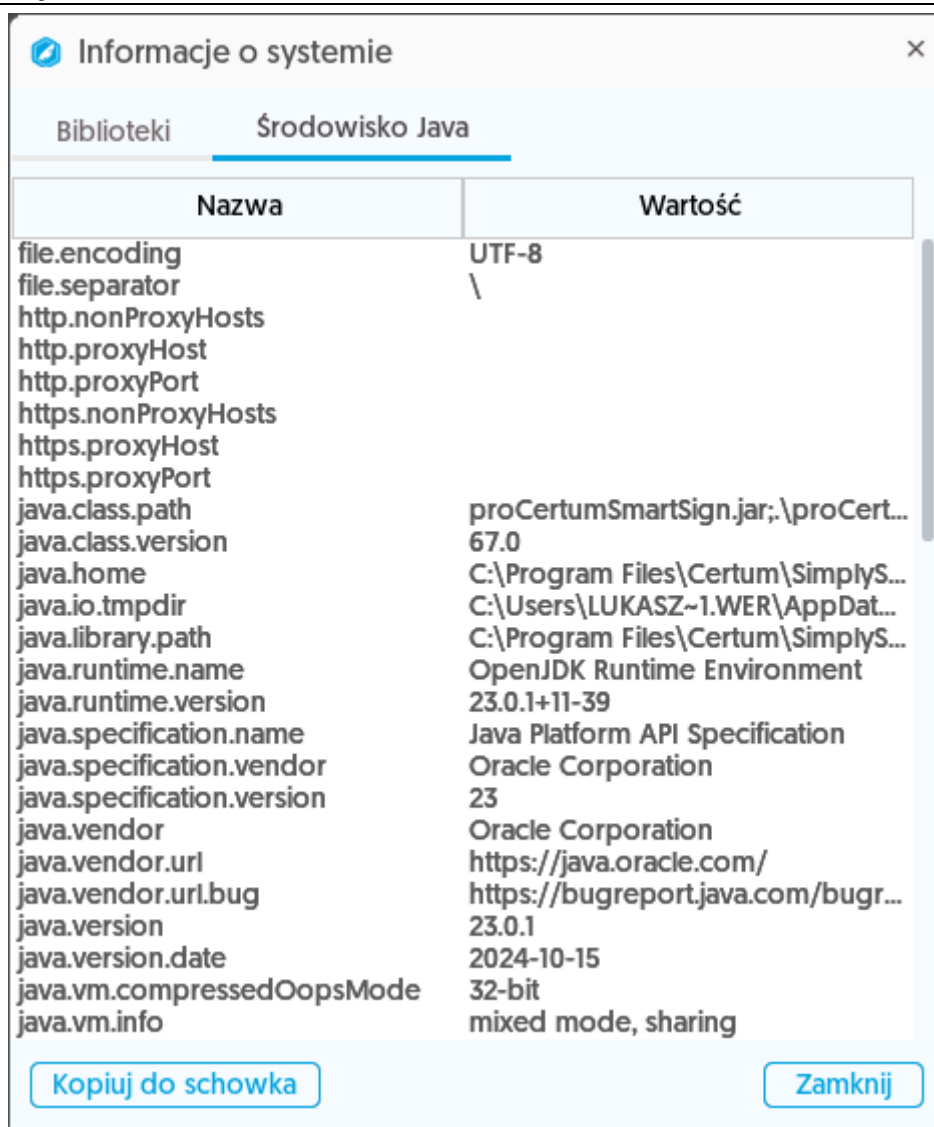


Rysunek 13: Informacja o niezgodności bibliotek



Rysunek 14: Informacje o systemie– Zakładka Biblioteki

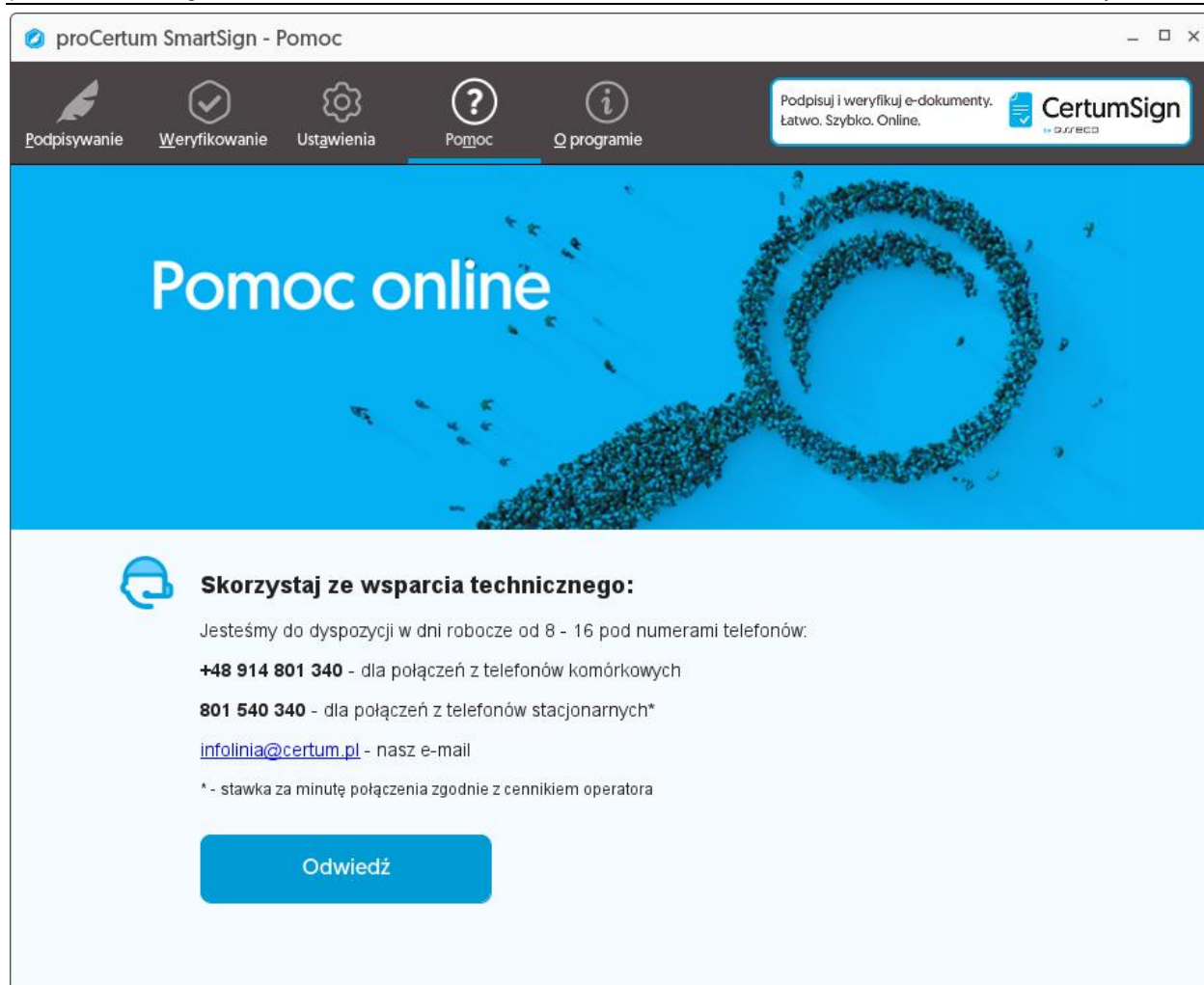
Na zakładce **Środowisko Java** prezentowane jest okno z informacjami na temat środowiska Java, w którym pracuje aplikacja.



Rysunek 15: Informacje o systemie– Zakładka Środowisko Java

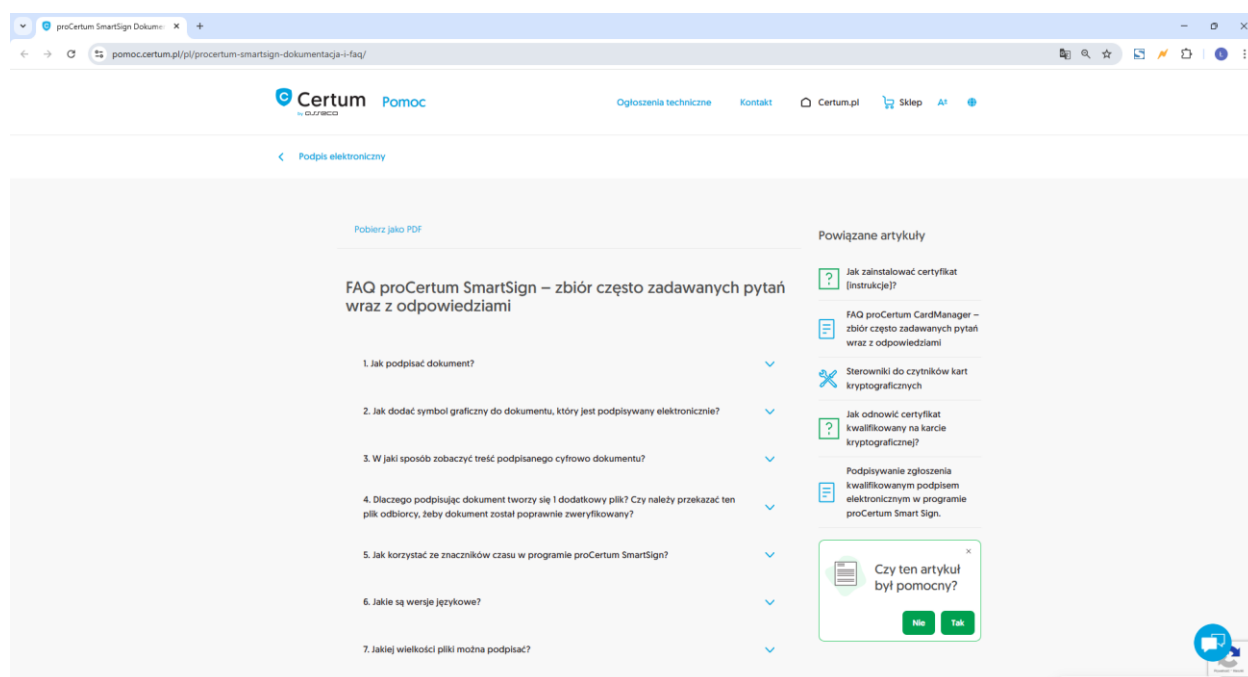
5.1. Pomoc

W celu uzyskania pomocy w zakresie obsługi aplikacji należy kliknąć przycisk **Pomoc**.



Rysunek 16: Zakładka Pomoc

Po naciśnięciu przycisku **Odwiedź** użytkownik zostanie przekierowany do strony www z najczęściej zadawanymi pytaniami i odpowiedziami do nich.



Rysunek 17: Zakładka Pomoc strona WWW

5.2. Ustawienia

Zakładka **Ustawienia** przeznaczona jest do konfiguracji ustawień:

- ogólnych;
- operacji składania podpisu elektronicznego;
- operacji weryfikacji podpisu elektronicznego;
- operacji znakowania czasem podczas składania lub weryfikacji podpisu elektronicznego;

'>

Rysunek 18: Zakładka - Ustawienia

Dodatkowo w Panelu ustawień znajduje się przycisk **Przywróć ustawienia domyślne** pozwalający powrócić do domyślnych ustawień programu.

5.2.1. Ustawienia – Ogólne

Zakładka **Ogólne** umożliwia konfigurację ustawień serwera proxy oraz automatycznego powiadamiania o aktualizacjach.

- **Aktualizacje** – aby zmienić okres czasu, co jaki ma być sprawdzana dostępności aktualizacji należy z listy rozwijanej wybrać jedną z dostępnych opcji : raz dziennie, raz na tydzień, raz na miesiąc, nigdy. Dodatkowo, w dowolnej chwili można samodzielnie sprawdzić, czy dostępne są aktualizacje poprzez naciśnięcie przycisku **Sprawdź teraz**.
- **Proxy** – po zaznaczeniu opcji **Używaj proxy** zostaną odblokowane dodatkowe pola do

konfiguracji ustawień proxy:

- **Host** – adres serwera proxy. (pole obowiązkowe)
- **Port** – port komunikacji z serwerem proxy. (pole obowiązkowe)
- **Wyłącz proxy dla** – wyłącza komunikację z serwerem proxy dla hostów wymienionych w polu np. **192.168.0.2 | 192.168.0.3**. (pole opcjonalne)

Jeśli serwer proxy wymaga uwierzytelnienia należy zaznaczyć opcję **Wymagana autoryzacja**, wtedy zostaną odblokowane dodatkowe pola:

- **Użytkownik** – identyfikator użytkownika serwera proxy. (pole obowiązkowe)
- **Hasło** – hasło użytkownika. (pole opcjonalne)
- **Historia** – po zaznaczeniu tej opcji zostanie udostępniona opcja zapisywania logów. Aplikacja generuje osobny plik logów, w którym rejestrowany jest czas, typ podpisu i nazwa pliku podpisu, CN certyfikatu oraz status operacji. Plik logów zapisywany jest w katalogu domowym użytkownika. Zawartość pliku logów jest przedstawiona w aplikacji w postaci tabeli w Panelu konfiguracyjnym.

proCertum SmartSign - Ustawienia

Podpisywanie Weryfikowanie Ustawienia Pomoc O programie

Podpisuj i weryfikuj e-dokumenty. Łatwo. Szybko. Online. CertumSign

Ogólne Podpis Weryfikacja Znacznik czasu

AKTUALIZACJE

Sprawdzanie dostępnych aktualizacji: raz dziennie [Ostatnio sprawdzano: 2025-12-08 13:00:21] Sprawdź

PROXY

☐ Używaj proxy ☐ Pobierz proxy automatycznie

Host Port

Wyłącz proxy dla

Poszczególne hosty rozdzielić znakiem "|"

☐ Wymagana autoryzacja

Użytkownik

Hasło

HISTORIA

☐ Zapisuj historię użycia certyfikatu

Ustawienia domyślne

Rysunek 19: Zakładka Ustawienia – Ogólne

5.2.2. Ustawienia – Podpis

Zakładka **Podpis** umożliwia konfigurację ustawień dla operacji podpisywania realizowanej w zakładce **Podpisywanie**.

proCertum SmartSign - Ustawienia

Podpisywanie Weryfikowanie Ustawienia Pomoc O programie

Podpisuj i weryfikuj e-dokumenty. Łatwo. Szybko. Online. CertumSign

Ogólne Podpis Weryfikacja Znacznik czasu

FORMAT PODPISU

☒ **XAdES**
Podpis XAdES - Podpis elektroniczny w formacie XAdES jest zgodny z najnowszymi standardami, jest oparty o język XML i zalecany do powszechnego stosowania.

☐ **CAdES/ETSI**
Podpis CAdES/ETSI - Podpis elektroniczny w formacie CAdES/ETSI jest starszym formatem podpisu elektronicznego.

TYP PODPISU

☐ **Podpis zewnętrzny**
Plik podpisu będzie zawierał tylko informacje o podpisie. Pamiętaj jednak, że w trakcie weryfikacji podpisu trzeba dostarczyć dokument wraz z podpisem.

☒ **Podpis wewnętrzny**
Plik podpisu będzie również zawierał treść dokumentu.

FUNKCJA SKRÓTU

Funkcja skrótu SHA-256

ARCHIWIZACJA

Ustawienia domyślne

Rysunek 20: Zakładka Ustawienia – Podpis – część dotycząca Formatu podpisu, Typu podpisu i ustawień Archiwizacji

Możemy określić następujące parametry:

- **Format podpisu:**
 - **XAdES** – Podpis elektroniczny w formacie **XAdES**;
 - **CAdES/ETSI** – Podpis elektroniczny w formacie **CAdES/ETSI**;
- **Funkcja skrótu** – parametr oznacza nazwę funkcji skrótu używanej podczas składania podpisu. Obecnie możliwe do wyboru tylko SHA-256;

UWAGA!!!

Zgodnie z artykułem 137 Ustawy o usługach zaufania oraz identyfikacji elektronicznej od dnia 1 lipca 2018 r. algorytm funkcji skrótu SHA-1 stosowany przy składaniu kwalifikowanych podpisów elektronicznego, zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych powinien być zastąpiony algorytmem funkcji skrótu SHA-2. W związku z tym aplikacja proCertum SmartSign umożliwia składanie podpisów tylko przy użyciu algorytmu SHA-2.

- **Typ podpisu:**

- **Podpis zewnętrzny** – plik podpisu będzie zawierał tylko informacje o podpisie. Należy pamiętać, że w trakcie weryfikacji podpisu trzeba dostarczyć podpisany dokument wraz z jego podpisem;
- **Podpis wewnętrzny** – plik podpisu będzie zawierał treść dokumentu.

proCertum SmartSign - Ustawienia

Podpisywanie Weryfikowanie Ustawienia Pomoc O programie

Podpisuj i weryfikuj e-dokumenty. Łatwo. Szybko. Online. CertumSign

Ogólne Podpis Weryfikacja Znacznik czasu

ARCHIWIZACJA

☐ Kopiuj po podpisaniu

Po wygenerowaniu podpisu zostanie on skopiowany do wybranego katalogu wraz z podpisanym dokumentem, jeśli wygenerowano podpis zewnętrzny.

C:\Users\lukasz.werkowski Wybierz

☒ Twórz podkatalogi w formacie: RRRR.MM.DD

DOMYŚLNY CERTYFIKAT

Informacje:

Podmiot: Wybierz

Wystawca: Pokaż

Numer seryjny: Usuń

DODATKOWE OPCJE PODPISU

☐ Przed podpisem pytaj o powód podpisu

☒ Twórz podpis specjalny PDF (PADES), gdy podpisywany jest dokument PDF

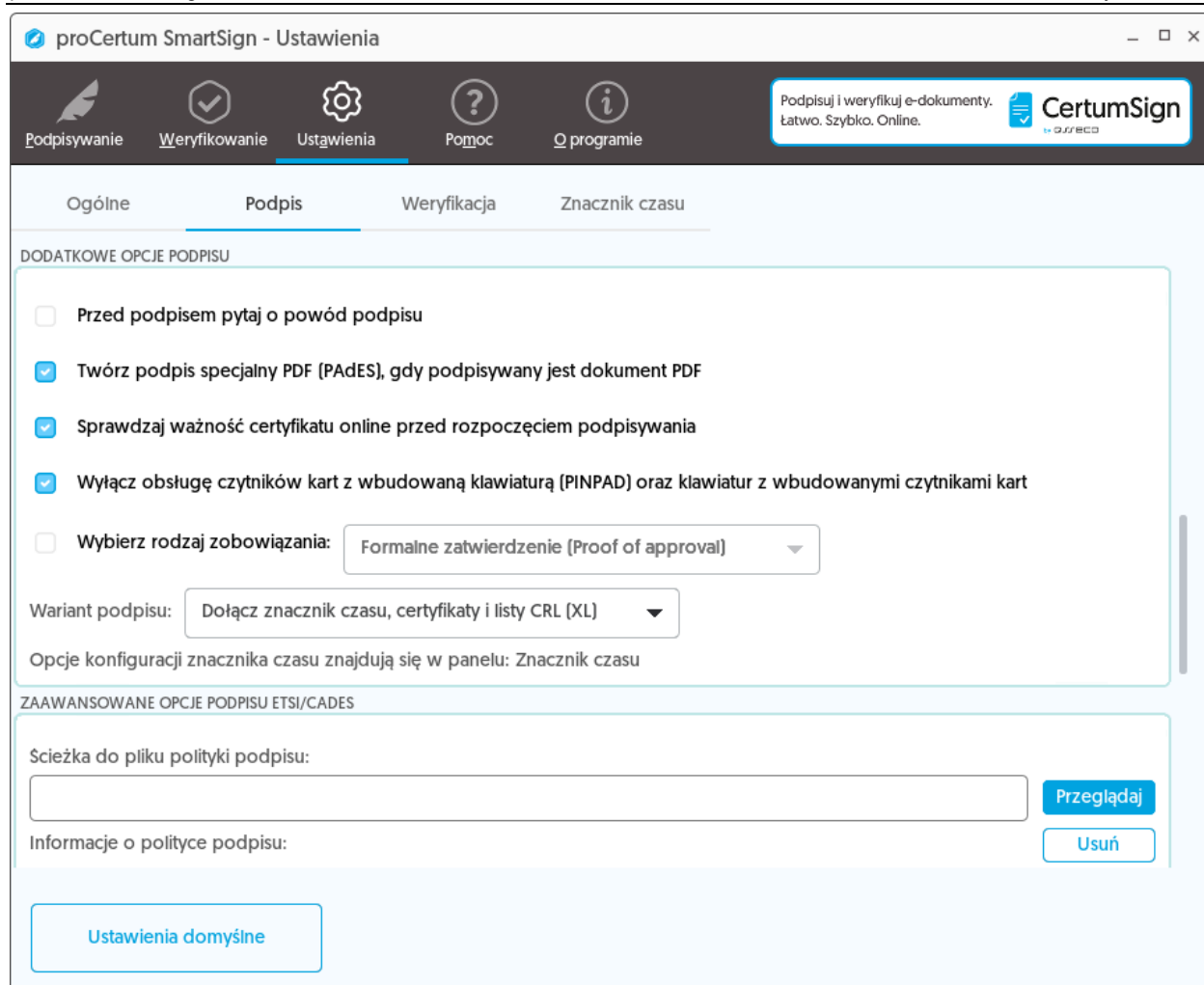
Ustawienia domyślne

Rysunek 21: Zakładka Ustawienia – Podpis – część dotycząca Domyślnego certyfikatu i dodatkowych opcji podpisu

- **Archiwizacja:**

- **Kopiuj po podpisaniu** – zaznaczenie tej opcji spowoduje umożliwienie wybrania katalogu do którego zostaną skopiowane pliki podpisu powstałe po zakończonej operacji podpisywania;
- **Twórz podkatalogi w formacie RRRR.MM.DD** – zaznaczenie tej opcji spowoduje, że w katalogu ustawionym dla podpisanych plików powstaną podkatalogi w formacie Rok.Miesiąc.Dzień stworzone na podstawie aktualnej daty.
- **Domyślny certyfikat** – opcja ta umożliwia wybranie certyfikatu który będzie domyślnym certyfikatem służącym do podpisywania.
 - **Wybierz certyfikat** – po naciśnięciu przycisku na listę zostaną wczytane wszystkie dostępne certyfikaty. Aby ustawić domyślny certyfikat należy wybrać jeden z certyfikatów i nacisnąć przycisk **OK**;
 - **Pokaż certyfikat** – po naciśnięciu przycisku zostaną wyświetlone szczegóły certyfikatu;
 - **Usuń certyfikat** – po naciśnięciu przycisku certyfikat zostanie usunięty z konfiguracji.

