



Podręcznik użytkownika

proCertum SmartSign 9.4

Wersja dokumentacji 1.03

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. INSTALACJA APLIKACJI	6
4. OBSŁUGA APLIKACJI	7
4.1. Pomoc	8
4.2. Ustawienia	10
4.2.1. Ustawienia – Ogólne	11
4.2.2. Ustawienia – Podpis	12
4.2.3. Ustawienia – Weryfikacja	18
4.2.3.1. Podstawowe opcje weryfikacji	18
4.2.3.2. Dodatkowe opcje weryfikacji	19
4.2.4. Ustawienia – Znacznik czasu	19
4.3. Podpisywanie plików	21
4.3.1. Dodawanie elementów do listy	22
4.3.2. Operacja podpisu	22
4.3.3. Podpis wielokrotny	29
4.3.4. Kontrasynata	32
4.3.5. Podpisywanie plików PDF	36
4.3.5.1. Dodawanie graficznego symbolu podpisu	36
4.4. Weryfikowanie podpisów	40
4.4.1. Dodawanie elementów do listy	40
4.4.2. Informacje o podpisie i weryfikowanym dokumencie	41
4.4.3. Operacja weryfikacji	42
4.4.4. Status weryfikacji	44
4.5. Powiadamianie o aktualizacji	47
5. SPIS RYSUNKÓW	49

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 przez Asseco Data Systems S.A.
- 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**:

- system operacyjny (architektura x86-64): dystrybucje Debian, Ubuntu, Mint, Centos, Fedora
- środowisko graficzne: Cinnamon, MATE lub KDE Plasma;
- 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. Instalacja aplikacji

Instalację aplikacji rozpoczyna się poprzez uruchomienie w terminalu pakietu instalacyjnego o nazwie SimplySignDesktop-2.9.8-9.1.6.0-x86_64-prod-ubuntu.bin.

Instalator powinien być uruchomiony w terminalu, na prawach zwykłego użytkownika.

Instalację przedstawia poniższy listing – pogrubioną, podkreśloną czcionką zaznaczono miejsca, w których następuje interakcja z Użytkownikiem.

administrator@administrator-OptiPlex-390:~/Pobrane\$./SimplySignDesktop-2.9.8-9.1.6.0-x86_64-prod-ubuntu.bin

Verifying archive integrity... 100% All good.

Uncompressing SimplySign Desktop 2.9.8 - proCertum SmartSign 9.1.6.0 100%

Instalacja oprogramowania SimplySign Desktop 2.9.8 oraz
proCertum SmartSign 9.1.6.0

Pakiety przeznaczone dla dystrybucji Debian, Ubuntu lub Mint.

Instalator powinien być uruchomiony w terminalu, na prawach zwykłego użytkownika.

Czy chcesz kontynuować (tak/nie)?

Instalator wymaga praw administratora.

Musisz uwierzytelnić się poprzez sudo:

[sudo] password for administrator:

System operacyjny : linux

Architektura systemu : x86_64

Instalacja aplikacji SimplySign Desktop.

Instalacja zostanie przeprowadzona dla użytkownika administrator (grupa administrator)

a odpowiednie pliki konfiguracyjne zostaną umieszczone

w jego katalogu domowym t/j /home/administrator

Czy chcesz kontynuować (tak/nie)?

Katalog /opt/SimplySignDesktop już istnieje.

Chcesz wymazać jego zawartość i kontynuować instalację (tak/nie)?

Zamykanie uruchomionej instancji (jeśli jest uruchomiona) SimplySignDesktop...

Trwa instalacja. Kopiowanie elementów. Czekaj...

Tworzenie konfiguracji użytkownika...

Tworzenie pliku dla desktopu w celu wyświetlenia ikonki aplikacji na desktopie...

Instalacja aplikacji SimplySign Desktop zakończyła się powodzeniem.

Instalacja aplikacji proCertum SmartSign.