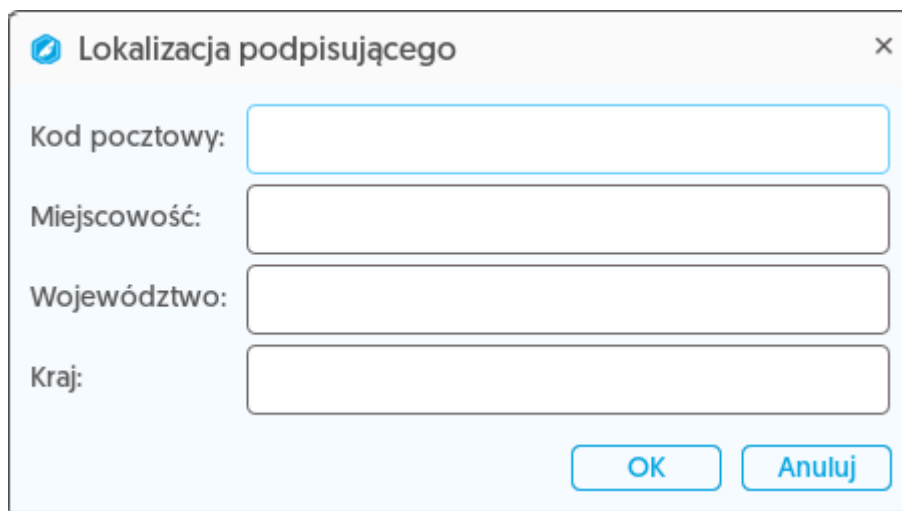
- **Dodatkowe opcje podpisu:**
 - **Przed podpisaniem pytaj o powód podpisu** – wybranie tej opcji spowoduje, że przed wykonaniem podpisu aplikacja zaprezentuje okno umożliwiające wybór powodu podpisu, który umieszczony zostanie w strukturze podpisu i prezentowany będzie później we właściwościach podpisu.
 - **Twórz podpis specjalny PDF (PAdES), gdy podpisywany jest dokument PDF** – wybranie tej opcji spowoduje, że w przypadku, gdy podpisywany plik będzie plikiem PDF to podpis zostanie umieszczony w wewnętrznej strukturze PDF i widoczny będzie po otwarciu pliku PDF w edytorze plików PDF.
 - **Sprawdź ważność certyfikatu online przed rozpoczęciem podpisywania** – wybranie tej opcji spowoduje, że certyfikat podpisujący będzie weryfikowany przed rozpoczęciem podpisywania plików.
 - **Wyłącz obsługę czytników kart z wbudowaną klawiaturą (PINPAD) oraz klawiatur z wbudowanym czytnikiem kart** – wybranie tej opcji spowoduje, że wyłączona zostanie obsługa kart z wbudowaną klawiaturą (PINPAD) oraz klawiatur z wbudowanym czytnikiem kart.
 - **Wybierz rodzaj zobowiązania (tylko podpis XAdES)** – umożliwia wybranie rodzaju zobowiązania dla którego tworzony jest podpis. Do wyboru są następujące rodzaje zobowiązań:
 - Formalne zatwierdzenie;
 - Potwierdzenie utworzenia;
 - Potwierdzenie dostawy;
 - Potwierdzenie pochodzenia;
 - Potwierdzenie odbioru;
 - Potwierdzenie nadania.
 - **Wariant podpisu** – umożliwia wybranie jednego z następujących wariantów podpisu:
 - **Nie dołączaj dodatkowych informacji (BES)** – wybranie tej opcji spowoduje, że podpis będzie tworzony w podstawowym formacie (bez znacznika czasu);
 - **Dołącz znacznik czasu (T)** – wybranie tej opcji spowoduje, że podpis będzie tworzony wraz ze znacznikiem czasu świadczącym o dacie złożenia podpisu – wymagane jest wtedy zdefiniowanie ustawień znacznika czasu na zakładce **Znacznik Czasu**;
 - **Dołącz znacznik czasu, certyfikaty i listy CRL (XL)** – wybranie tej opcji spowoduje, że podpis będzie tworzony w tzw. formacie rozszerzonym zawierającym znacznik czasu świadczący o dacie złożenia podpisu oraz zawierający listy CRL jako dowody ważności podpisu w chwili jego złożenia – wymagane jest wtedy zdefiniowanie ustawień znacznika czasu na zakładce **Znacznik Czasu**;



Rysunek 22: Zakładka Ustawienia – Podpis – część dotycząca zaawansowanych opcji podpisu

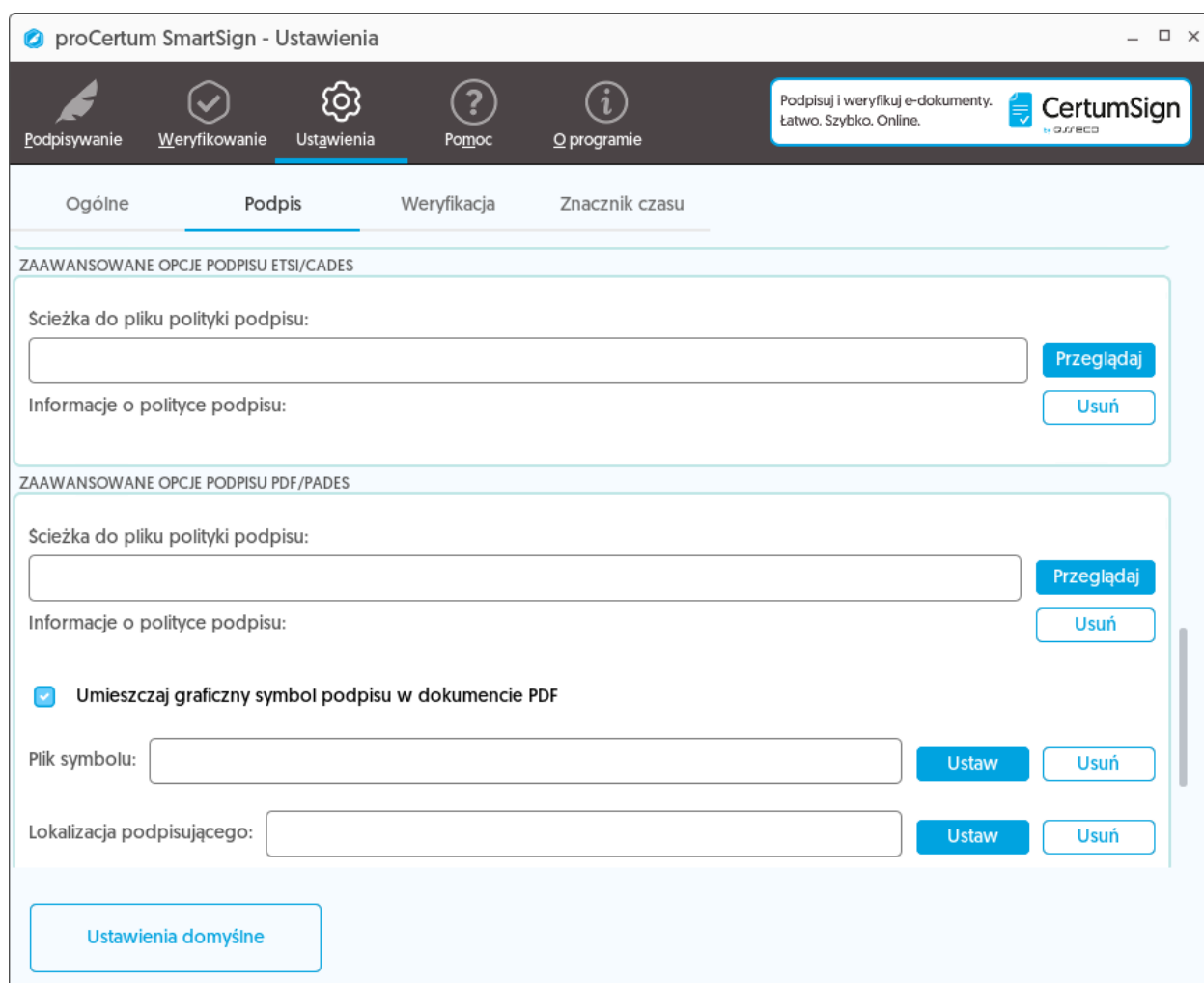
- Zaawansowane opcje podpisu ETSI/CADES
 - **Ścieżka do pliku polityki podpisu** – wskazuje na ścieżkę do pliku Polityki Podpisu definiującej kryteria składania i weryfikacji podpisu. Wybór odpowiedniej polityki podpisu dokonuje się przyciskiem **Przeglądaj**. Przycisk **Usuń** pozwala na usunięcie wybranej polityki i powrót do ustawienia domyślnego.
- Zaawansowane opcje podpisu PDF/PAdES
 - **Ścieżka do pliku polityki podpisu** – wskazuje na ścieżkę do pliku Polityki Podpisu definiującej kryteria składania i weryfikacji podpisu. Wybór odpowiedniej polityki podpisu dokonuje się przyciskiem **Przeglądaj**. Przycisk **Usuń** pozwala na usunięcie wybranej polityki i powrót do ustawienia domyślnego.
 - **Umieszczaj graficzny symbol podpisu w dokumencie PDF** – zaznaczenie tej opcji powoduje, że podczas podpisywania plików PDF, dla każdego pliku możliwe będzie wskazanie pliku graficznego, który posłuży jako graficzny symbol podpisu. Dodano dialog umożliwiający zastosowanie ustawienia graficznego symbolu podpisu pierwszego podpisywanego pliku PDF do kolejnych plików PDF podpisywanych w tym samym procesie.
 - **Plik symbolu** – opcja ta pozwala na zdefiniowanie pliku domyślnego symbolu podpisu umieszczanego w plikach PDF

- o **Lokalizacja podpisującego** - opcja pozwala na wskazanie w konfiguracji lokalizacji podpisującego dla podpisu PDF



Dialog box titled "Lokalizacja podpisującego" (Location of the signer). It contains four text input fields: "Kod pocztowy:" (Postal code), "Miejscowość:" (Locality), "Województwo:" (Voivodeship), and "Kraj:" (Country). At the bottom right, there are two buttons: "OK" and "Anuluj" (Cancel).

Rysunek 23: Zakładka Ustawienia – Podpis –Lokalizacja podpisującego



Screenshot of the "proCertum SmartSign - Ustawienia" (Settings) window, "Podpis" (Signature) tab. The window has a dark header with navigation icons and a "CertumSign" logo. Below the header, there are tabs: "Ogólne", "Podpis", "Weryfikacja", and "Znacznik czasu". The "Podpis" tab is active. The main content area is titled "ZAAWANSOWANE OPCJE PODPISU ETSI/CADES" and "ZAAWANSOWANE OPCJE PODPISU PDF/PADES". Under "ZAAWANSOWANE OPCJE PODPISU ETSI/CADES", there is a text field for "Ścieżka do pliku polityki podpisu:" with a "Przeglądaj" (Browse) button, and a button "Usuń" (Delete). Under "ZAAWANSOWANE OPCJE PODPISU PDF/PADES", there is a text field for "Ścieżka do pliku polityki podpisu:" with a "Przeglądaj" button, and a button "Usuń". Below this, there is a checked checkbox "Umieszczaj graficzny symbol podpisu w dokumencie PDF" (Place graphical signature symbol in PDF document). Below the checkbox, there is a text field for "Plik symbolu:" (Symbol file) with "Ustaw" (Set) and "Usuń" buttons. At the bottom, there is a text field for "Lokalizacja podpisującego:" (Location of the signer) with "Ustaw" and "Usuń" buttons. At the very bottom, there is a button "Ustawienia domyślne" (Default settings).

Rysunek 24: Zakładka Ustawienia – Podpis – Zaawansowane opcje podpisu XAdES

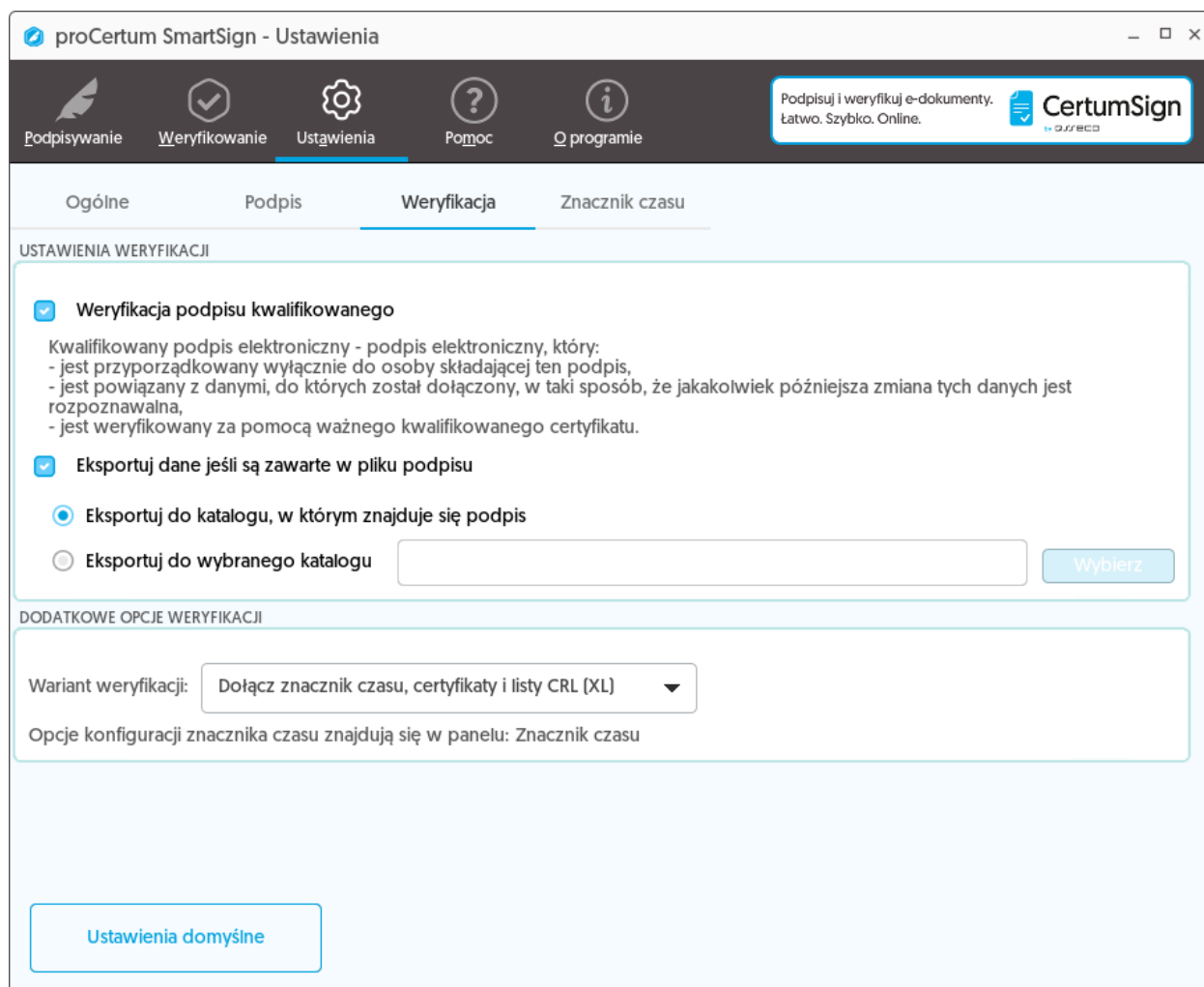
- Zaawansowane opcje podpisu XAdES
 - o **Twórz podpis rozszerzony** – wybranie tej opcji spowoduje, że w przypadku, gdy podpisywany plik będzie plikiem XML o poprawnej strukturze to podpis zostanie

wykonany w tzw. **standardowym** trybie Enveloped – **tryb ten wymagany jest przez Komisję Europejską**;

- **Ogranicz podpis do wersji podstawowej** – wybranie tej opcji spowoduje, że do podpisu nie będzie można dodać już kolejnego podpisu
- **Twórz podpis na potrzeby eKRS** – wybranie tej opcji spowoduje, że podpisy będą zgodne z wymaganiami eKRS

5.2.3. Ustawienia – Weryfikacja

Zakładka **Weryfikacja** umożliwia konfigurację ustawień dla operacji weryfikacji realizowanej w zakładce **Weryfikowanie**.



Rysunek 25: Zakładka Ustawienia - Weryfikacja

5.2.3.1. Podstawowe opcje weryfikacji

Zaznaczenie pola **Weryfikacja podpisu kwalifikowanego** spowoduje ustawienie odpowiedniego trybu pracy aplikacji **proCertum SmartSign**, który polega na sprawdzeniu czy operacja podpisu została wykonana certyfikatem kwalifikowanym w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania (...) z dnia 23 lipca 2014 r. (UE) NR 910/2014r.

Uwaga!

Jeżeli jest zaznaczone pole **Weryfikacja podpisu kwalifikowanego** to aplikacja sprawdzi czy certyfikat podpisujący jest certyfikatem kwalifikowanym. Jeżeli certyfikat nie jest certyfikatem kwalifikowanym to

podpis nie zostanie poprawnie zweryfikowany i zostanie zgłoszony błąd weryfikacji podpisu.

Jeżeli dane zawarte są w pliku podpisu to zaznaczenie opcji **Eksportuj dane jeśli są zawarte w pliku podpisu** spowoduje ich wyodrębnienie i zapisanie w wybranej lokalizacji.

5.2.3.2. Dodatkowe opcje weryfikacji

Dodatkową opcją weryfikacji jest tzw. **wariant weryfikacji** określający szczegółowość procesu weryfikacji. Do wyboru dostępne są następujące **warianty weryfikacji**:

- **Nie dołączaj dodatkowych informacji (BES)** – wybranie tej opcji spowoduje, że weryfikacji podlegała będzie tylko integralność podpisu;
- **Dołącz znacznik czasu (T)** – wybranie tej opcji spowoduje, że weryfikacji podlegała będzie integralność podpisu, po pozytywnej weryfikacji do podpisu zostanie dołączony znacznik czasu świadczący o czasie pozytywnej weryfikacji podpisu – wymagane jest wtedy zdefiniowanie ustawień znacznika czasu na zakładce **Znacznik Czasu**;
- **Dołącz znacznik czasu, certyfikaty i listy CRL (XL)** – wybranie tej opcji spowoduje, że przeprowadzona zostanie pełna weryfikacja podpisu, po pozytywnej weryfikacji do podpisu zostaną dołączone: znacznik czasu świadczący o czasie pozytywnej weryfikacji podpisu oraz listy CRL, które użyte zostały podczas weryfikacji – wymagane jest wtedy zdefiniowanie ustawień znacznika czasu na zakładce **Znacznik Czasu**;

5.2.4. Ustawienia – Znacznik czasu

Zakładka **Znacznik czasu** umożliwia konfigurację ustawień dla operacji znakowania czasem realizowanej podczas składania lub weryfikowania podpisu elektronicznego.

proCertum SmartSign - Ustawienia

Podpisywanie Weryfikowanie Ustawienia Pomoc O programie

Podpisuj i weryfikuj e-dokumenty. Łatwo. Szybko. Online. CertumSign

Ogólne Podpis Weryfikacja Znacznik czasu

USTAWIENIA ZNAKOWANIA CZASEM

Adres serwera znacznika czasu [adres publicznego serwera kwalifikowanego znacznika czasu SHA-256 Certum] http://public-q...

☐ Dostęp do serwera znacznika czasu przez certyfikat (wymagany dla płatnego kwalifikowanego znacznika czasu)

CERTYFIKAT DOSTĘPU DO ZNACZNIKA CZASU

Informacje:
Podmiot:
Wystawca:
Numer seryjny:

Wybierz
Pokaż
Usuń

Ustawienia domyślne

Rysunek 26: Zakładka Ustawienia – Znacznik czasu

Możemy określić następujące parametry:

- **Adres serwera znacznika czasu** umożliwia włączenie znakowania pliku podpisu znacznikiem czasu – dostępne są następujące predefiniowane ustawienia:
 - adres publicznego serwera kwalifikowanego znacznika czasu SHA-256 Certum – publiczny kwalifikowany znacznik czasu, który nie wymaga posiadania certyfikatu dostępu, usługa bezpłatna dla posiadaczy certyfikatów kwalifikowanych wydanych przez Certum PCC

Dodatkowo ręcznie można dodać następujące pozycje:

- <http://qts.certum.pl/default/clide> - adres serwera kwalifikowanego znacznika czasu CERTUM – kwalifikowany znacznik czasu, który wymaga posiadania certyfikatu dostępu;
- <http://localhost:801/pk-tsa> - adres, który należy wybrać w przypadku korzystania z aplikacji proCertum CLIDE Client zainstalowanej na komputerze użytkownika;
- <http://time.certum.pl> - adres serwera niekwalifikowanego znacznika czasu CERTUM;

UWAGA!!!

Dostęp do kwalifikowanego znacznika czasu CERTUM dostępnego pod adresem <http://qts.certum.pl/default/clide> możliwy jest wyłącznie przy użyciu certyfikatu dostępowego. W takim przypadku należy zaznaczyć opcję **Dostęp do serwera znacznika czasu przez certyfikat. Po zaznaczeniu zostaną odblokowane opcje ustawienia certyfikatu:**

- **Wybierz certyfikat** – po naciśnięciu przycisku, na listę zostaną wczytane wszystkie dostępne certyfikaty. Należy wybrać certyfikat uprawniający do dostępu do kwalifikowanego znacznika czasu CERTUM i nacisnąć przycisk **OK**;
- **Pokaż certyfikat** – po naciśnięciu przycisku zostaną wyświetlone szczegóły certyfikatu;
- **Usuń certyfikat** – naciśnięciu przycisku certyfikat zostanie usunięty z konfiguracji.

5.3. Podpisywanie plików

UWAGA!!!

Zgodnie z artykułem 137 Ustawy o usługach zaufania oraz identyfikacji elektronicznej od dnia 1 lipca 2018 r. algorytm funkcji skrótu SHA-1 stosowany przy składaniu kwalifikowanych podpisów elektronicznego, zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych powinien być zastąpiony algorytmem funkcji skrótu SHA-2. W związku z tym aplikacja proCertum SmartSign umożliwia składanie podpisów tylko przy użyciu algorytmu SHA-2.

Niezależnie od posiadanej wersji oprogramowania jedyną rekomendowaną funkcją skrótu jest funkcja skrótu SHA2.

Zakładka **Podpisywanie** umożliwia złożenie podpisu elektronicznego na pliku. Składają się na nią cztery sekcje:

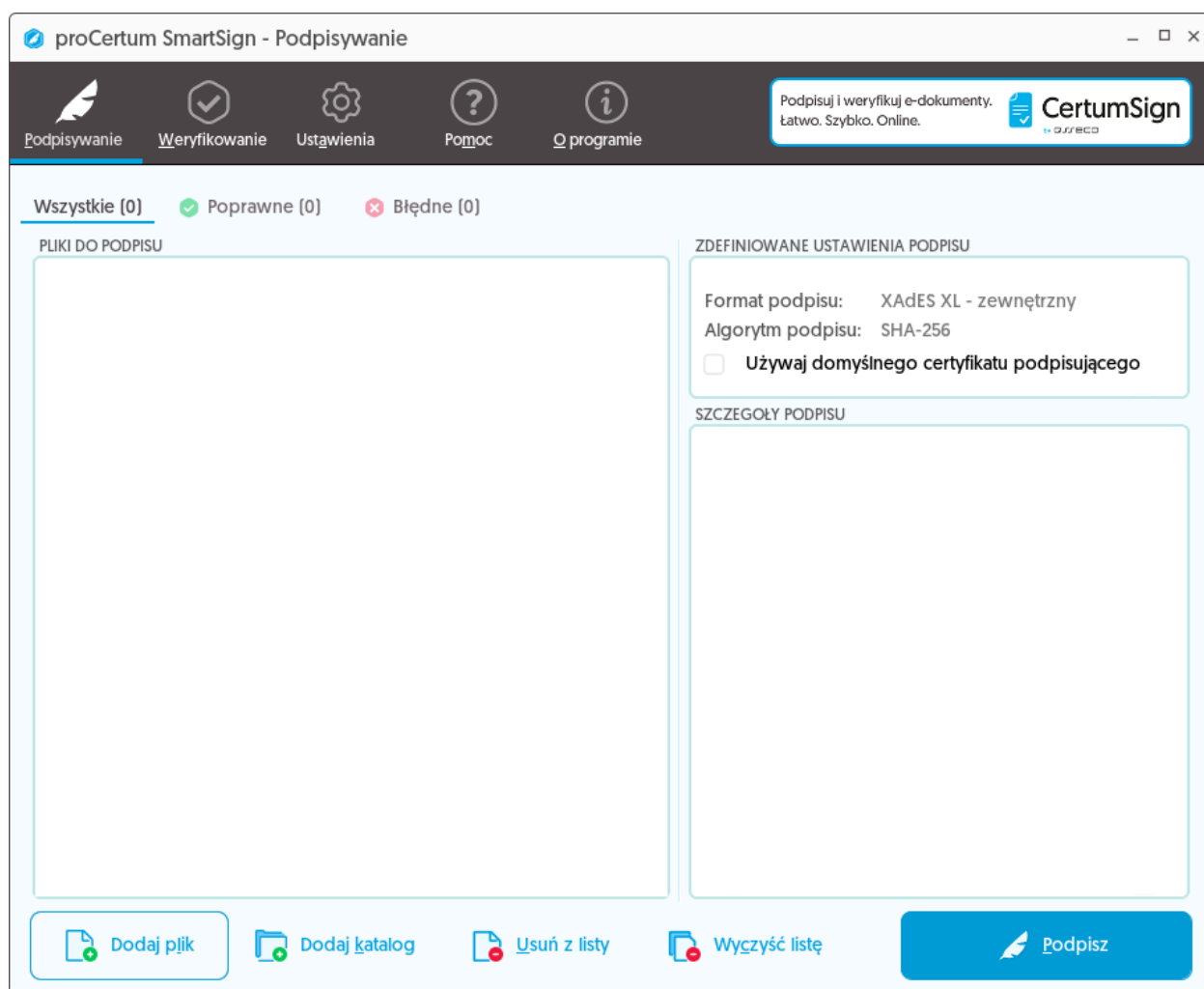
- **lista elementów do podpisania** **lista elementów do podpisania** – na liście wyświetlone są nazwy plików, data ich modyfikacji, rozmiar oraz status podpisu (Do podpisania | Podpisany | Plik został pominięty | Niepodpisany);
- **Zdefiniowane ustawienia podpisu** – zawiera informacje na temat formatu podpisu (ETSI/XAdES typie podpisu: wewnętrzny/zewnętrzny i algorytm podpisu) oraz opcję umożliwiającą użycie

certyfikatu domyślnego poprzez zaznaczenie opcji **Używaj domyślnego certyfikatu podpisującego**.

- **Szczegóły podpisu** – informacje dotyczące podpisu. Pojawiają się one po wykonaniu podpisu.
- **Informacje** – Informacje statystyczne na temat ilości wybranych plików z podziałem na łączną liczbę plików, pliki które nie zostały jeszcze podpisane, pliki już podpisane oraz pliki, które nie zostały jeszcze podpisane.

UWAGA!!!

Zalecane jest aby przy jednorazowym podpisywaniu plików nie przekraczać ilości 10 000 plików o rozmiarze ok. 50 KB



Rysunek 27: Zakładka Podpisywanie

5.3.1. Dodawanie elementów do listy

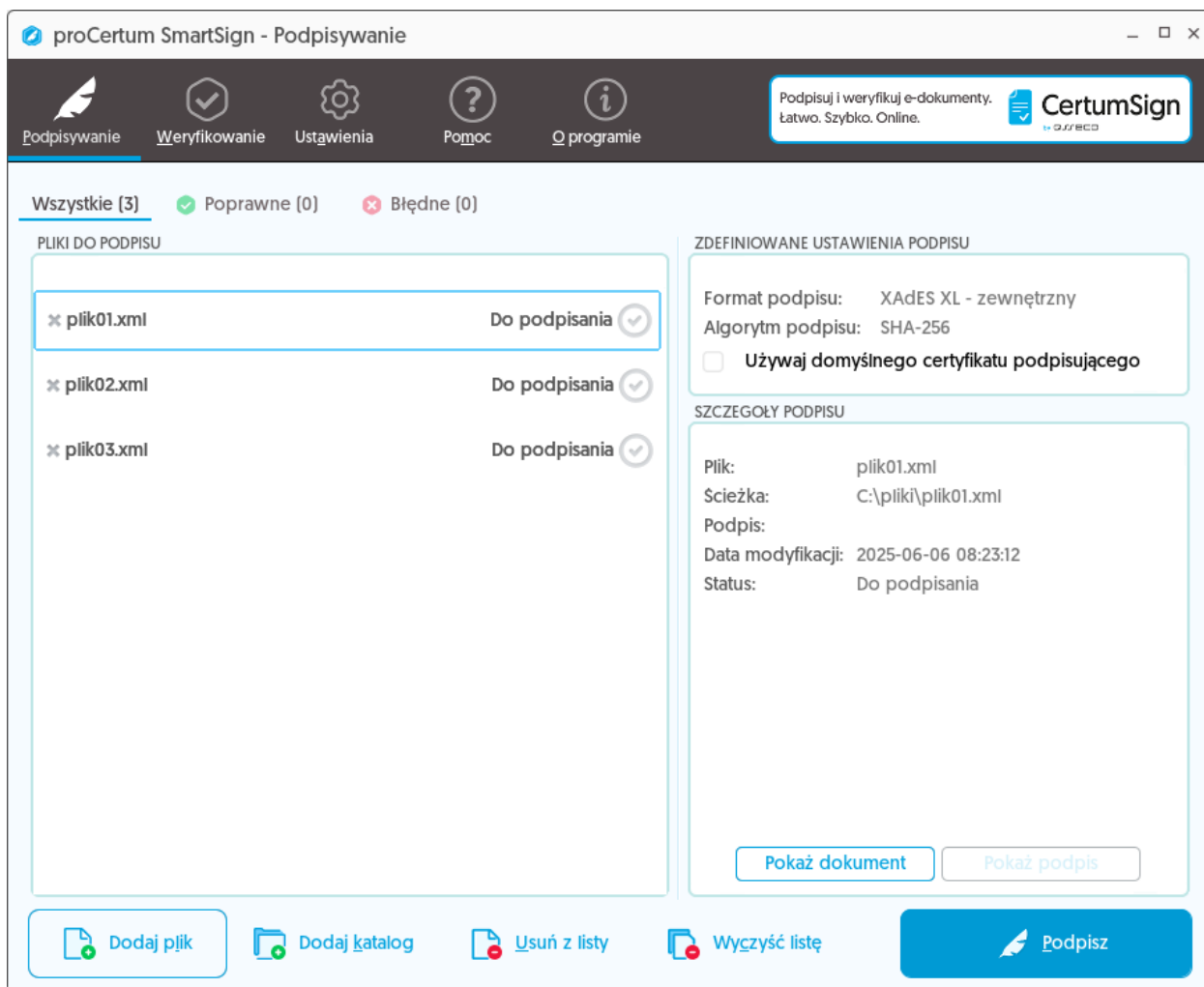
Operację podpisu elektronicznego można wykonać na dwa sposoby:

- na pojedynczym pliku – poprzez wskazanie pliku za pomocą przycisku **Dodaj plik**,
- na grupie plików – poprzez wielokrotny wybór plików za pomocą przycisku **Dodaj plik** lub poprzez dodanie katalogu za pomocą przycisku **Dodaj katalog**.

Wskazane pliki zostaną dodane do listy elementów do podpisania. Aby usunąć selektywnie plik(i) z listy do podpisania należy wskazać wybrany(e) i nacisnąć przycisk **Usuń z listy**. Aby usunąć wszystkie pliki z listy elementów do podpisania należy nacisnąć przycisk **Wyczyść listę**.

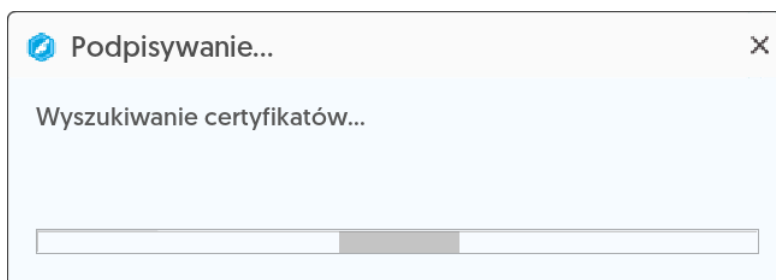
5.3.2. Operacja podpisu

Jeżeli na liście znajdują się już wszystkie elementy do podpisania to należy nacisnąć przycisk **Podpisz**.



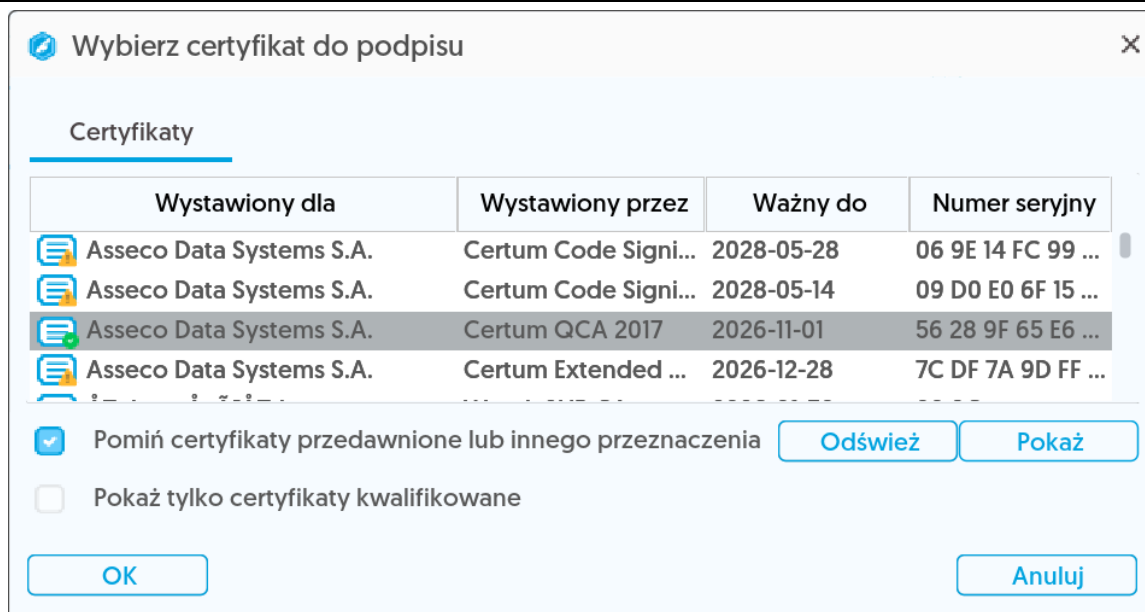
Rysunek 28: Zakładka Podpisywanie – Lista elementów do podpisania

Aplikacja **proCertum SmartSign** wyszuka certyfikaty umożliwiające opatrzenie dokumentu podpisem elektronicznym.



Rysunek 29: Wyszukiwanie certyfikatów

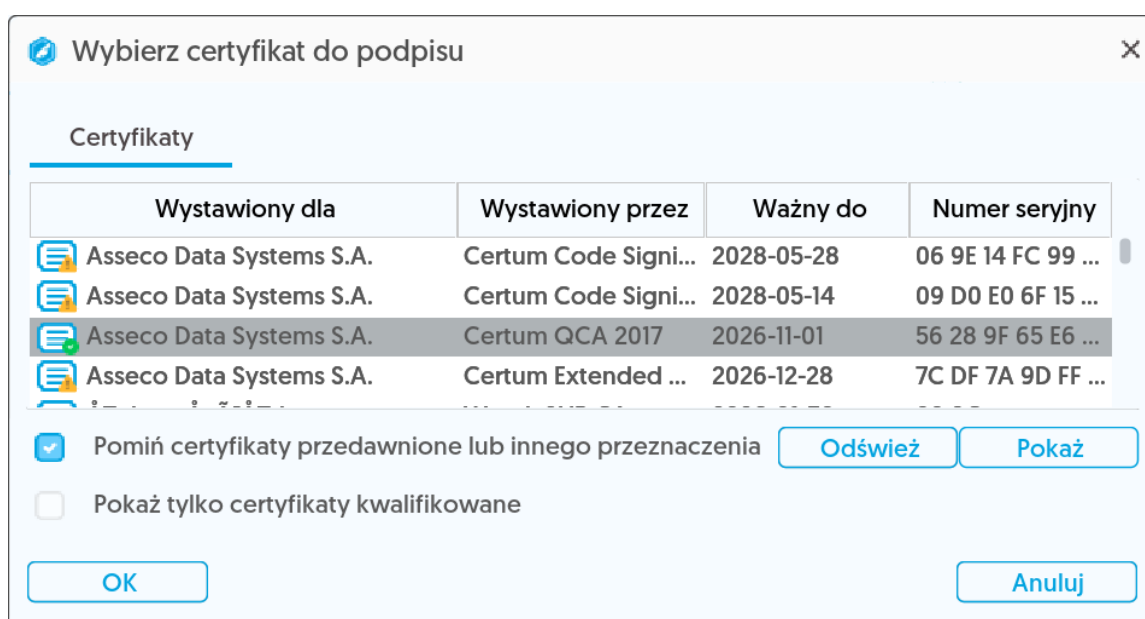
Po zakończeniu wyszukiwania zostaną wyświetlone certyfikaty. W przypadku gdy została zaznaczona opcja **Używaj domyślnego certyfikatu podpisującego** krok wyboru certyfikatów zostanie pominięty.



Rysunek 30: Lista certyfikatów kwalifikowanych

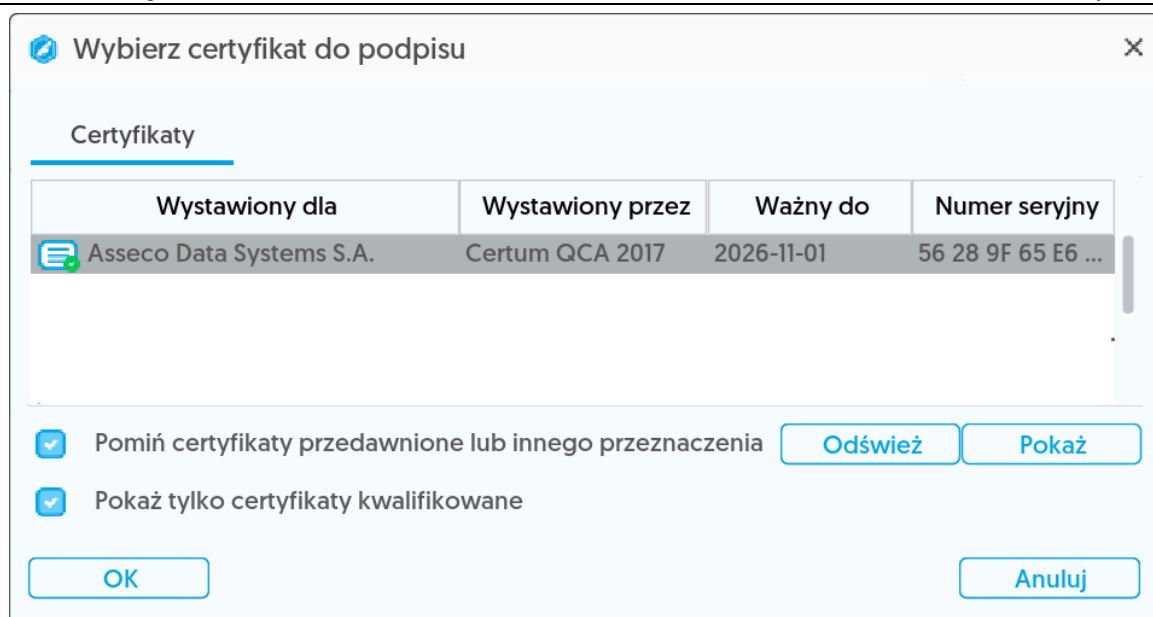
Uwaga!

W oknie dialogowym zostaną wyświetlone certyfikaty kwalifikowane. Aby wyświetlić wszystkie certyfikaty dostępne na danym komputerze należy odznaczyć opcję **Pokaż tylko certyfikaty kwalifikowane**.



Rysunek 31: Lista certyfikatów kwalifikowanych i niekwalifikowanych

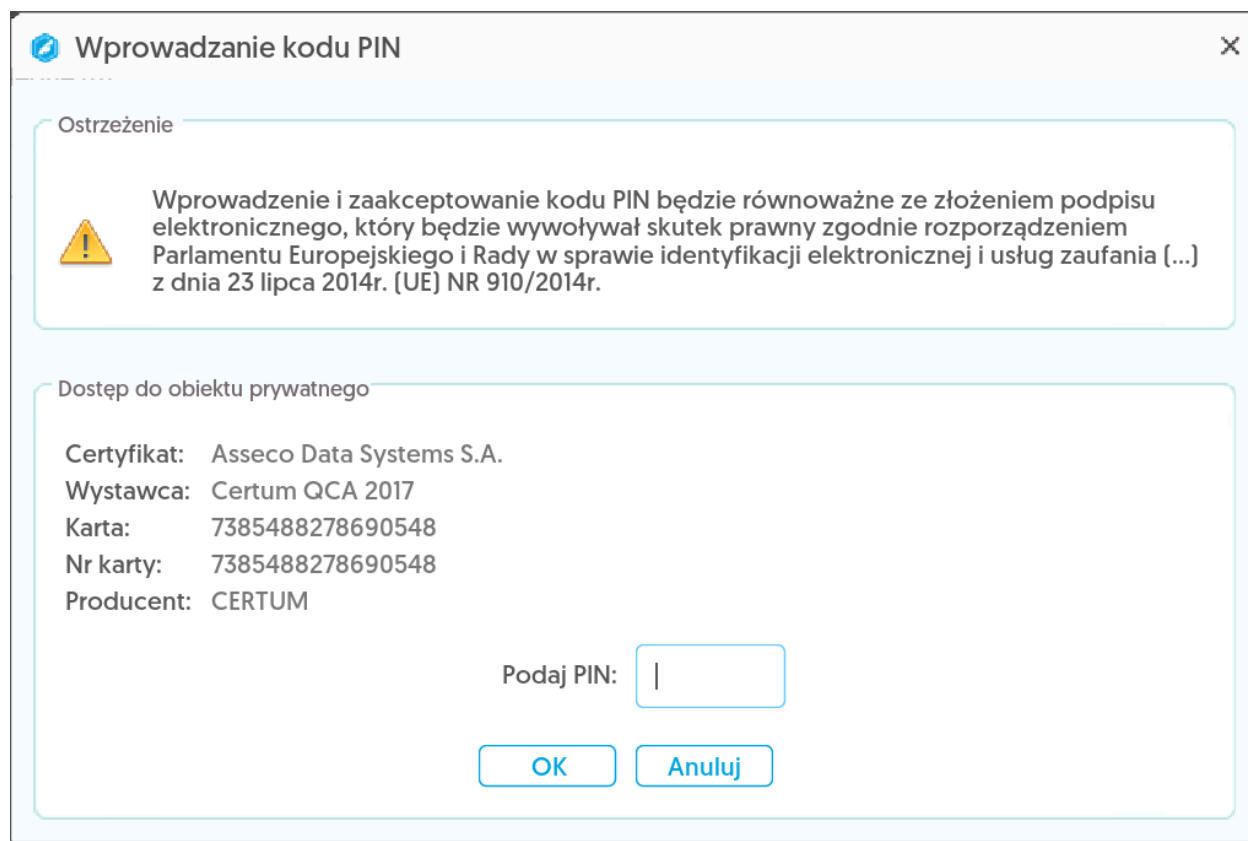
Należy wskazać certyfikat dla wykonania operacji podpisu i nacisnąć przycisk **OK**.



Rysunek 32: Wybór certyfikatu dla operacji podpisu

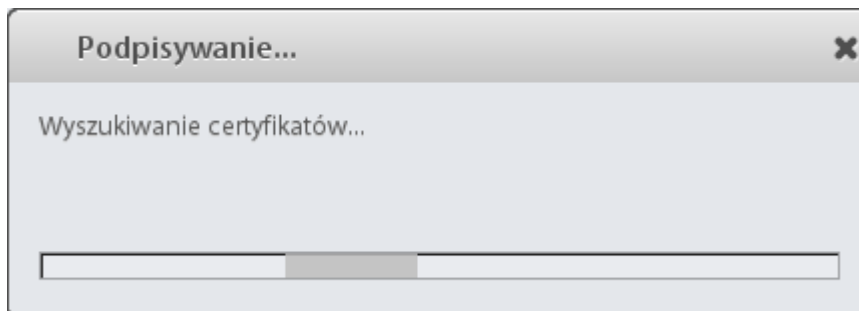
Jeżeli użytkownik dla operacji podpisu cyfrowego wybrał certyfikat kwalifikowany to wyświetlona zostanie prośba o wprowadzenie kodu uwierzytelniającego PIN. Należy wprowadzić PIN i nacisnąć przycisk **OK**.

Podpis elektroniczny złożony za pomocą tego oprogramowania i przy użyciu ważnego certyfikatu kwalifikowanego będzie wywoływał skutki prawne równoważne podpisowi własnoręcznemu zgodnie z Rozporządzeniem eIDAS (Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. (Dz.Urz.UE.L Nr 257, str. 73).

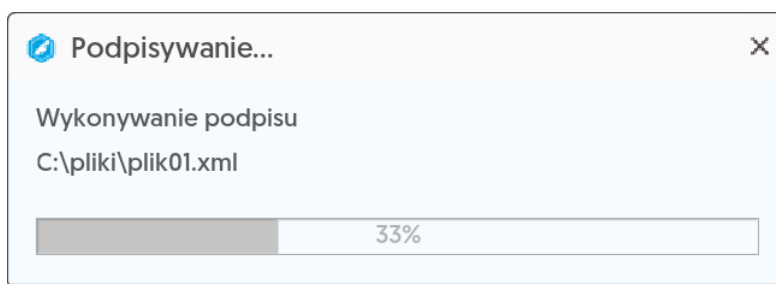


Rysunek 33: Prośba o wprowadzenie kodu PIN

Jeżeli wprowadzony PIN jest prawidłowy to aplikacja **proCertum SmartSign** rozpocznie proces składania podpisu.