Instalacja zostanie przeprowadzona dla użytkownika administrator (grupa administrator)

Czy chcesz kontynuować (tak/nie)?

Katalog /opt/proCertumSmartSign już istnieje.

Chcesz wymazać jego zawartość i kontynuować instalację (tak/nie)?

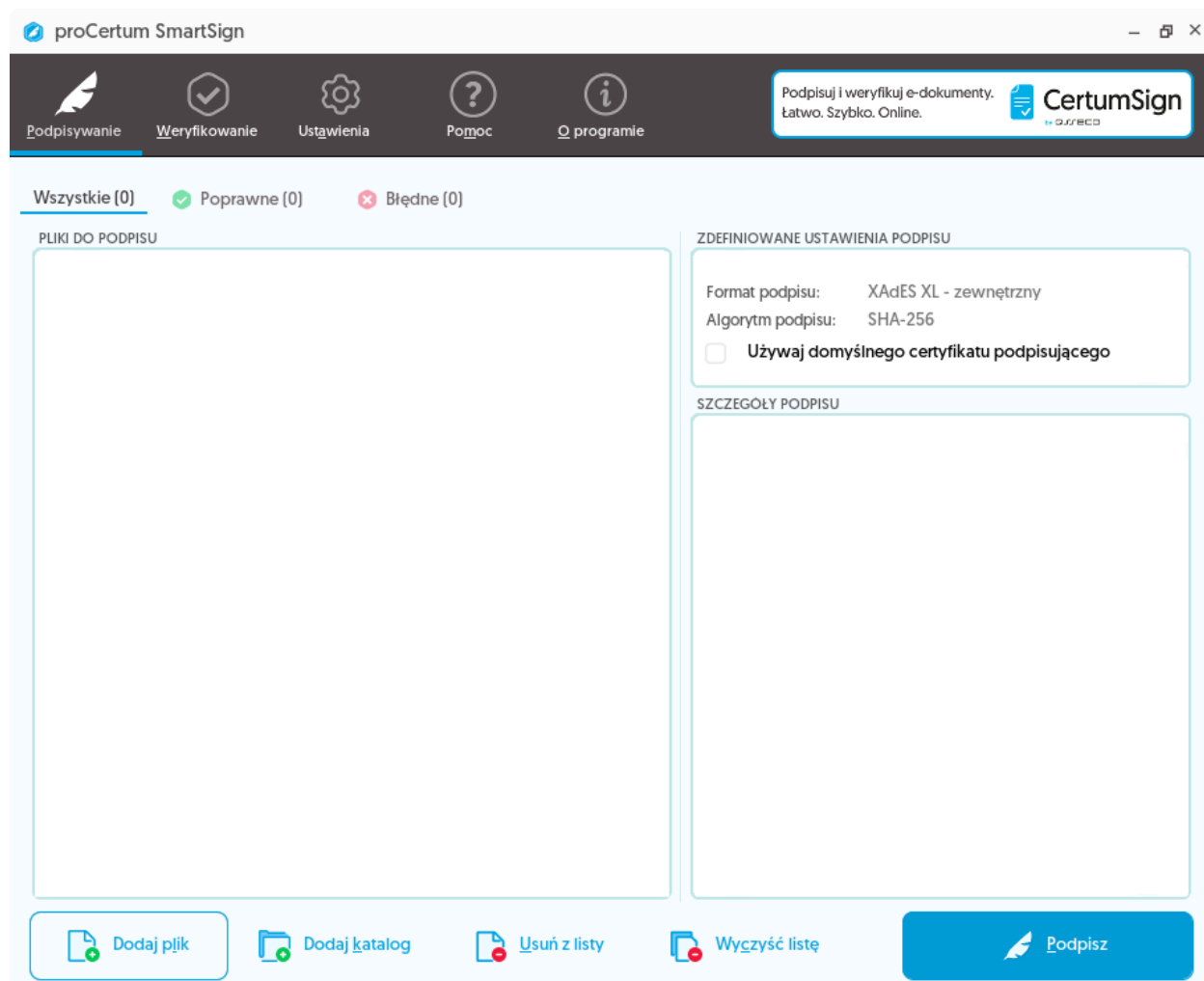
Trwa instalacja. Kopiowanie elementów. Czekaj...