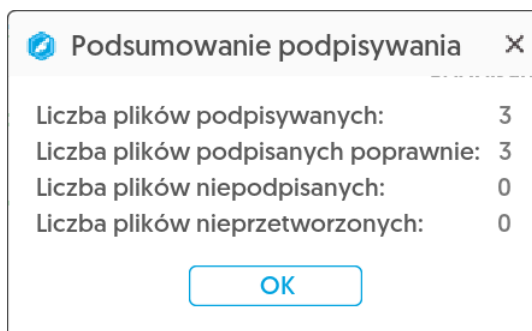


Rysunek 34: Podpisywanie... - Wyszukiwanie kluczy



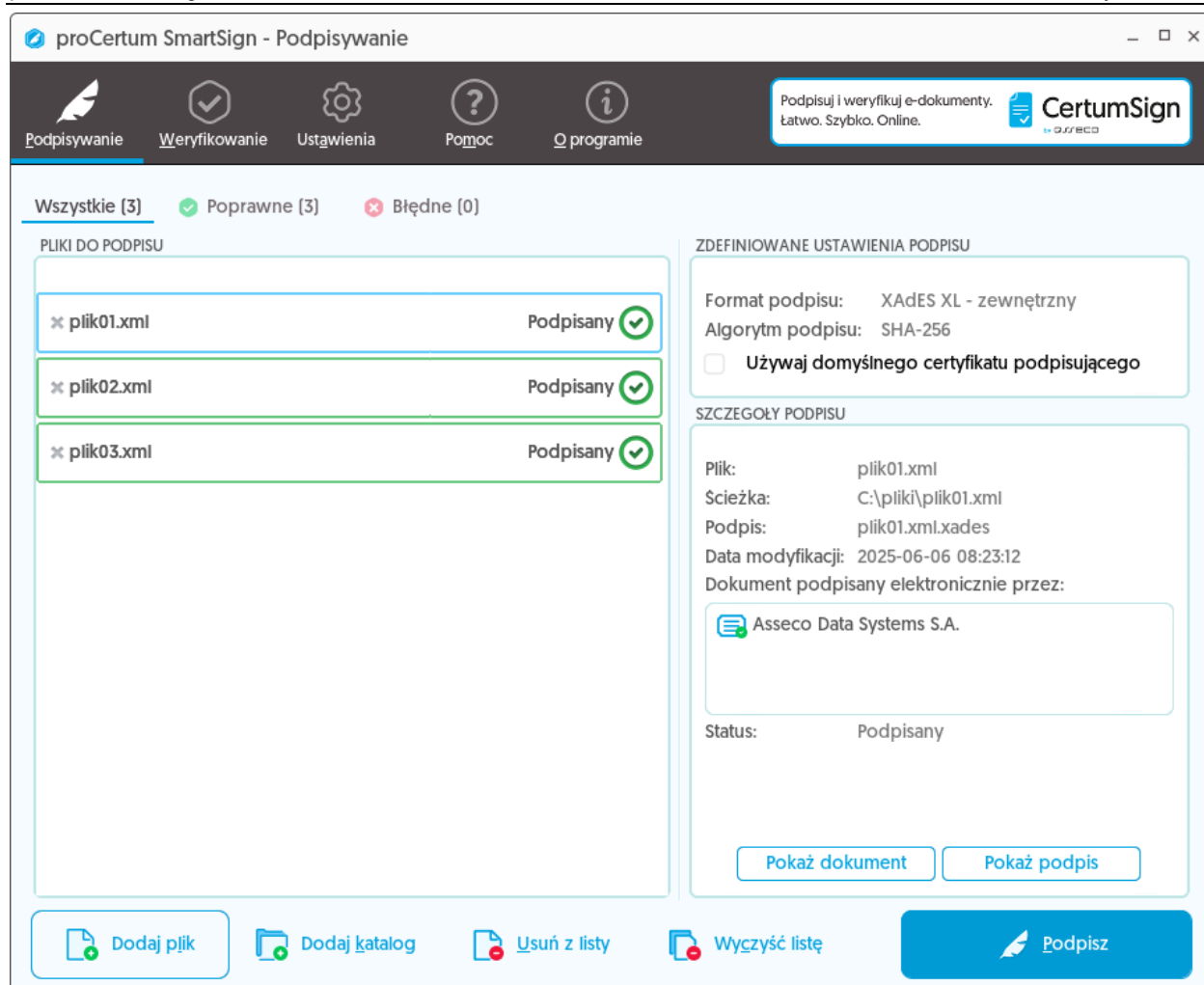
Rysunek 35: Podpisywanie... - Wykonywanie podpisu

Po zakończeniu procesu składania podpisu elektronicznego zostanie wyświetlone podsumowanie.



Rysunek 36: Podsumowanie podpisywania

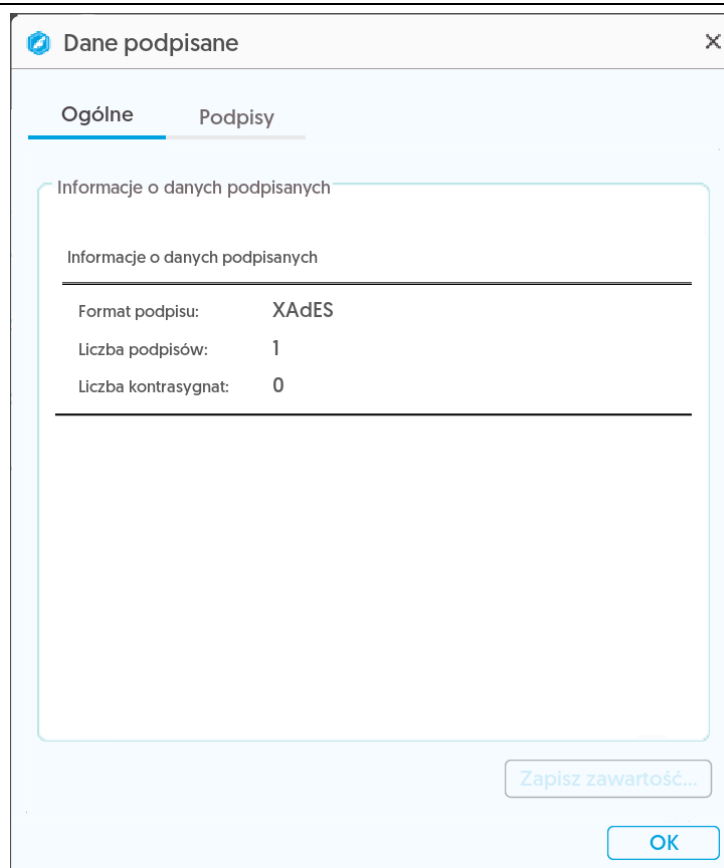
Sekcja **Szczegóły podpisu** na zakładce **Podpisywanie** zostanie uaktualniona o informacje dotyczące pliku podpisu oraz podpisującego (pole **Dokument podpisany przez**).



Rysunek 37: Zakładka Podpisywanie – wykonany podpis

Można przejrzeć właściwości podpisu poprzez naciśnięcie przycisku **Pokaż podpis**: Pojawia się wówczas okienko prezentujące strukturę podpisu. Znajdują się w nim zakładki:

- **Ogólne** - Ogólne informacje o danych podpisanych, format podpisu, liczba podpisów równoległych oraz kontrasygnat. W przypadku podpisu zewnętrznego aktywny jest przycisk **Zapisz zawartość**, który pozwala na wyodrębnienie z podpisu i zapisanie na dysku danych.



Rysunek 38: Dane podpisane – zakładka ogólne

Rysunek 39: Dane podpisane - zakładka podpis

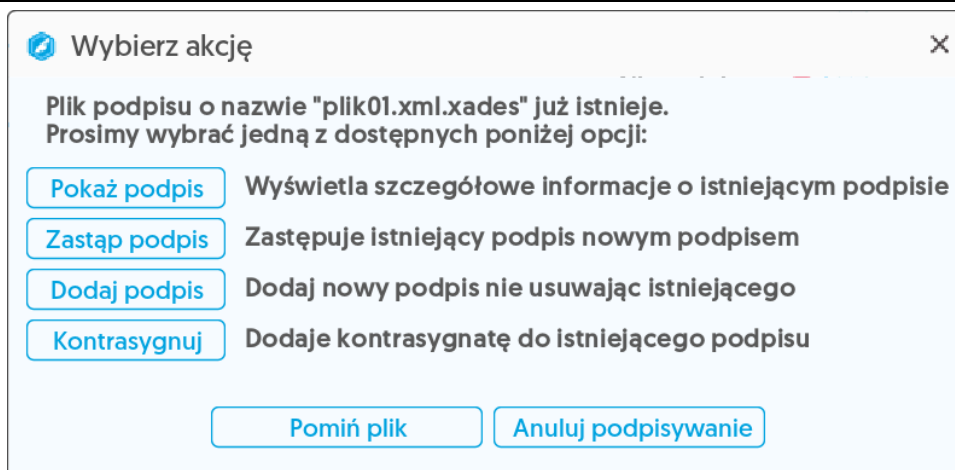
5.3.3. Podpis wielokrotny

W celu wykonania **podpisu wielokrotnego**, należy wybrać plik, który został już wcześniej podpisany. Wskazać można oryginalny plik, jak również plik podpisu. Domyślnie okno wyboru pliku pozwala wybierać wszystkie pliki oprócz plików podpisu. Jeśli chcemy skorzystać z opcji wskazywania pliku podpisu, należy w oknie wyboru pliku zmienić filtr na **Pliku podpisu (*.xades, *.xad, *.sign, *.sig)**. Następnie po wybraniu odpowiednich plików, należy nacisnąć przycisk **Podpisz**.

UWAGA!!!

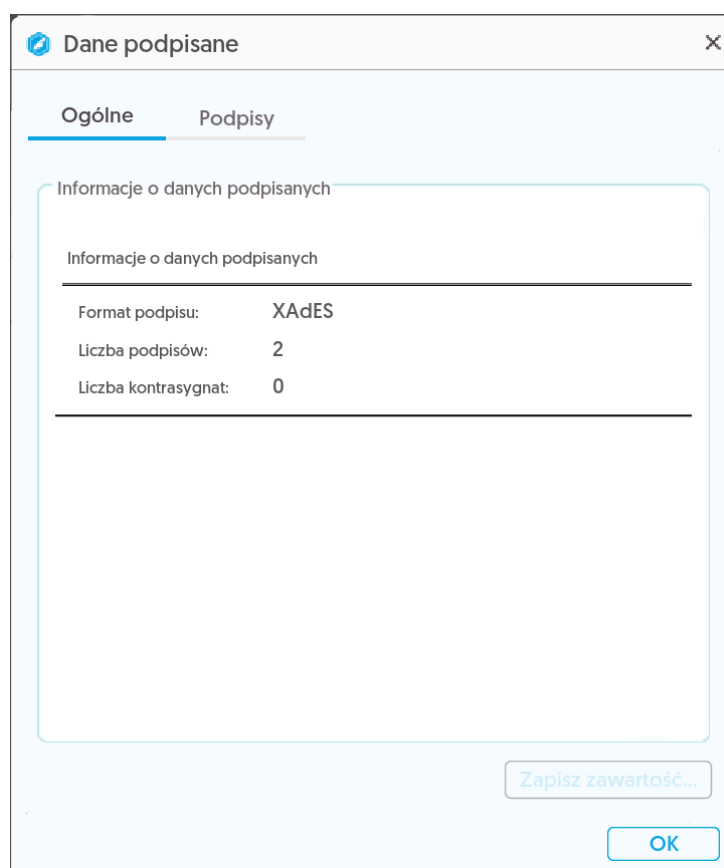
Przy tworzeniu podpisu wielokrotnych nie ma możliwości składania podpisów „mieszanych” tzn. aplikacja ignoruje wszelkie ustawienia dot. formatów podpisu i wykonuje podpis w takim trybie, w jakim złożony jest pierwszy podpis na dokumencie.

Proces wybierania certyfikatu i wprowadzania kodu PIN jest identyczny jak podczas składania podpisu jednokrotnego. Po poprawnym wprowadzeniu kodu PIN pojawi się następujące okno:

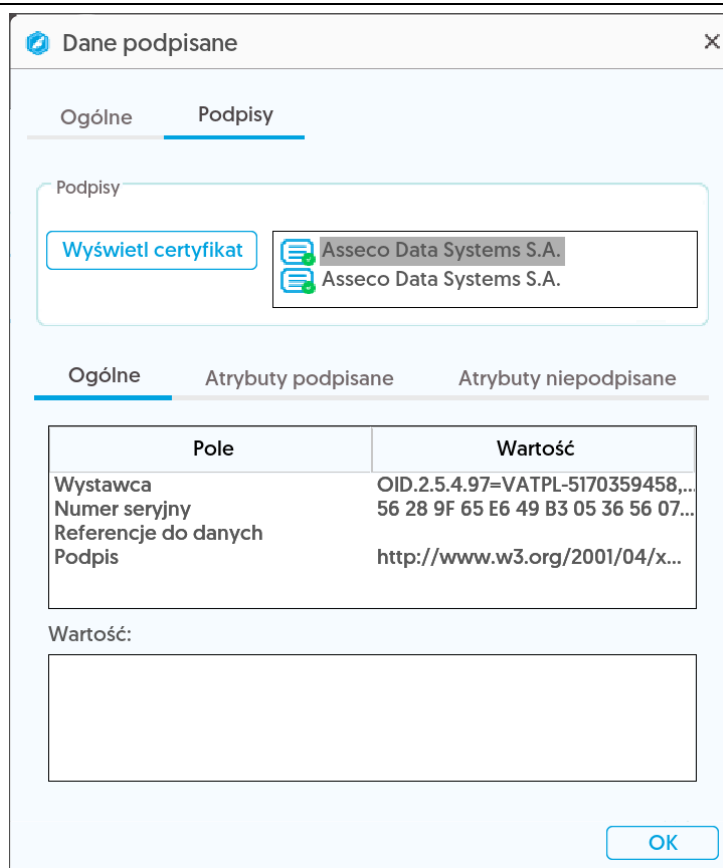


Rysunek 40: Okno wyboru akcji przy obecnym już co najmniej jednym podpisie

Dla **podpisu wielokrotnego** należy nacisnąć przycisk **Dodaj podpis**. W przypadku wybrania opcji **Zastąp podpis**, wszystkie dotychczasowe podpisy zostaną usunięte i zostanie stworzony nowy podpis. Można także wyświetlić dane o istniejącym podpisie poprzez naciśnięcie przycisku **Pokaż podpis**. Gdy podpis zostanie wykonany można sprawdzić wszystkie podpisy danego pliku poprzez naciśnięcie przycisku **Pokaż podpis**.



Rysunek 41: Dane podpisane - zakładka ogólna dla podpisu wielokrotnego



Rysunek 42: Dane podpisane - zakładka podpis dla podpisu wielokrotnego

5.3.4. Kontrasygndata

W celu wykonania **kontrasygnaty**, należy wybrać plik, który został już wcześniej podpisany. Wskazać można zarówno oryginalny plik, jak również plik podpisu. Domyślnie okno wyboru pliku pozwala wybierać wszystkie pliki, oprócz plików podpisu. Jeśli chcemy skorzystać z opcji wskazywania pliku podpisu, należy w oknie wyboru pliku zmienić filtr na Pliki podpisu (*.xades, *.xad, *.sign, *.sig). Następnie po wybraniu odpowiednich plików, należy nacisnąć przycisk **Podpisz**.

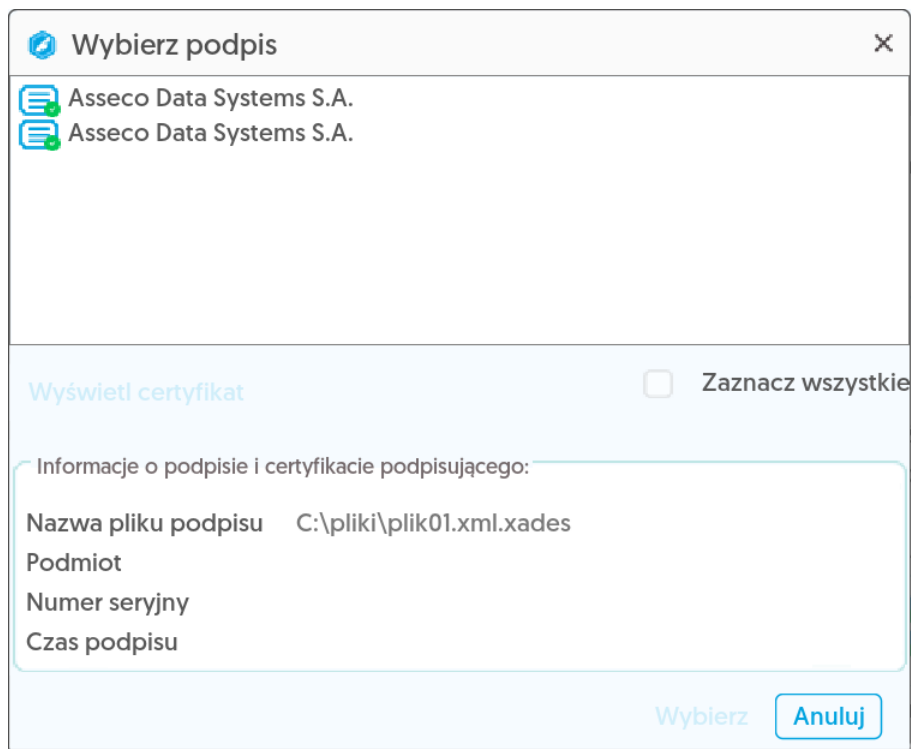
Proces wybierania certyfikatu i wprowadzania kodu PIN jest identyczny jak podczas składania podpisu jednokrotnego. Po poprawnym wprowadzeniu kodu PIN pojawi się następujące okno:



Rysunek 43: Okno wyboru akcji przy obecnym już co najmniej jednym podpisie

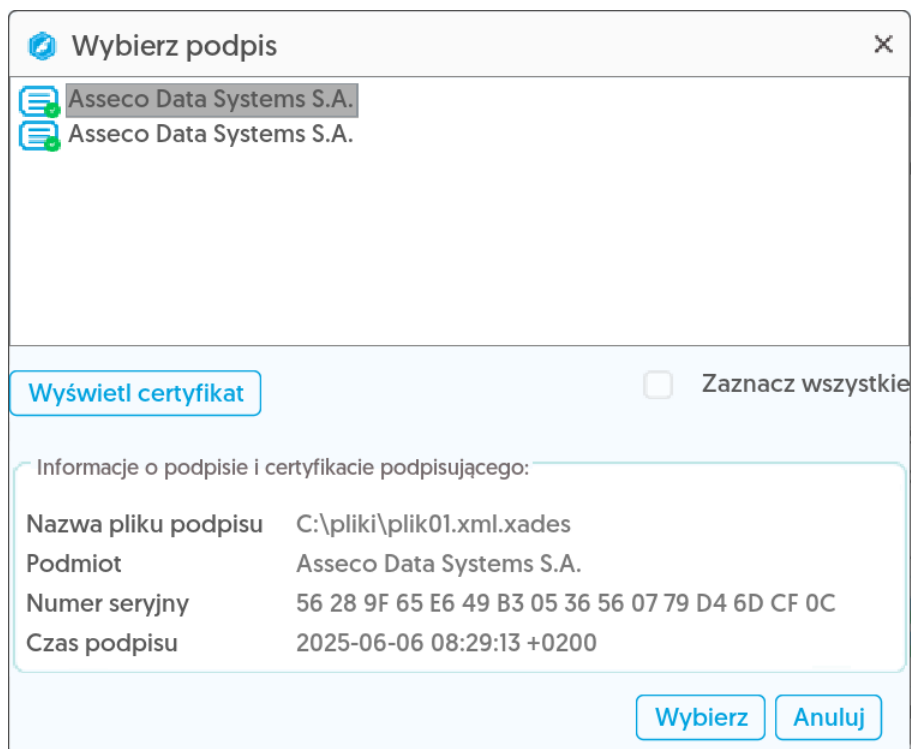
Dla **kontrasygnaty** należy nacisnąć przycisk **Kontrasygnuj**. W przypadku wybrania opcji **Zastąp podpis** wszystkie dotychczasowe podpisy zostaną usunięte i zostanie stworzony nowy podpis. Można także

wyświetlić dane o istniejącym podpisie poprzez naciśnięcie przycisku **Pokaż podpis**. Po naciśnięciu przycisku **Kontrasygnuj** pojawi się okno, z którego należy wybrać certyfikat, który chcemy kontrasygnować:



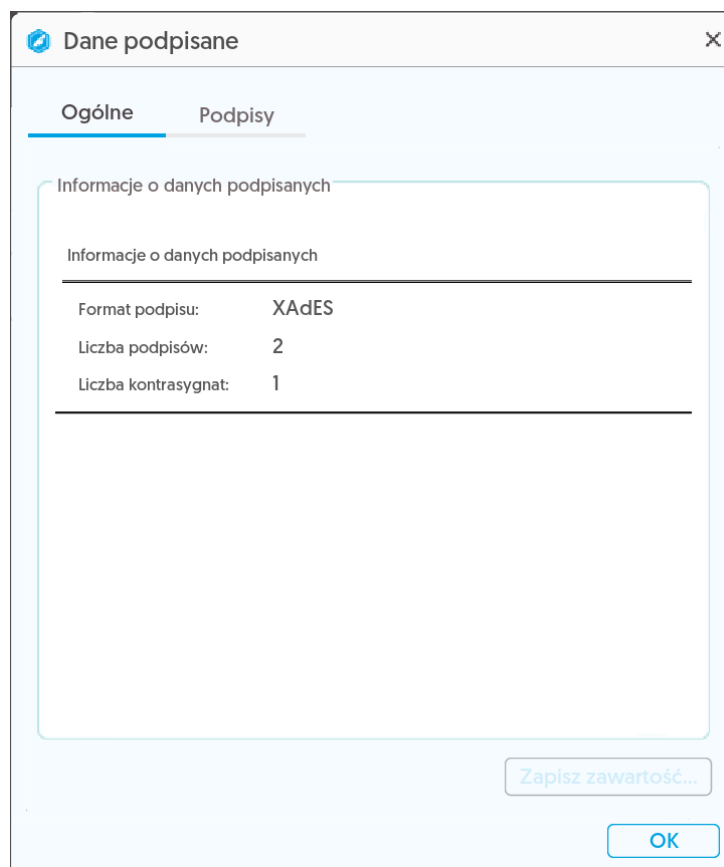
Rysunek 44: Okno wyboru podpisu, który chcemy kontrasygnować

Po wybraniu certyfikatu należy nacisnąć przycisk **Wybierz**. Jeśli chcemy kontrasygnować wszystkie podpisy, wtedy należy zaznaczyć opcję **Zaznacz wszystkie** i nacisnąć przycisk **Wybierz**:

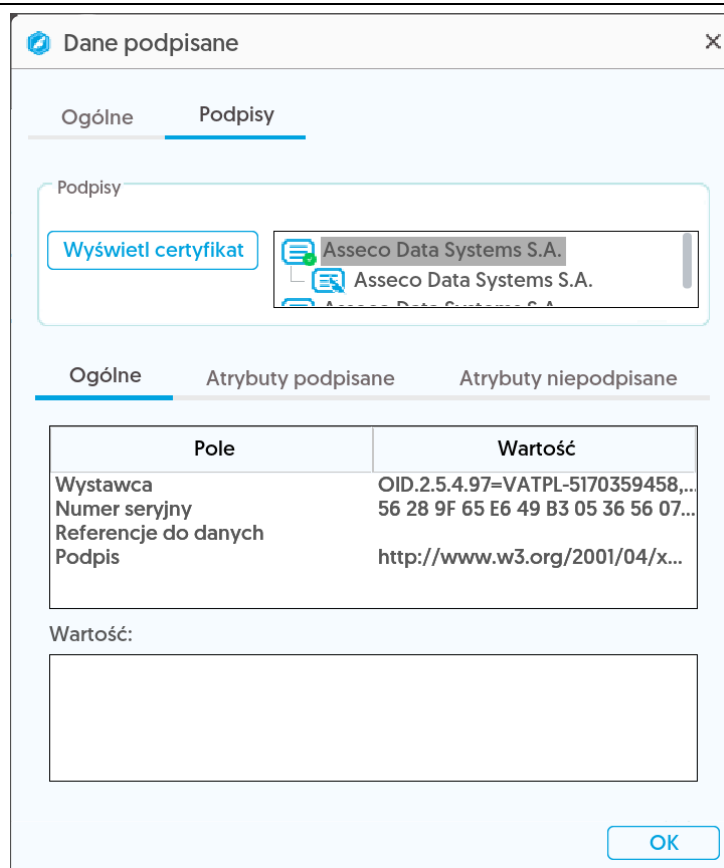


Rysunek 45: Okno wyboru podpisu, gdy wybrano wszystkie podpisy do kontrasygnowania

Gdy podpis zostanie wykonany można sprawdzić wszystkie podpisy danego pliku poprzez naciśnięcie przycisku **Pokaż podpis**.