Tworzenie pliku dla desktopu w celu wyświetlenia ikonki aplikacji na desktopie...

Instalacja aplikacji proCertum SmartSign zakończyła się powodzeniem.

4. Obsługa aplikacji

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

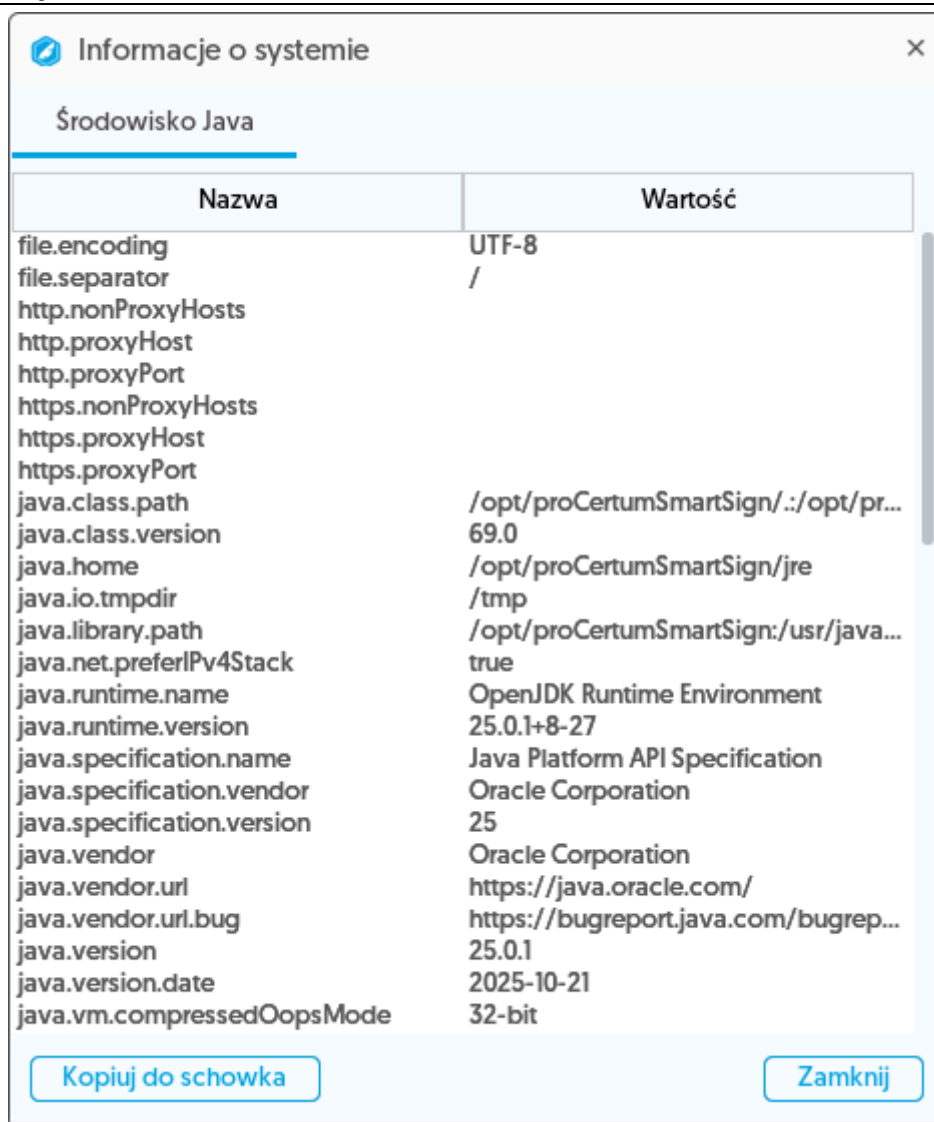


Rysunek 1: Okno główne aplikacji proCertum SmartSign

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**.