Rysunek 46 Dane podpisane - zakładka ogólna dla kontrasygnaty



Rysunek 47 Dane podpisane - zakładka podpis dla kontrasygnaty

Literą **C** oznaczone są **kontrasygnaty** podpisów.

5.3.5. Podpisywanie plików PDF

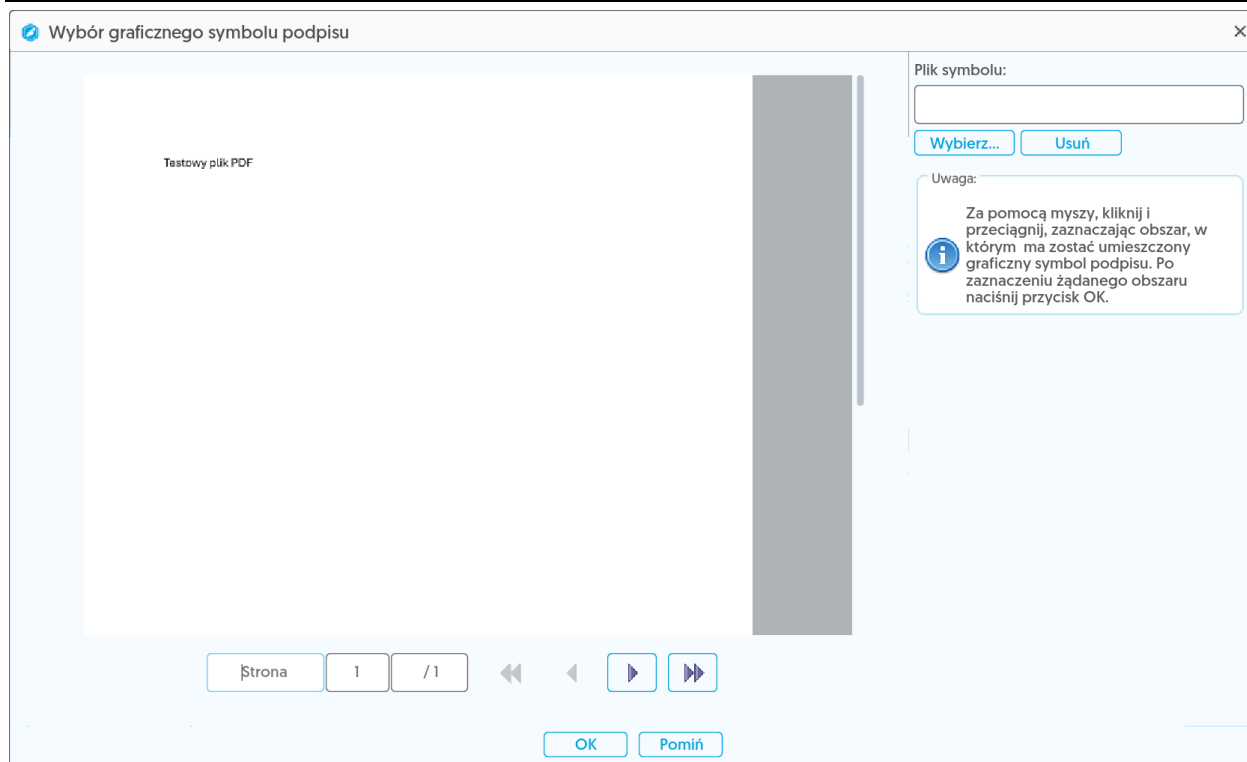
Jeśli w Ustawieniach włączona jest opcja **Twórz podpis specjalny PDF (PAdES)**, gdy podpisany jest dokument PDF to aplikacja przy natrafieniu na plik PDF wykonana podpis w pliku PDF w tzw. formacie PAdES. Sam proces podpisywania nie różni się w zasadzie od procesu przedstawionego powyżej. Podpis umieszczany jest bezpośrednio w pliku PDF.

UWAGA!!!

Do poprawnej interpretacji podpisów w plikach PDF wymagane jest oprogramowanie Adobe® Reader® w wersji co najmniej 10.0.

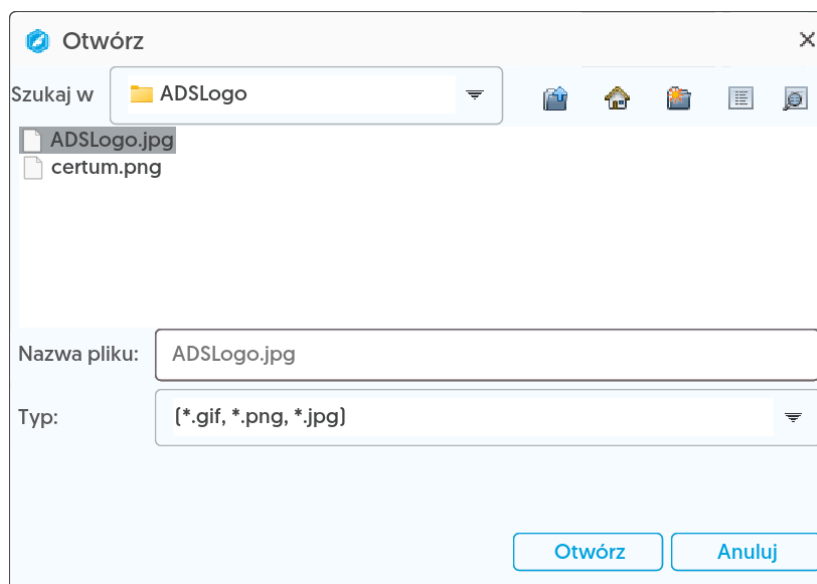
5.3.5.1. Dodawanie graficznego symbolu podpisu

Jeśli w zaawansowanych opcjach podpisu PDF/PAdES zaznaczona jest opcja **Umieszczaj graficzny symbol podpisu w dokumencie PDF** to w trakcie podpisywania plików PDF, po wybraniu certyfikatu podpisującego umożliwia wybranie pliku graficznego symbolu podpisu. W przypadku seryjnego podpisywania plików PDF, dla każdego podpisywanego pliku PDF aplikacja umożliwia definiowanie osobnego symbolu.



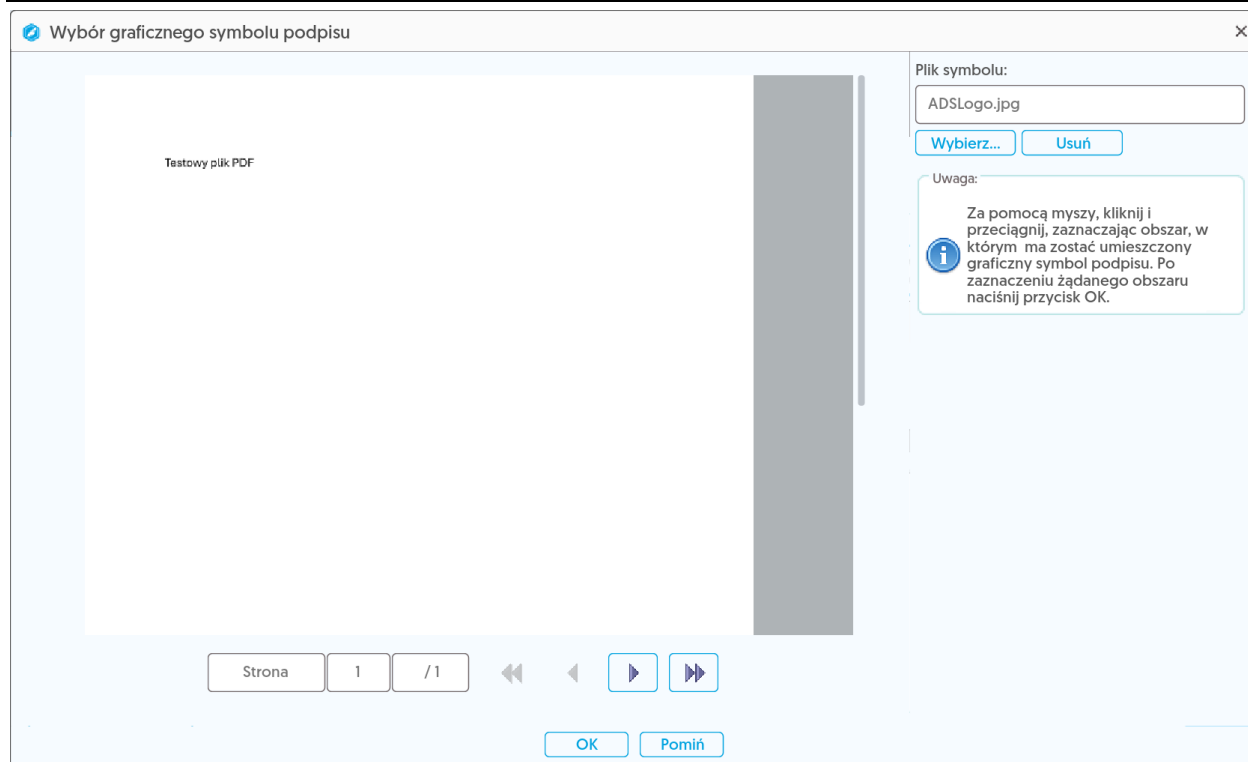
Rysunek 48 Dodawanie graficznego symbolu podpisu – okno główne

Po naciśnięciu przycisku **Wybierz** umożliwiające zostanie wskazanie graficznego pliku służącego jako graficzny symbol podpisu (dopuszczalne formaty to jpg, gif i png).



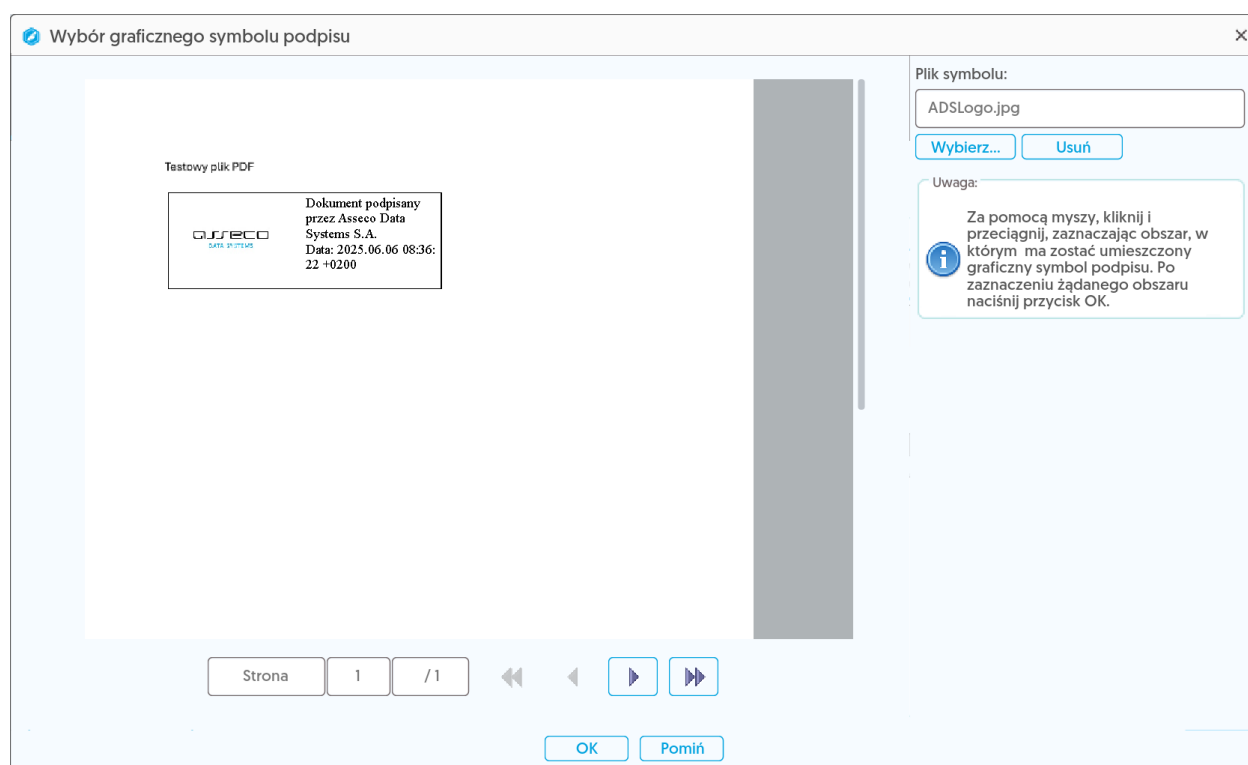
Rysunek 49 Dodawanie graficznego symbolu podpisu – wskazanie pliku graficznego

Po wybraniu pliku, okno główne zostanie zaktualizowane o wybrany plik.



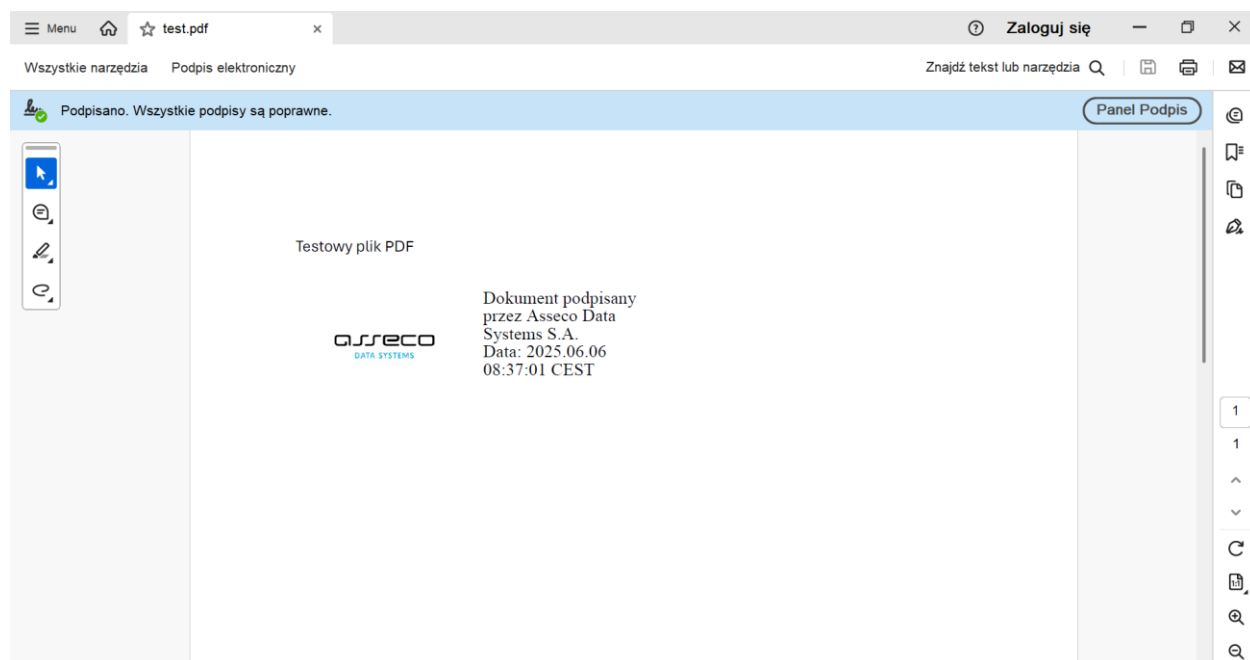
Rysunek 50 Dodawanie graficznego symbolu podpisu – wybrany plik graficzny

Pole, w którym graficzny symbol ma znaleźć się na dokumencie wskazuje się myszą przy wciśniętym lewym klawiszu myszy. Po zdefiniowaniu tego pola symbol wraz z informacją o podpisującym pojawi się na dokumencie.



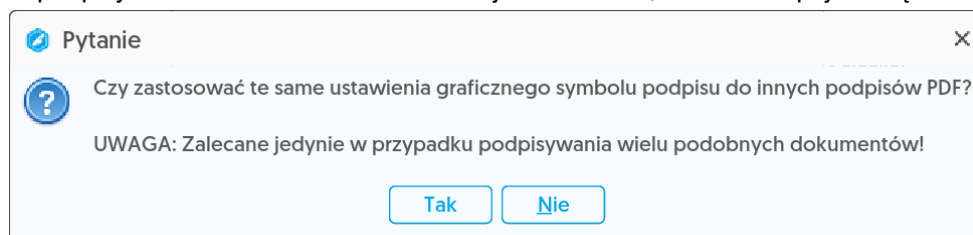
Rysunek 51 Dodawanie graficznego symbolu podpisu – symbol graficzny dodany do dokumentu

Po zatwierdzeniu przyciskiem **OK** podpis zostanie wykonany. Po otwarciu dokumentu PDF podpis wraz symbolem graficznym będzie od razu widoczny.



Rysunek 52 Dodawanie graficznego symbolu podpisu – podpisany plik z umieszczonym graficznym symbolem podpisu

W przypadku podpisywania wielu dokumentów PDF jednocześnie, na ekranie pojawi się komunikat.

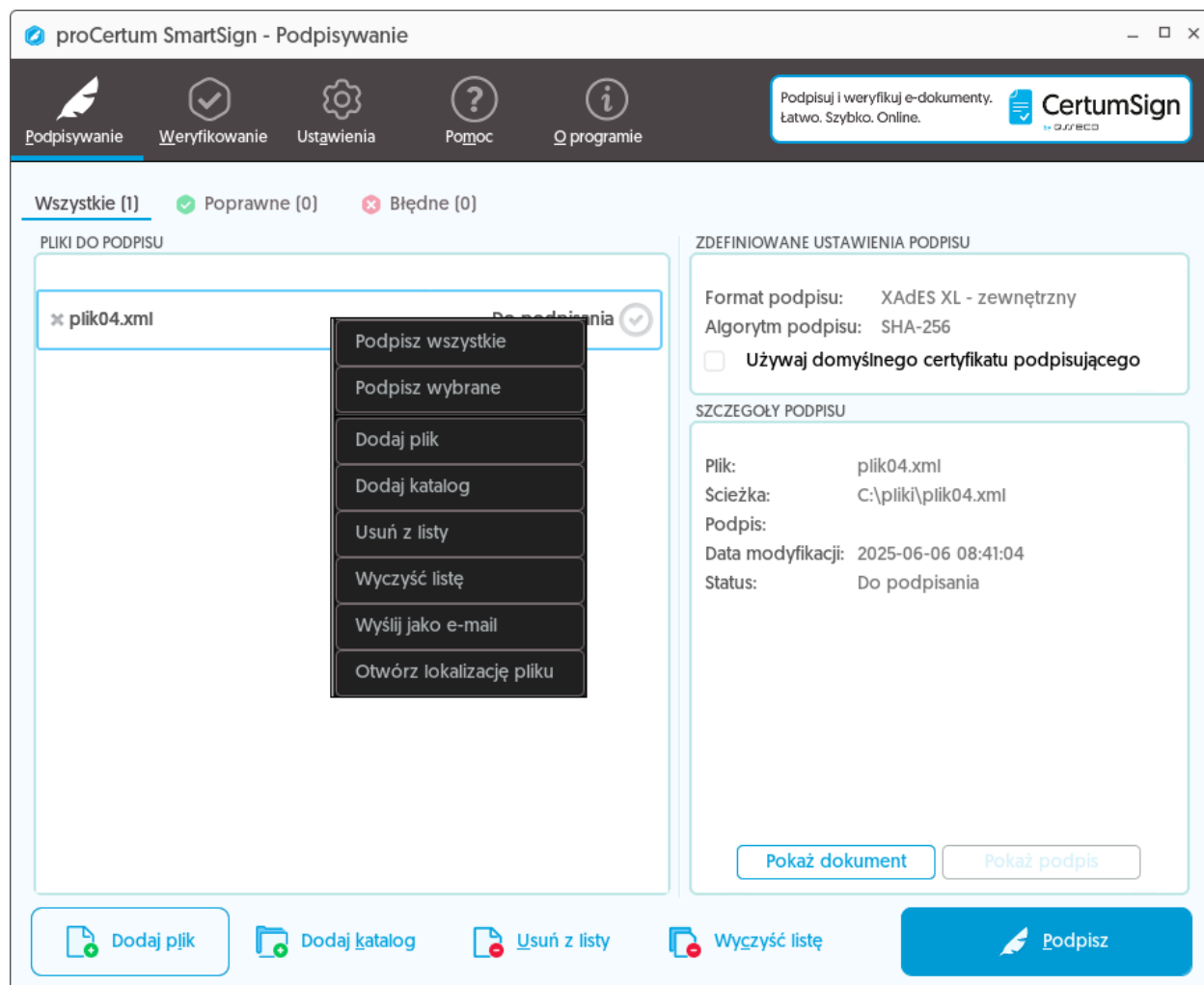


Rysunek 53 Dodawanie graficznego symbolu podpisu – podpisywanie wielu plików

5.3.6. Menu kontekstowe

Aby uruchomić **menu kontekstowe** należy nacisnąć prawym klawiszem myszki w dowolnym miejscu na liście. Dostępne jest 8 opcji w menu:

- **Podpisz wszystkie** – po wybraniu tej opcji zostanie wykonany podpis na wszystkich plikach znajdujących się na liście.
- **Podpisz wybrane** – po wybraniu tej opcji podpis zostanie wykonany tylko na plikach zaznaczonych. Aby zaznaczyć więcej niż jeden plik należy przytrzymać lewy klawisz **Ctrl** i poprzez naciśnięcie lewego klawisza myszki wskazać następne plik(i).
- **Dodaj plik** – opcja ta działa na takiej samej zasadzie jak przycisk **Dodaj plik**.
- **Dodaj katalog** – opcja ta działa na takiej samej zasadzie jak przycisk **Dodaj katalog**.
- **Usuń z listy** – opcja ta działa na takiej samej zasadzie jak przycisk **Usuń z listy**.
- **Wyczyść listę** – opcja ta działa na takiej samej zasadzie jak przycisk **Wyczyść listę**.
- **Wyślij jako e-mail** – opcja ta uruchamia program pocztowy ustawiony w systemie operacyjnym jako domyślny i generuje maila załączając do niego utworzone pliki podpisów oraz pliki podpisywane (w przypadku podpisu zewnętrznego).
- **Otwórz lokalizację pliku** – opcja pozwala na wyświetlenie katalogu z plikiem

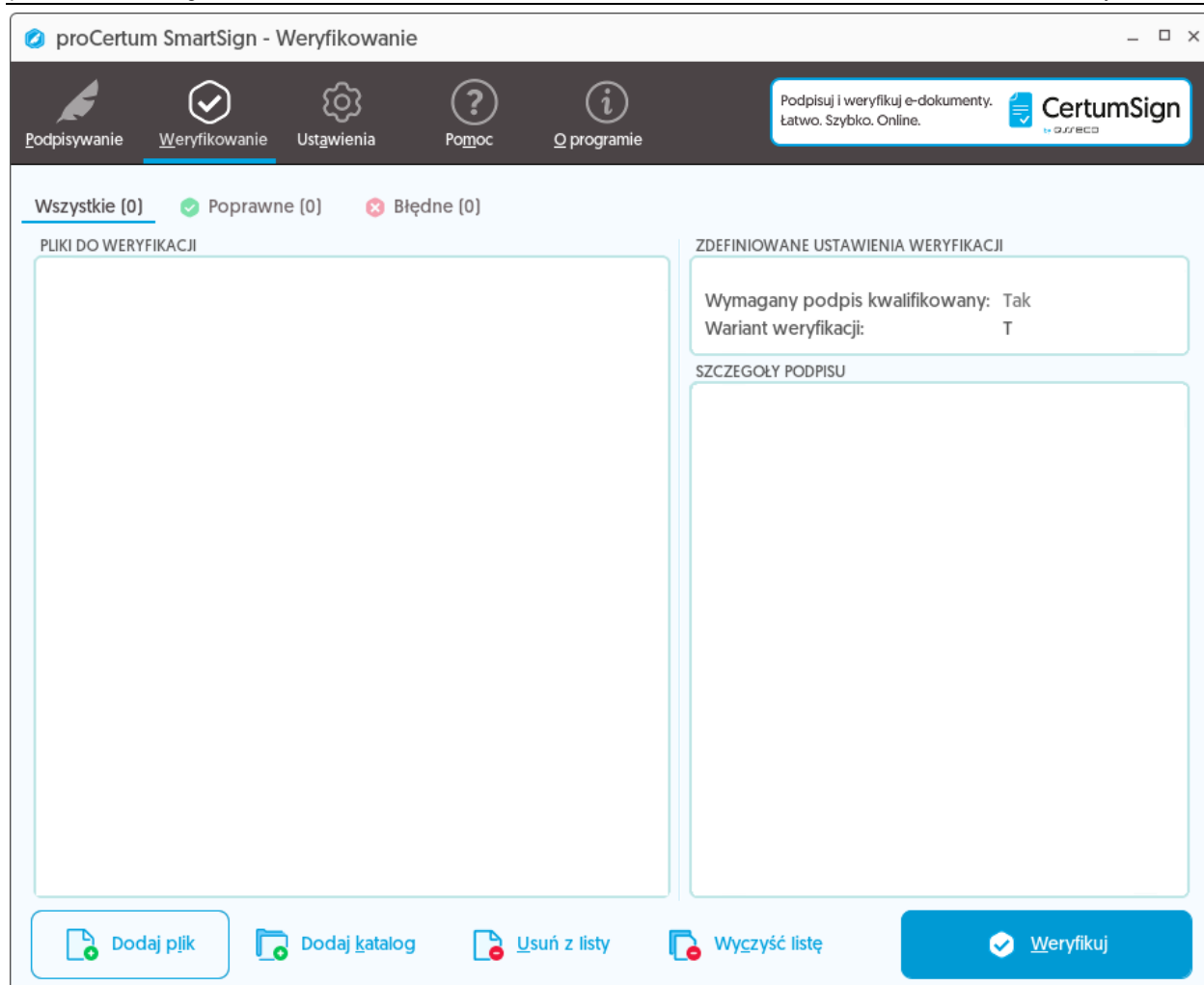


Rysunek 54: Zakładka Podpisywanie – menu kontekstowe

5.4. Weryfikowanie podpisów

Zakładka **Weryfikowanie** umożliwia weryfikację podpisu elektronicznego. Składają się na nią cztery sekcje:

- **lista elementów do weryfikacji** – na liście wyświetlone są nazwy plików, data ich modyfikacji, rozmiar oraz status podpisu (Do weryfikacji/Pozytywnie zweryfikowany/Negatywnie zweryfikowany).
- **Zdefiniowane ustawienia weryfikacji** – informacje na temat ustawień weryfikacji dotyczących weryfikacji podpisu kwalifikowanego. (Patrz: punkt 4.1.3).
- **Informacje o podpisie** – informacje dotyczące podpisu na wybranym pliku.
- **Informacje** – Informacje statystyczne na temat ilości wybranych plików z podziałem wszystkie wybrane pliki, na pliki przeznaczone do weryfikacji, pliki już zweryfikowane poprawnie oraz pliki, które nie zostały zweryfikowane poprawnie.



Rysunek 55: Zakładka Weryfikowanie

5.4.1. Dodawanie elementów do listy

Jeżeli chcemy wykonać operację weryfikacji podpisu elektronicznego to możemy ją wykonać:

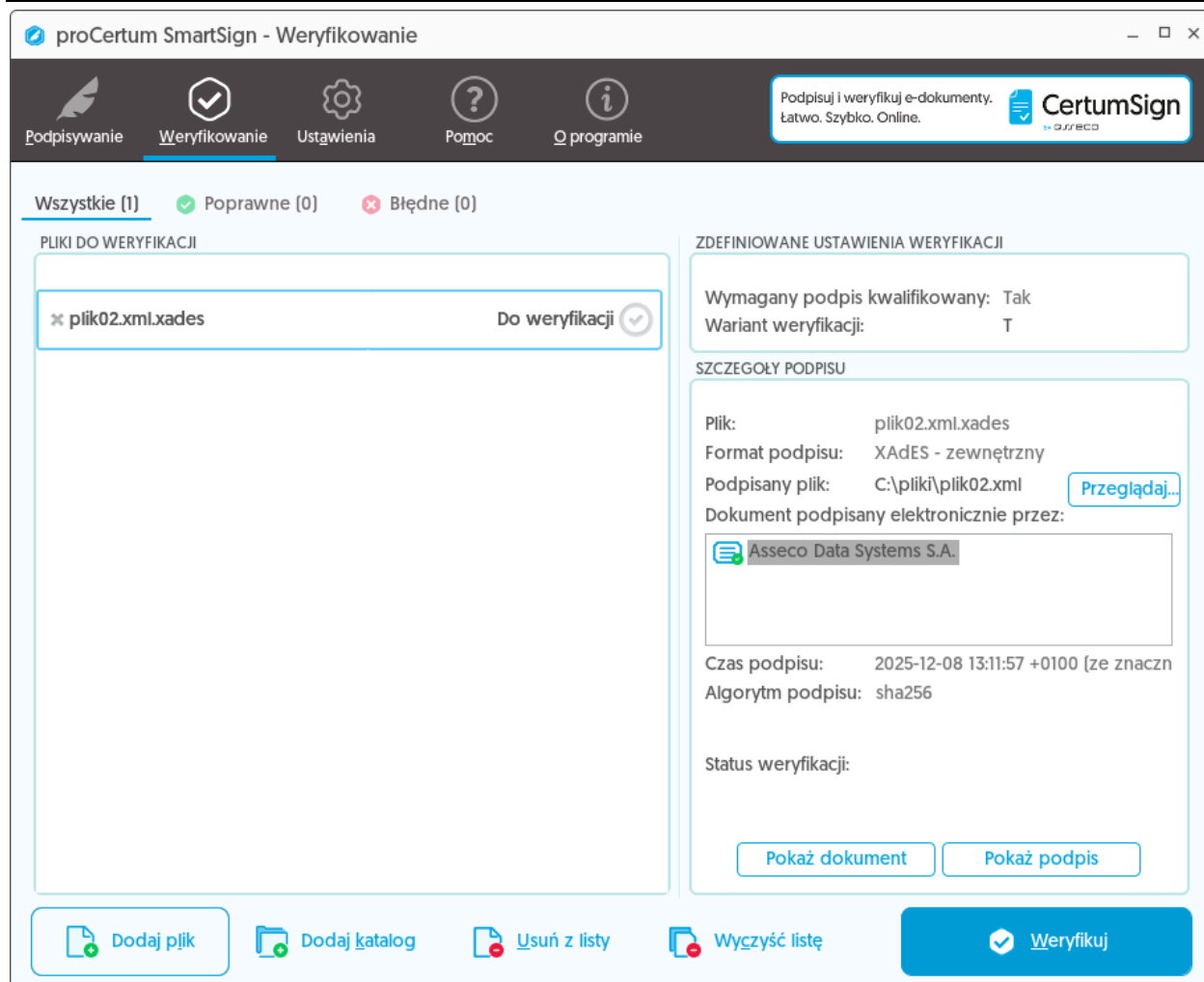
- na pojedynczym pliku – poprzez wskazanie pliku za pomocą przycisku **Dodaj plik**,
- na grupie plików – poprzez wielokrotny wybór plików za pomocą przycisku **Dodaj plik** lub poprzez dodanie katalogu za pomocą przycisku **Dodaj katalog**.

Wskazane pliki zostaną dodane do listy elementów do weryfikacji. Aby usunąć selektywnie plik(i) z listy do weryfikacji należy wskazać wybrany(e) i nacisnąć przycisk **Usuń z listy**. Aby usunąć wszystkie pliki z listy elementów do weryfikacji należy nacisnąć przycisk **Wyczyść listę**.

Uwaga!

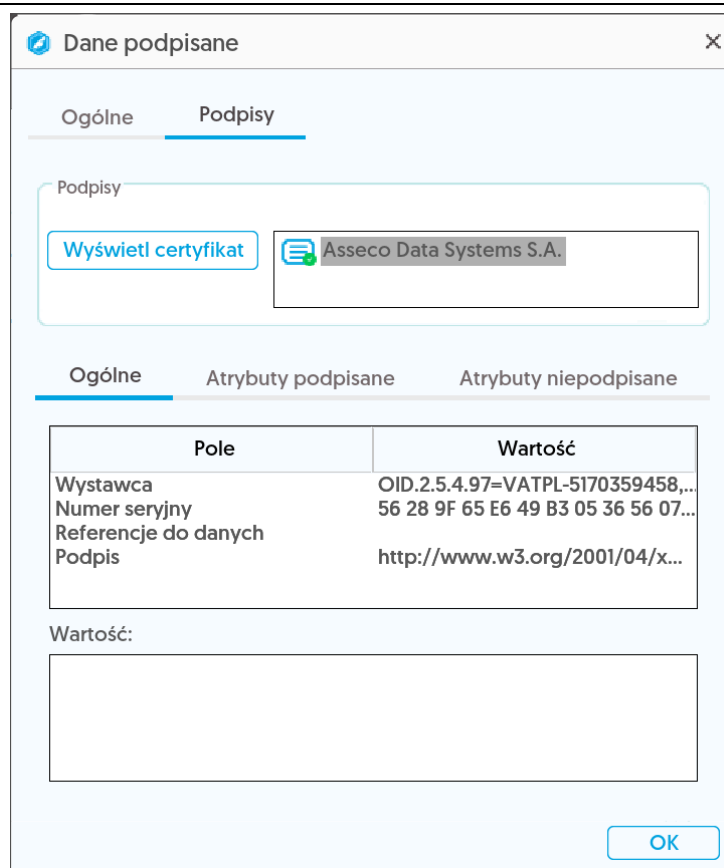
Na liście elementów do weryfikacji mogą figurować pliki z wewnętrznym bądź zewnętrznym podpisem (informacja o typie podpisu znajduje się w sekcji **Szczegóły podpisu**). Jeżeli wybrany element jest podpisem zewnętrznym i program nie odnalazł pliku podpisanego w katalogu pliku podpisu, to w sekcji **Szczegóły podpisu** należy wskazać plik źródłowy, na którym wykonana była operacja podpisu, poprzez naciśnięcie przycisku **Przeglądaj...**.

5.4.2. Informacje o podpisie i weryfikowanym dokumencie



Rysunek 56: Zakładka Weryfikowanie – Lista elementów do weryfikacji

Szczegółowe informacje o podpisie można uzyskać poprzez naciśnięcie przycisku **Pokaż podpis**. Otworzy się okno **Dane podpisane**.



Rysunek 57: Dane podpisane

W oknie **Dane podpisane** znajdują się dwie zakładki:

- **Ogólne** – zawiera informacje o rodzaju podpisu oraz liczbie podpisów, kontrasygnat i certyfikatów;
- **Podpisy** – zawiera informacje o podpisie i certyfikacie podpisującego, atrybutach podpisanych i niepodpisanych itp.;

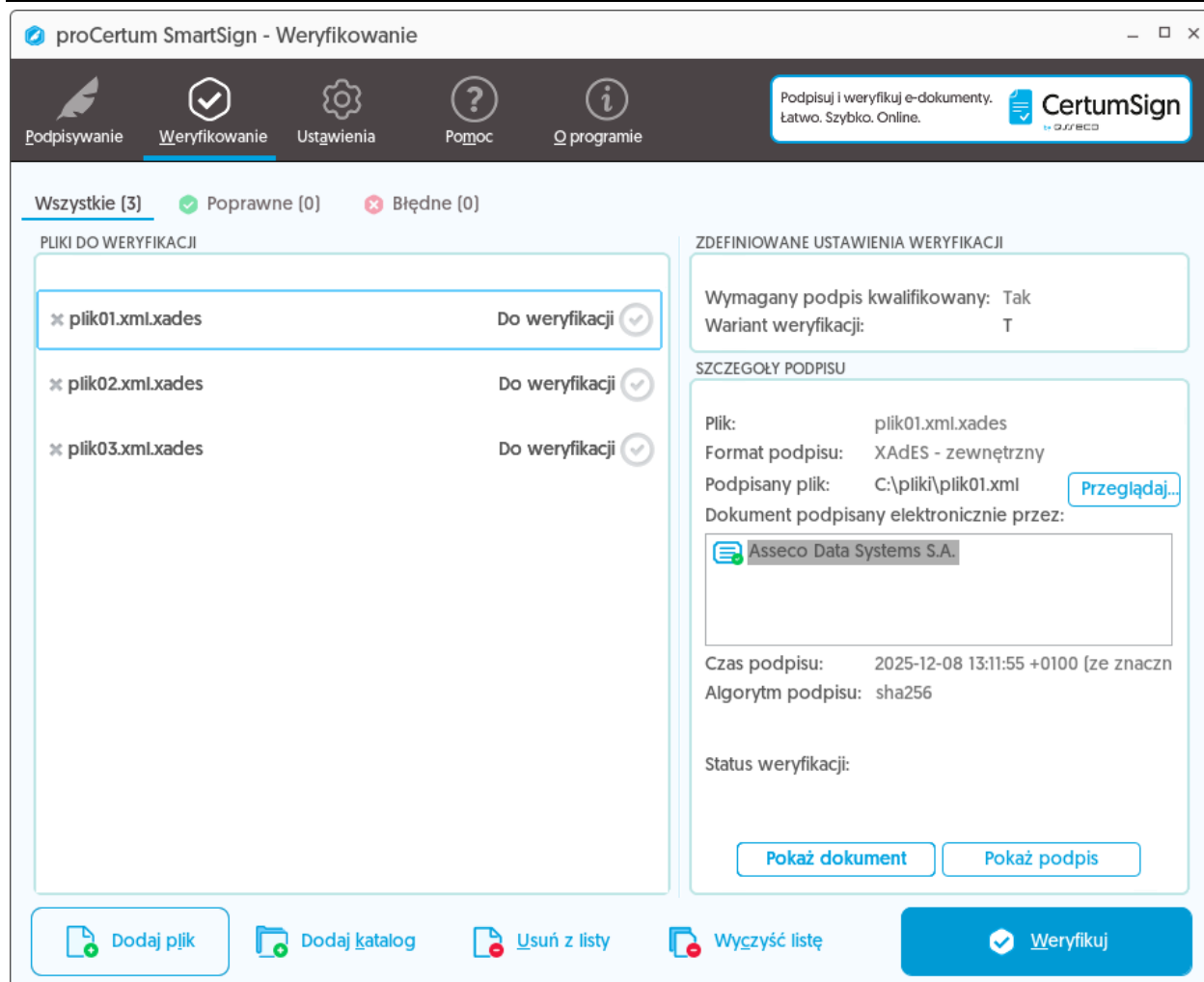
Aby wyświetlić weryfikowany dokument należy nacisnąć przycisk **Pokaż dokument**.

Uwaga!

Dokument jest wyświetlany poza kontrolą programu **proCertum SmartSign**, za pomocą zewnętrznej aplikacji odpowiedniej dla tego typu dokumentu.

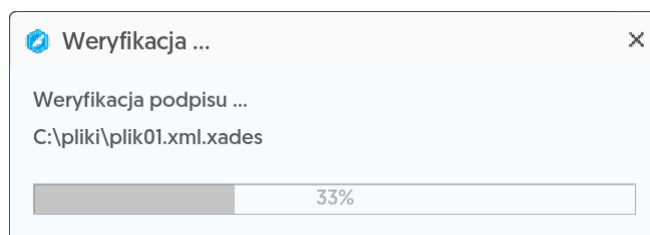
5.4.3. Operacja weryfikacji

Jeżeli na liście znajdują się już wszystkie elementy do weryfikacji to należy nacisnąć przycisk **Weryfikuj**.



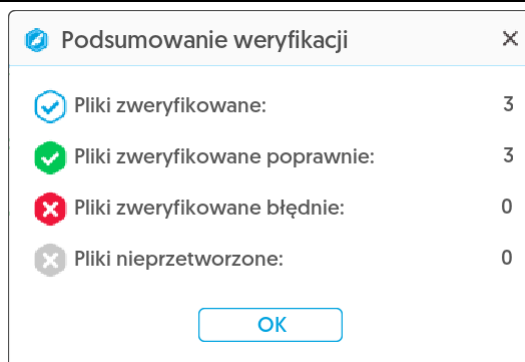
Rysunek 58: Zakładka Weryfikowanie – Lista elementów do weryfikacji

Rozpocznie się proces weryfikacji podpisu.



Rysunek 59: Weryfikacja...

Po zakończeniu procesu weryfikacji podpisu elektronicznego zostanie wyświetlone podsumowanie.