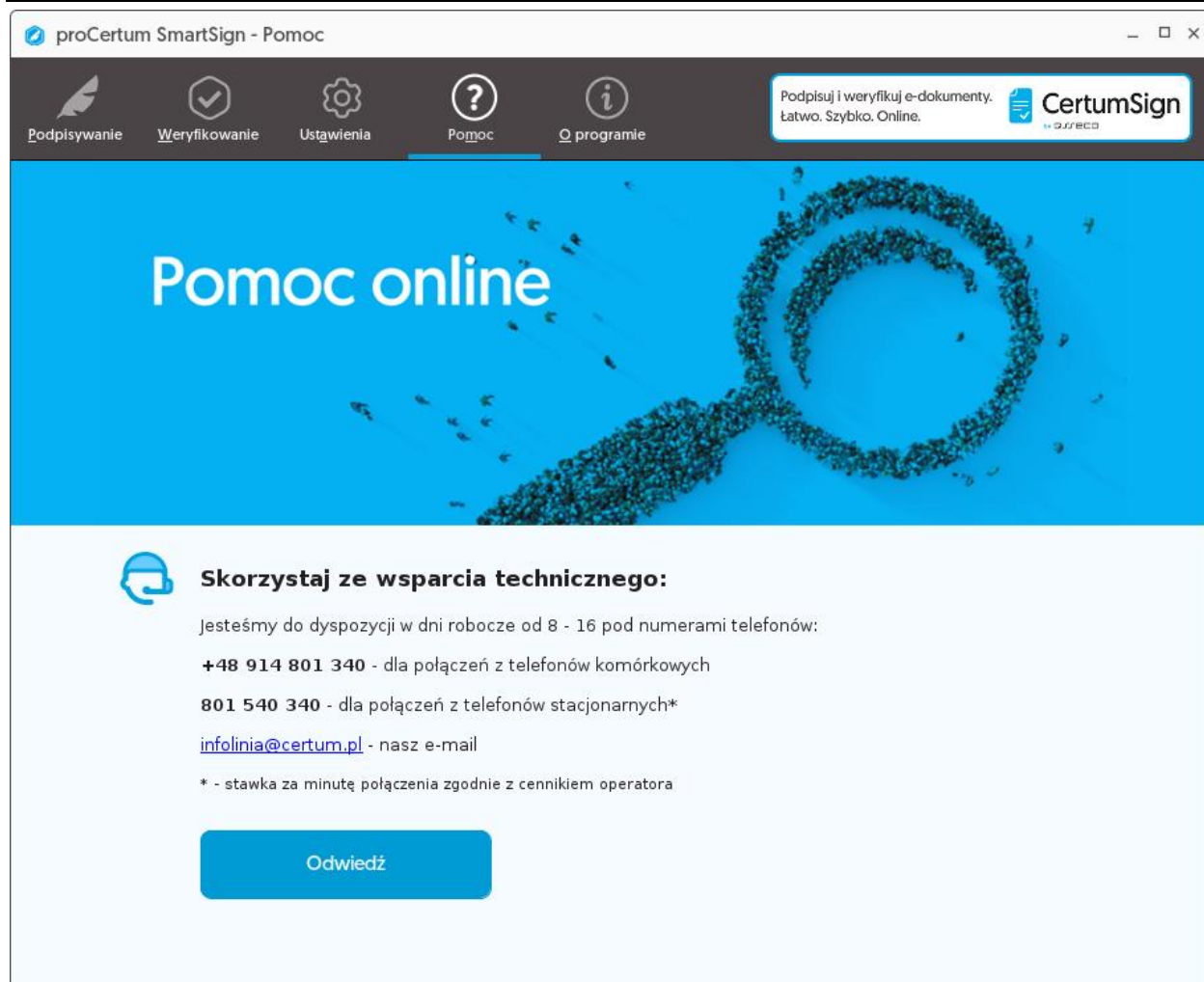
W oknie powitalnym oraz w oknie **O programie** znajduje się przycisk **Informacje o systemie**. Jego naciśnięcie powoduje wyświetlenie okna zawierającego informacje o środowisku, w którym uruchomiona została aplikacja.