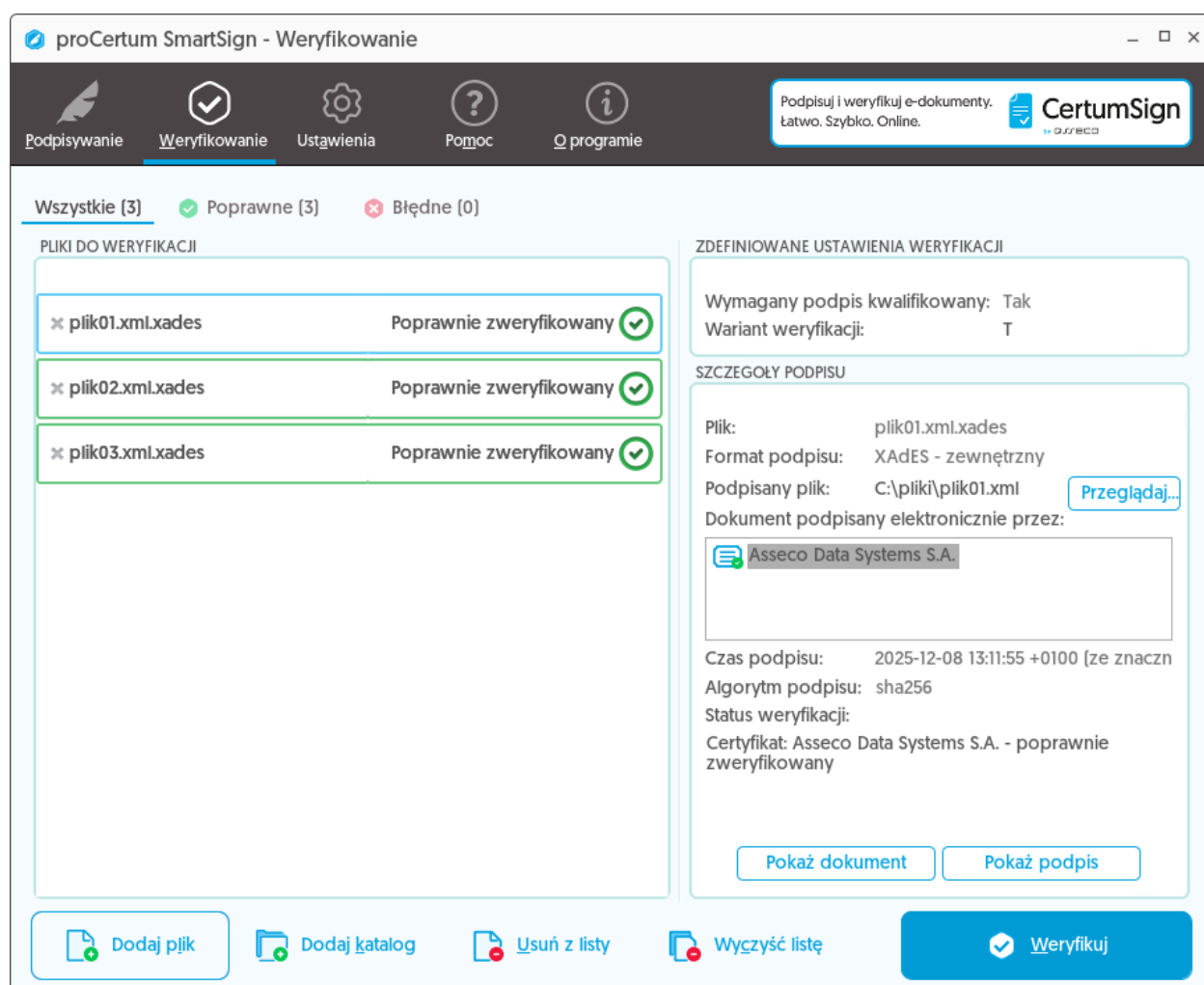
Rysunek 60: Podsumowanie weryfikacji

5.4.4. Status weryfikacji

Operacja weryfikacji może dać pozytywny lub negatywny rezultat. W zależności od wyniku operacji jej status będzie określony jako:

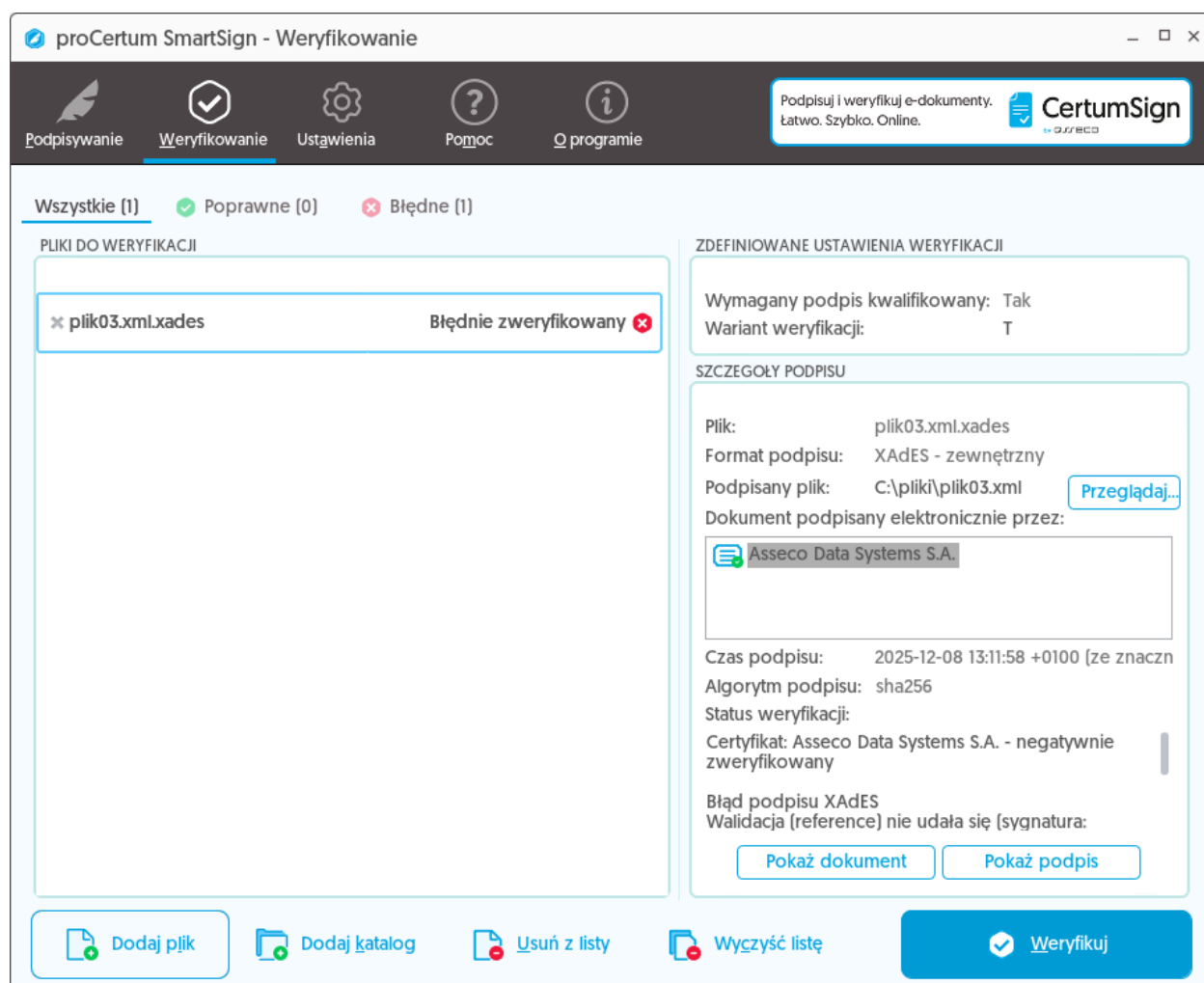
- **Poprawnie zweryfikowany;**
- **Błędnie zweryfikowany.**

Jeżeli status jest określony jako **Poprawnie zweryfikowany** to w sekcji **Informacje o podpisie** w polu **Status weryfikacji** widnieje wpis *Certyfikat: Łukasz Werkowski – poprawnie zweryfikowany*.



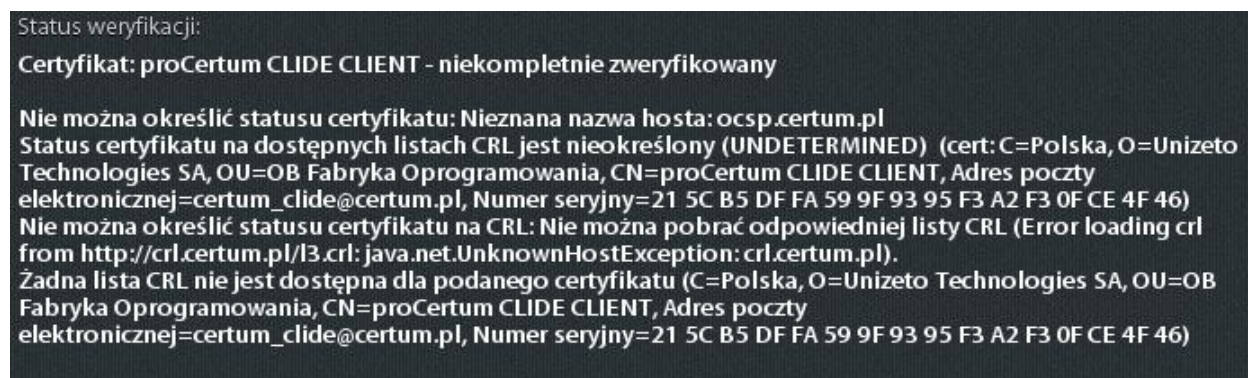
Rysunek 61: Status weryfikacji: Poprawnie zweryfikowany

Jeżeli status jest określony jako **negatywny** to element na liście jest oznaczony kolorem czerwonym, a w sekcji **Informacje o podpisie** w polu **Status weryfikacji** widnieje wpis *Certyfikat: Łukasz Werkowski – negatywnie zweryfikowany*.



Rysunek 62: Status weryfikacji: Błędnie zweryfikowany

Dla danego pliku podpisu w polu **Status weryfikacji** wskazana jest również przyczyna błędu. Przykładowe błędy są przedstawione na poniższych rysunkach.



Rysunek 63: Brak certyfikatu wystawcy lub niemożliwość pobrania aktualnych list CRL

Certyfikat: Adam Nowak - negatywnie zweryfikowany

Błąd podpisu XAdES
Walidacja (reference) nie udała się (sygnatura:
Signature_4fc2f279-55b6-4f20-9c2e-b0b225db750c_19; referencja:
Reference1_4fc2f279-55b6-4f20-9c2e-b0b225db750c_27).
Prawdopodobnie dane zostały zmienione.

Rysunek 64: Nieprawidłowa wartość podpisu

Status weryfikacji:
Certyfikat: MARUA - negatywnie zweryfikowany

Nie znaleziono certyfikatu (CN=LEVEL, OU=LEVEL, O=LEVEL,
L=Szczecin, ST=Zachodniopomorskie, C=PL)

Rysunek 65: Nieprawidłowy certyfikat

Status weryfikacji:
Certyfikat: Basic ID - negatywnie zweryfikowany

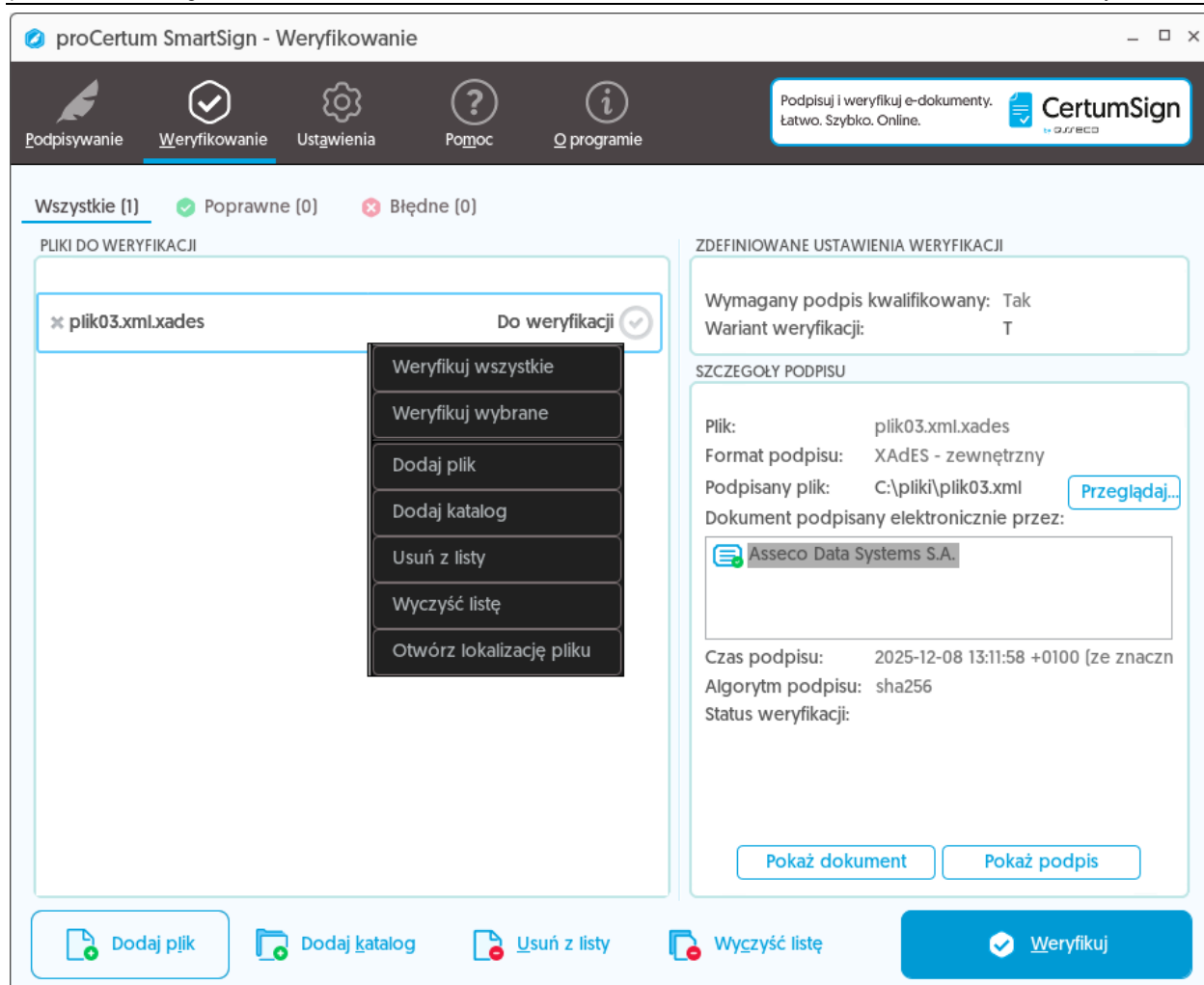
Błąd podpisu XAdES
Certyfikat podpisującego nie może być użyty jako certyfikat
kwalifikowany (C=Polska, CN=Basic ID, Adres poczty
elektronicznej=adam.nowak@assecods.pl, Numer
seryjny=67 27 7D 17 31 C6 12 E1 A4 12 3C B4 2C 18 F1 14)

Rysunek 66: Błąd przy weryfikacji certyfikatu niekwalifikowanego

5.4.5. Menu kontekstowe

Aby uruchomić **menu kontekstowe** należy nacisnąć prawym klawiszem myszki w dowolnym miejscu na liście. Dostępne jest 7 opcji w menu:

- **Weryfikuj wszystkie** – po wybraniu tej opcji zostanie zweryfikowany podpis wszystkich plików znajdujących się na liście.
- **Weryfikuj wybrane** – po wybraniu tej opcji zostanie zweryfikowany podpis tylko dla wybranych plików. Aby zaznaczyć więcej niż jeden plik należy przytrzymać lewy klawisz **Ctrl** i poprzez naciśnięcie lewego klawisza myszki wskazać następnego plik(i).
- **Dodaj plik** – opcja ta działa na takiej samej zasadzie jak przycisk **Dodaj plik**.
- **Dodaj katalog** – opcja ta działa na takiej samej zasadzie jak przycisk **Dodaj katalog**.
- **Usuń z listy** – opcja ta działa na takiej samej zasadzie jak przycisk **Usuń z listy**.
- **Wyczyść listę** – opcja ta działa na takiej samej zasadzie jak przycisk **Wyczyść listę**.
- **Otwórz lokalizację pliku** – opcja pozwala na wyświetlenie katalogu z plikiem.

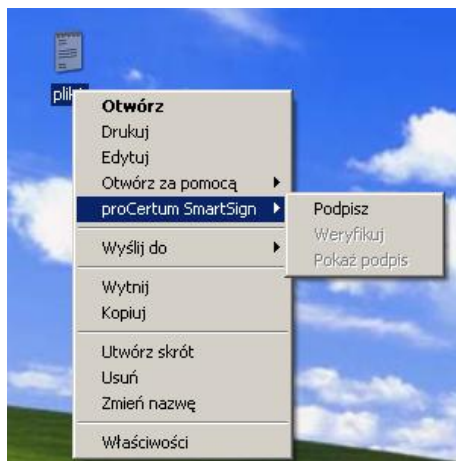


Rysunek 67: Zakładka Weryfikowanie – menu kontekstowe

5.5. Systemowe menu kontekstowe

Po zainstalowaniu aplikacji **proCertum SmartSign**, w systemie zostanie dodana nowa pozycja w menu kontekstowym. Aby uruchomić menu należy nacisnąć **prawym klawiszem myszy** na **dowolnym pliku**. W menu będzie widoczna nowa pozycja o nazwie **proCertum SmartSign**. Po wybraniu jej kursorem myszy pojawią się 3 opcje:

- **Podpisz** – po wybraniu tej opcji uruchomiona zostanie aplikacja **proCertum SmartSign** z wybraną zakładką **Podpisywanie**, a zaznaczony plik zostanie wczytany na listę plików przeznaczonych do podpisania. Dalsza procedura podpisywania jest przedstawiona punkcie 4.3.
- **Weryfikuj** – po wybraniu tej opcji uruchomiona zostanie aplikacja **proCertum SmartSign** z wybraną zakładką **Weryfikowanie**, a zaznaczony plik zostanie wczytany na listę plików przeznaczonych do weryfikacji. Ta opcja jest dostępna wyłącznie dla pliku podpisu. Dalsza procedura weryfikacji jest przedstawiona punkcie 4.4.
- **Pokaż podpis** – po wybraniu tej opcji zostaną wyświetlone **Dane podpisane** przy pomocy mechanizmów zawartych w aplikacji **proCertum SmartSign**. Ta opcja jest dostępna wyłącznie dla pliku podpisu.



Rysunek 68: Systemowe menu kontekstowe

5.6. Uruchamianie z linii poleceń

Aplikacja umożliwia uruchamianie jej z tzw. linii poleceń z parametrami. Dostępne są następujące parametry:

- -s, --sign [katalog] - parametr umożliwia podpisywanie plików ze wskazanego katalogu
- -v, --verify [katalog] - parametr umożliwia weryfikowanie plików ze wskazanego katalogu
- -r, --recursive – parametr ten w połączeniu z jednym z dwóch powyższych powoduje, że uwzględniany będzie wskazany katalog i jego podkatalogi
- -ss, --show-sign [plik] – umożliwia wyświetlenie informacji o podpisie znajdującym się we wskazanym pliku
- -V, --version – parametr ten umożliwia wyświetlenie informacji o aktualnej wersji aplikacji

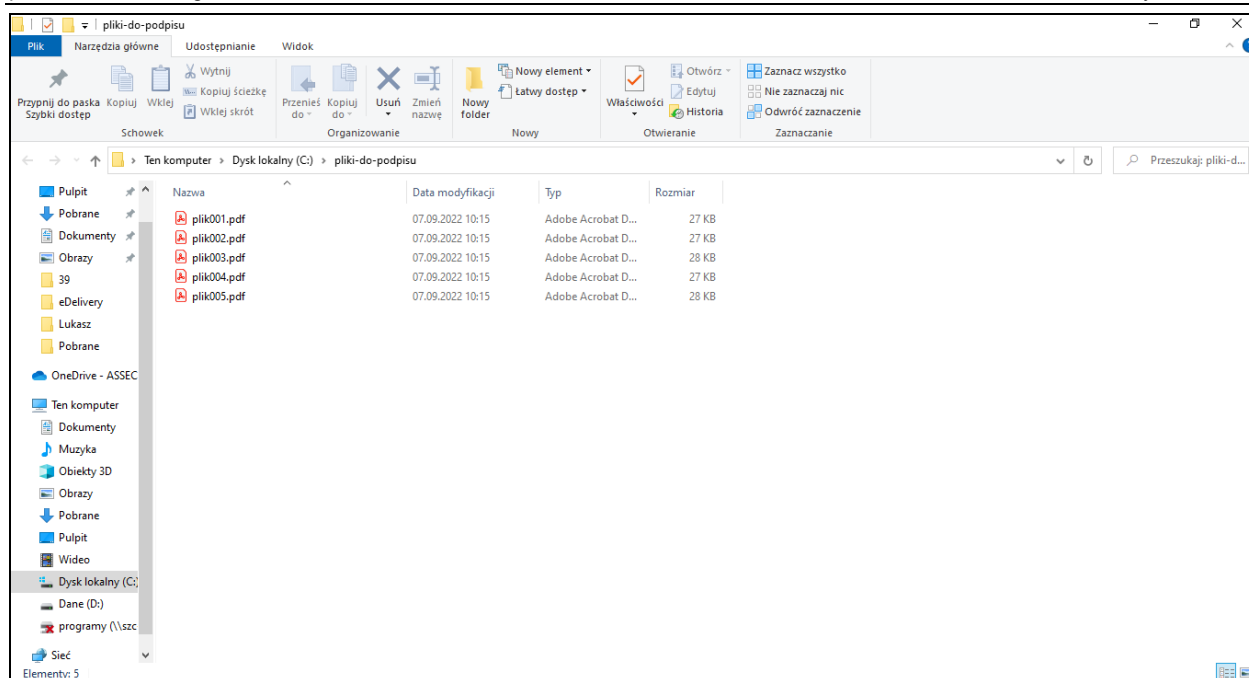
5.6.1. Przykłady

5.6.1.1. Podpisywanie plików

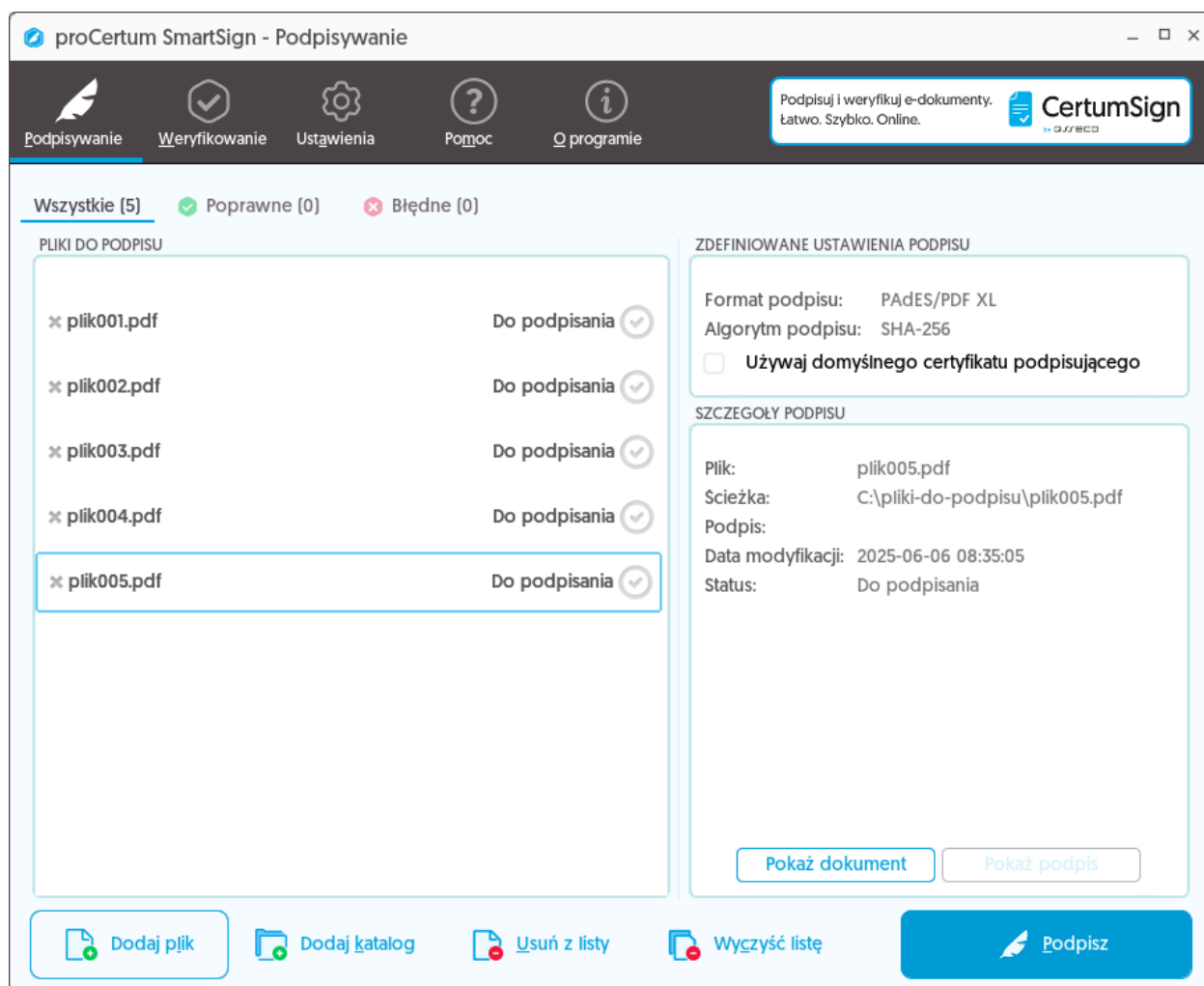
Poniżej przedstawiono przykład w którym uruchomiono aplikację z parametrem wskazującym katalog z plikami do podpisu.