Rysunek 2: Informacje o systemie– Zakładka Środowisko Java

4.1. Pomoc

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

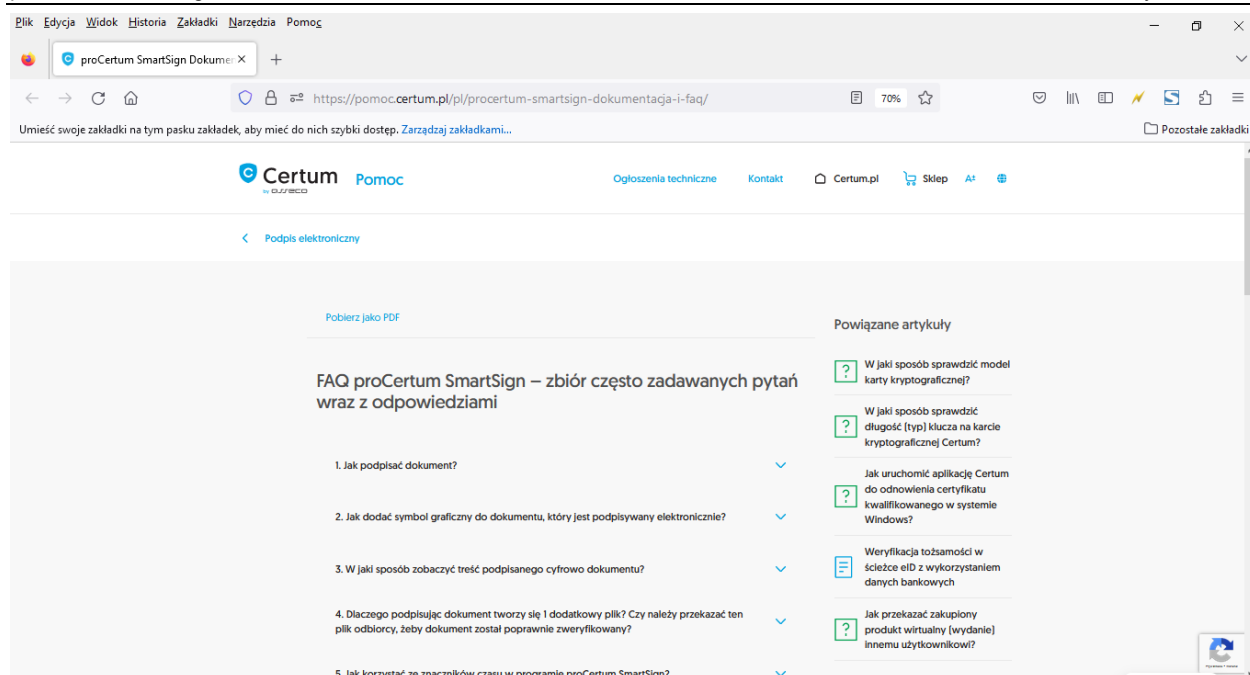


Rysunek 3: Zakładka Pomoc

Sekcja **Pomoc** podzielona została na 3 grupy:

- **Pierwsze kroki** – informacje w zakresie wymagań sprzętowych i programowych, procesu instalacji, pierwszego uruchomienia aplikacji, itp.
- **Uzyskaj pomoc** – ogólne informacje o programie
- **Potrzebuję wsparcia** – informacje w zakresie uzyskania wsparcia telefonicznego, mailowego

Po wybraniu tematu pomocy użytkownik zostanie przekierowany do stosownej sekcji na stronie www.