Poniższe polecenie spowoduje uruchomienie aplikacji i załadowanie do zakładki **Podpisywanie**, plików znajdujących się w katalogu **C:\pliki-do-podpisu**:

```
proCertumSmartSign.exe -s C:\pliki-do-podpisu
```



Rysunek 69: Pliki do podpisania



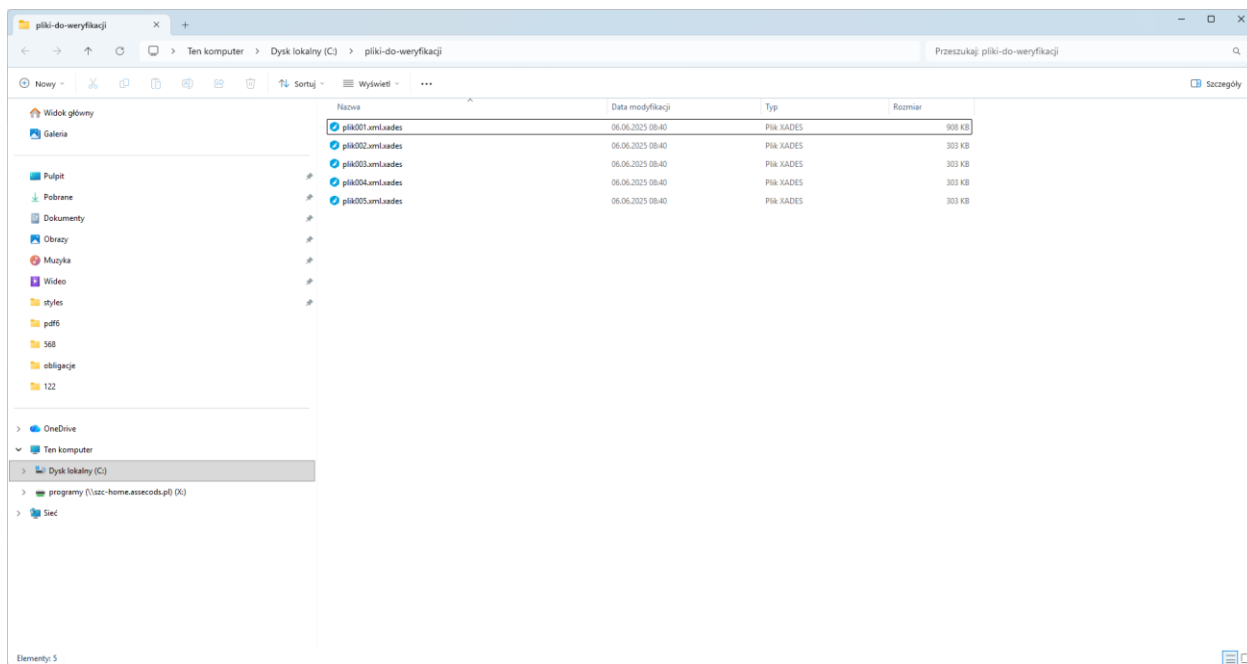
Rysunek 70: Pliki do podpisania umieszczone automatycznie w zakładce Podpisywanie

5.6.1.2. Weryfikowanie podpisów

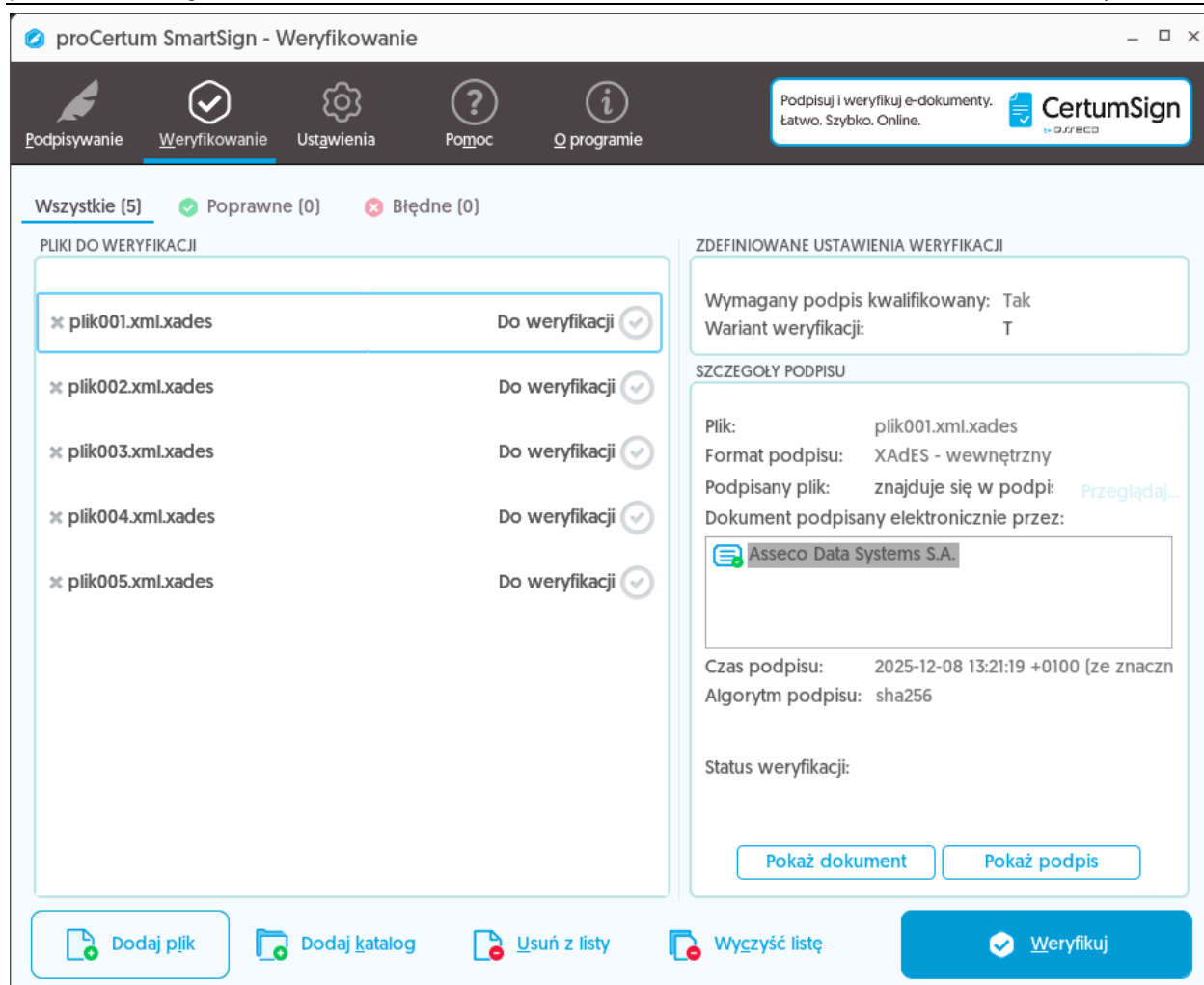
Poniżej przedstawiono przykład w którym uruchomiono aplikację z parametrem wskazującym katalog z plikami do weryfikacji.

Poniższe polecenie spowoduje uruchomienie aplikacji i załadowanie do zakładki **Weryfikowanie**, plików znajdujących się w katalogu **C:\pliki-do-weryfikacji**:

```
proCertumSmartSign.exe -v C:\pliki-do-weryfikacji
```



Rysunek 71: Pliki do weryfikacji



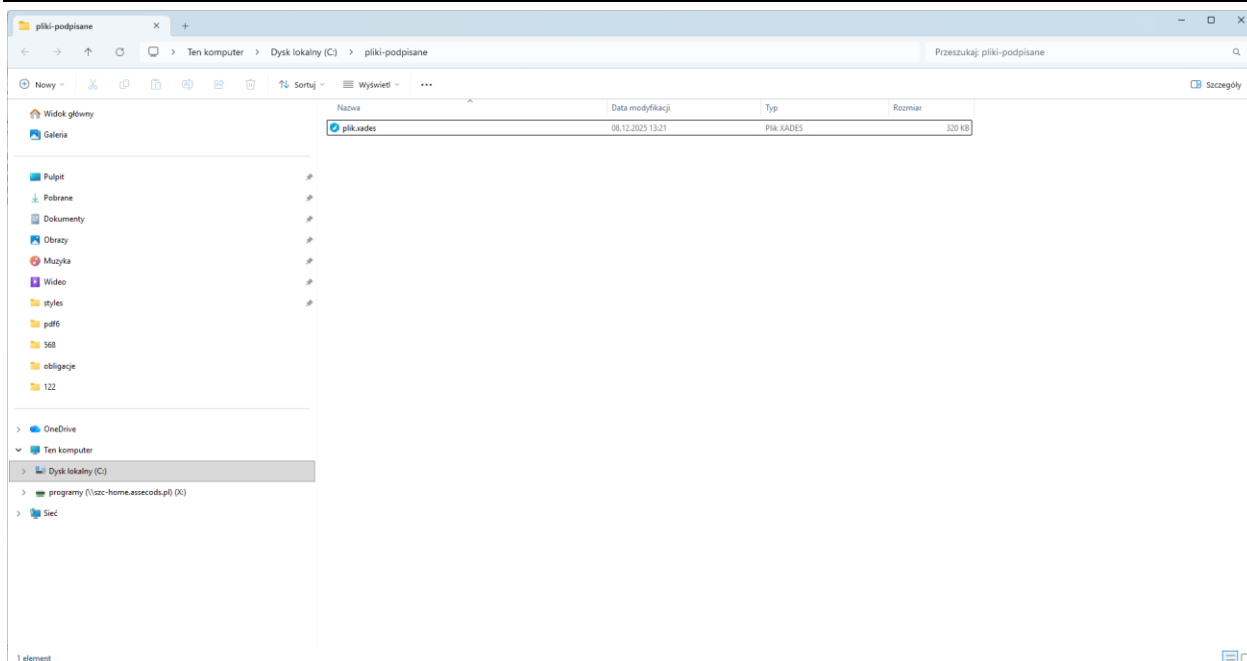
Rysunek 72: Pliki do weryfikacji umieszczone automatycznie w zakładce Weryfikowanie

5.6.1.3. Wyświetlenie informacji o podpisie

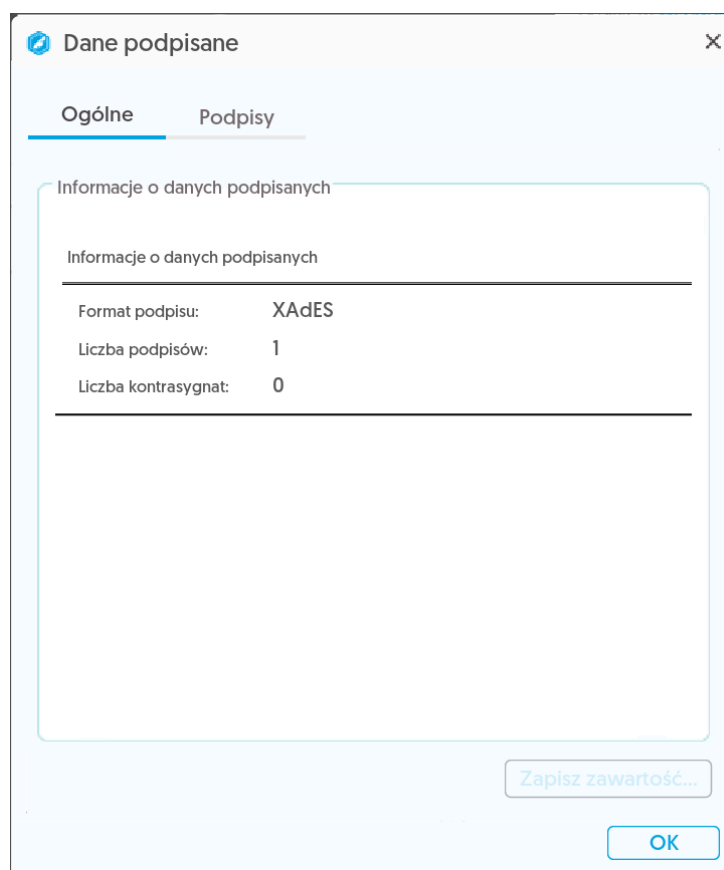
Poniżej przedstawiono przykład w którym uruchomiono aplikację z parametrem wskazującym podpisany plik

Poniższe polecenie spowoduje uruchomienie aplikacji i wyświetlenie informacji o podpisie:

```
proCertumSmartSign.exe -ss C:\pliki-podpisane\plik.xades
```



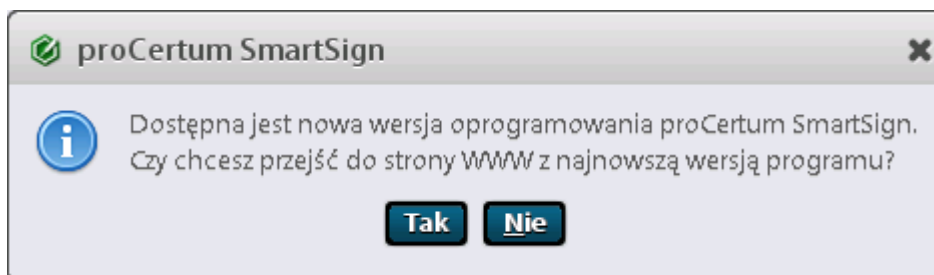
Rysunek 73: Pliki z podpisem



Rysunek 74: Informacje o podpisie

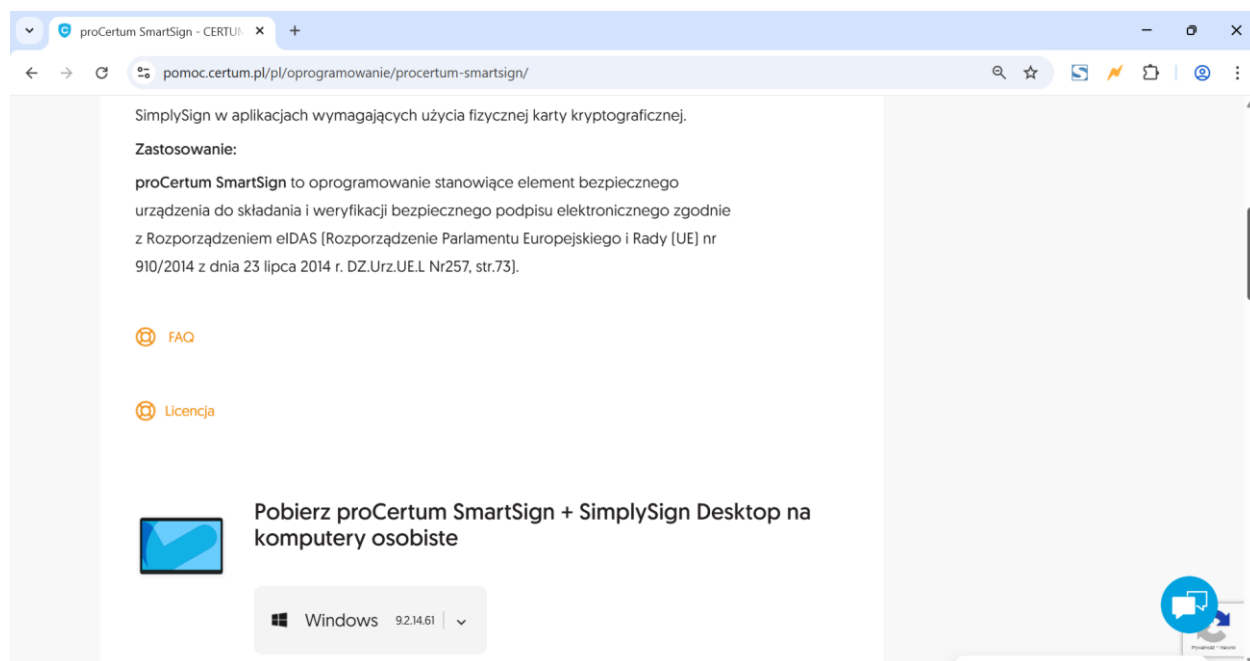
5.7. Powiadamianie o aktualizacji.

Podczas uruchamiania **proCertum SmartSign**, w zależności od konfiguracji (Ustawienia – Ogólne, pkt. 4.1.1), mechanizm **powiadamiania o aktualizacji** sprawdza, czy dostępna jest nowsza wersja aplikacji. W przypadku gdy używasz starszej wersji aplikacji, na ekranie pojawi się komunikat o możliwości pobrania najnowszej wersji.



Rysunek 75: Powiadomienie o aktualizacji

Po naciśnięciu przycisku **Tak** otworzy się okno ze **stroną WWW**, z której będzie można pobrać nową wersję aplikacji. **Aby mechanizm zadziałał komputer musi być podłączony do Internetu.**



Rysunek 76: Strona WWW z nową wersją proCertum SmartSign

6. Spis rysunków

Rysunek 1: Informacja o aktualizacji	6
Rysunek 2: Przebieg procesu aktualizacji	7
Rysunek 3: Informacja o zakończeniu aktualizacji	7
Rysunek 4: Ikona instalatora	9
Rysunek 5: Wybór języka oprogramowania	9
Rysunek 6: Okno powitalne kreatora instalacji	10
Rysunek 7: Umowa licencyjna	10
Rysunek 8: Wybór katalogu docelowego aplikacji	11
Rysunek 9: Wybór komponentów, które zostaną zainstalowane	11
Rysunek 10: Instalator jest gotowy do rozpoczęcia procesu instalacji	12
Rysunek 11: Zakończenie procesu instalacji	13
Rysunek 12: Okno główne aplikacji proCertum SmartSign	14
Rysunek 13: Informacja o niezgodności bibliotek	15
Rysunek 14: Informacje o systemie– Zakładka Biblioteki	15
Rysunek 15: Informacje o systemie– Zakładka Środowisko Java	16
Rysunek 16: Zakładka Pomoc	17
Rysunek 17: Zakładka Pomoc strona WWW	18
Rysunek 18: Zakładka - Ustawienia	18
Rysunek 19: Zakładka Ustawienia – Ogólne	19
Rysunek 20: Zakładka Ustawienia – Podpis – część dotycząca Formatu podpisu, Typu podpisu i ustawień Archiwizacji	20
Rysunek 21: Zakładka Ustawienia – Podpis – część dotycząca Domyślnego certyfikatu i dodatkowych opcji podpisu	21
Rysunek 22: Zakładka Ustawienia – Podpis – część dotycząca zaawansowanych opcji podpisu	23
Rysunek 23: Zakładka Ustawienia – Podpis –Lokalizacja podpisującego	24
Rysunek 24: Zakładka Ustawienia – Podpis – Zaawansowane opcje podpisu XAdES	24
Rysunek 25: Zakładka Ustawienia - Weryfikacja	25
Rysunek 26: Zakładka Ustawienia – Znacznik czasu	26
Rysunek 27: Zakładka Podpisywanie	28
Rysunek 28: Zakładka Podpisywanie – Lista elementów do podpisania	29
Rysunek 29: Wyszukiwanie certyfikatów	29
Rysunek 30: Lista certyfikatów kwalifikowanych	30
Rysunek 31: Lista certyfikatów kwalifikowanych i niekwalifikowanych	30
Rysunek 32: Wybór certyfikatu dla operacji podpisu	31
Rysunek 33: Prośba o wprowadzenie kodu PIN	31
Rysunek 34: Podpisywanie... - Wyszukiwanie kluczy	32
Rysunek 35: Podpisywanie... - Wykonywanie podpisu	32
Rysunek 36: Podsumowanie podpisywania	32
Rysunek 37: Zakładka Podpisywanie – wykonany podpis	33
Rysunek 38: Dane podpisane – zakładka ogólne	34
Rysunek 39: Dane podpisane - zakładka podpis	34
Rysunek 40: Okno wyboru akcji przy obecnym już co najmniej jednym podpisie	35
Rysunek 41: Dane podpisane - zakładka ogólne dla podpisu wielokrotnego	35
Rysunek 42: Dane podpisane - zakładka podpis dla podpisu wielokrotnego	36
Rysunek 43: Okno wyboru akcji przy obecnym już co najmniej jednym podpisie	36
Rysunek 44: Okno wyboru podpisu, który chcemy kontrasygnować	37

Rysunek 45: Okno wyboru podpisu, gdy wybrano wszystkie podpisy do kontrasygnowania	37
Rysunek 46 Dane podpisane - zakładka ogólne dla kontrasygnaty	38
Rysunek 47 Dane podpisane - zakładka podpis dla kontrasygnaty	39
Rysunek 48 Dodawanie graficznego symbolu podpisu – okno główne	40
Rysunek 49 Dodawanie graficznego symbolu podpisu – wskazanie pliku graficznego	40
Rysunek 50 Dodawanie graficznego symbolu podpisu – wybrany plik graficzny	41
Rysunek 51 Dodawanie graficznego symbolu podpisu – symbol graficzny dodany do dokumentu	41
Rysunek 52 Dodawanie graficznego symbolu podpisu – podpisany plik z umieszczonym graficznym symbolem podpisu.....	42
Rysunek 53 Dodawanie graficznego symbolu podpisu – podpisywanie wielu plików	42
Rysunek 54: Zakładka Podpisywanie – menu kontekstowe	43
Rysunek 55: Zakładka Weryfikowanie.....	44
Rysunek 56: Zakładka Weryfikowanie – Lista elementów do weryfikacji	45
Rysunek 57: Dane podpisane	46
Rysunek 58: Zakładka Weryfikowanie – Lista elementów do weryfikacji	47
Rysunek 59: Weryfikacja.....	47
Rysunek 60: Podsumowanie weryfikacji	48
Rysunek 61: Status weryfikacji: Poprawnie zweryfikowany	48
Rysunek 62: Status weryfikacji: Błędnie zweryfikowany	49
Rysunek 63: Brak certyfikatu wystawcy lub niemożliwość pobrania aktualnych list CRL	49
Rysunek 64: Nieprawidłowa wartość podpisu	50
Rysunek 65: Nieprawidłowy certyfikat	50
Rysunek 66: Błąd przy weryfikacji certyfikatu niekwalifikowanego	50
Rysunek 67: Zakładka Weryfikowanie – menu kontekstowe	51
Rysunek 68: Systemowe menu kontekstowe	52
Rysunek 69: Pliki do podpisania	53
Rysunek 70: Pliki do podpisania umieszczone automatycznie w zakładce Podpisywanie	53
Rysunek 71: Pliki do weryfikacji	54
Rysunek 72: Pliki do weryfikacji umieszczone automatycznie w zakładce Weryfikowanie	55
Rysunek 73: Pliki z podpisem	56
Rysunek 74: Informacje o podpisie	56
Rysunek 75: Powiadomienie o aktualizacji.....	57
Rysunek 76: Strona WWW z nową wersją proCertum SmartSign	57