Rysunek 4: Zakładka Pomoc strona WWW

4.2. 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 5: Zakładka - Ustawienia

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

4.2.1. 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.

The screenshot shows the 'proCertum SmartSign - Ustawienia' window. The top navigation bar includes icons for 'Podpisywanie', 'Weryfikowanie', 'Ustawienia' (active), 'Pomoc', and 'O programie'. A 'CertumSign' logo is also present. Below the navigation bar, the 'Ogólne' tab is selected, with other tabs being 'Podpis', 'Weryfikacja', and 'Znacznik czasu'. The 'AKTUALIZACJE' section shows a dropdown for 'Sprawdzanie dostępnych aktualizacji' set to 'raz dziennie', with a 'Sprawdź' button and a timestamp '[Ostatnio sprawdzano: 2026-01-29 06:18:54]'. The 'PROXY' section contains checkboxes for 'Używaj proxy' and 'Pobierz proxy automatycznie'. Below these are input fields for 'Host', 'Port', and 'Wyłącz proxy dla', with a note 'Poszczególne hosty rozdzielć znakiem ";"'. There is also a 'Wymagana autoryzacja' section with 'Użytkownik' and 'Hasło' fields. The 'HISTORIA' section has a checkbox for 'Zapisuj historię użycia certyfikatu'. At the bottom, there is a button labeled 'Ustawienia domyślne'.

Rysunek 6: Zakładka Ustawienia – Ogólne

4.2.2. 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 7: Zakładka Ustawienia – Podpis – część dotycząca Formatu podpisu, Typu podpisu i ustawień Archiwizacji

Możemy określić następujące parametry:

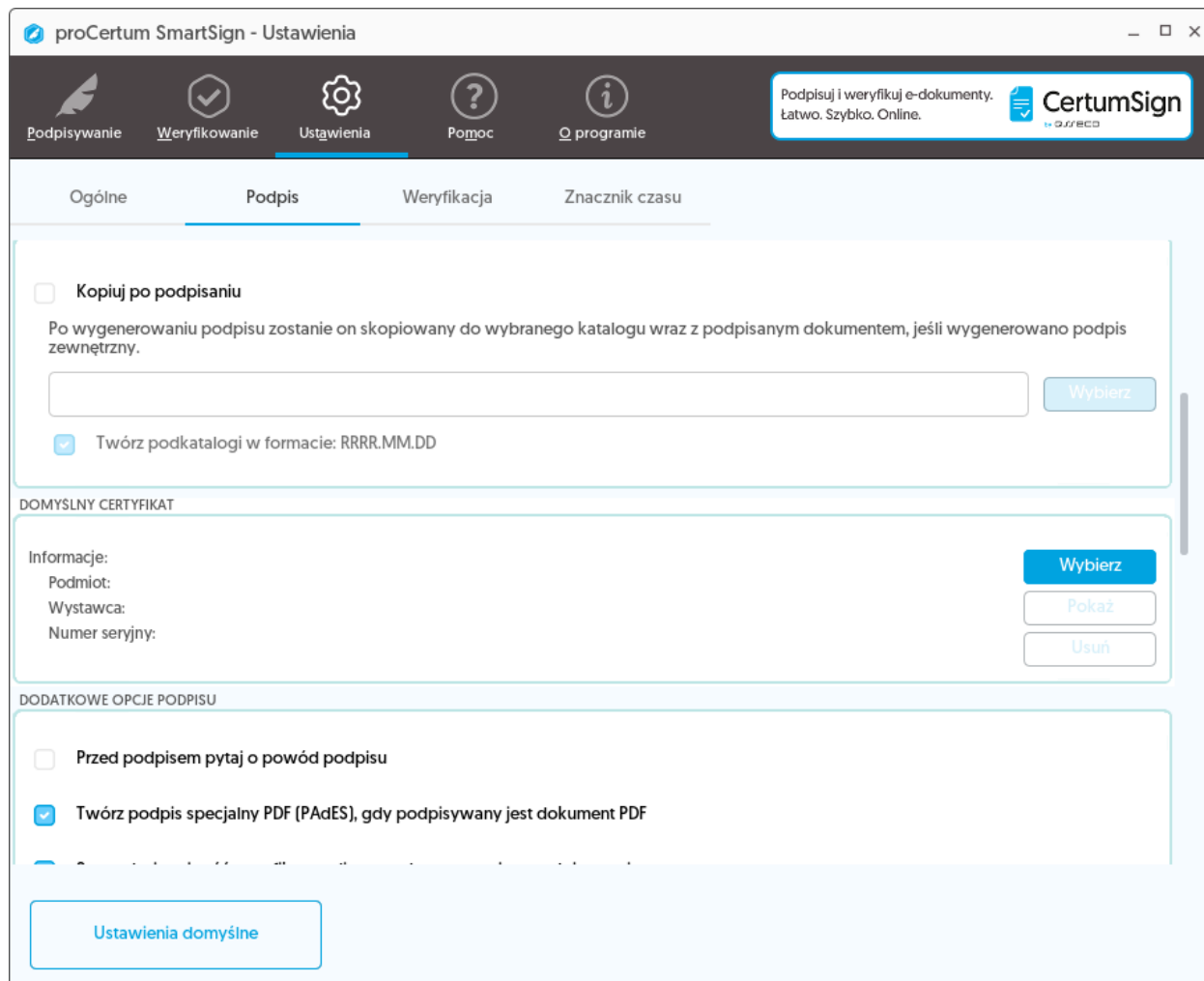
- **Format podpisu:**
 - **XAdES** – Podpis elektroniczny w formacie **XAdES**;
 - **CAdES/ETSI** – Podpis elektroniczny w formacie **CAdES/ETSI**;
- **Funkcja skrótu** – parametr oznacza nazwę funkcji skrótu używanej podczas składania podpisu. Obecnie możliwe do wyboru tylko SHA-256;

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.

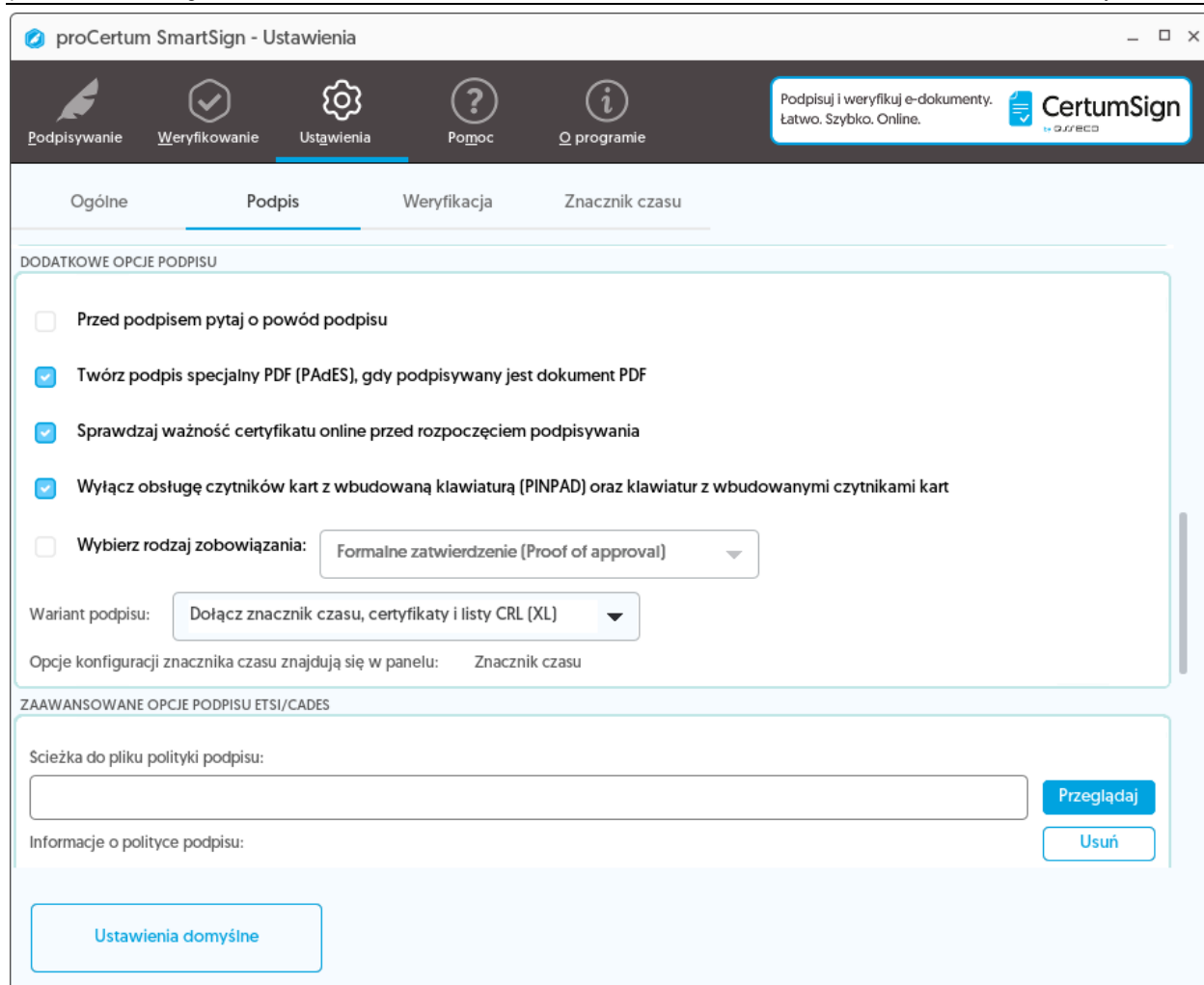


Rysunek 8: Zakładka Ustawienia – Podpis – część dotycząca Domyślnego certyfikatu i dodatkowych opcji podpisu

- **Archiwizacja:**

- **Kopuj 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.

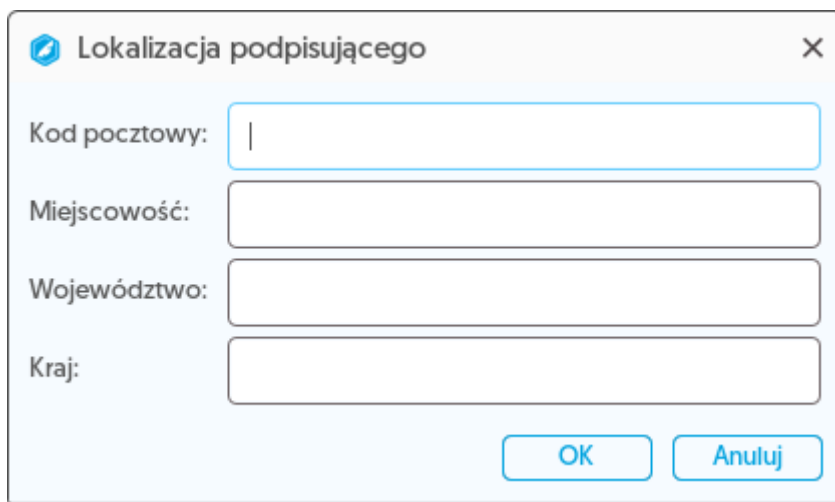
- **Dodatkowe opcje podpisu:**
 - **Przed podpisaniem pytaj o powód podpisu** – wybranie tej opcji spowoduje, że przed wykonaniem podpisu aplikacja zaprezentuje okno umożliwiające wybór powodu podpisu, który umieszczony zostanie w strukturze podpisu i prezentowany będzie później we właściwościach podpisu.
 - **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 9: Zakładka Ustawienia – Podpis – część dotycząca zaawansowanych opcji podpisu

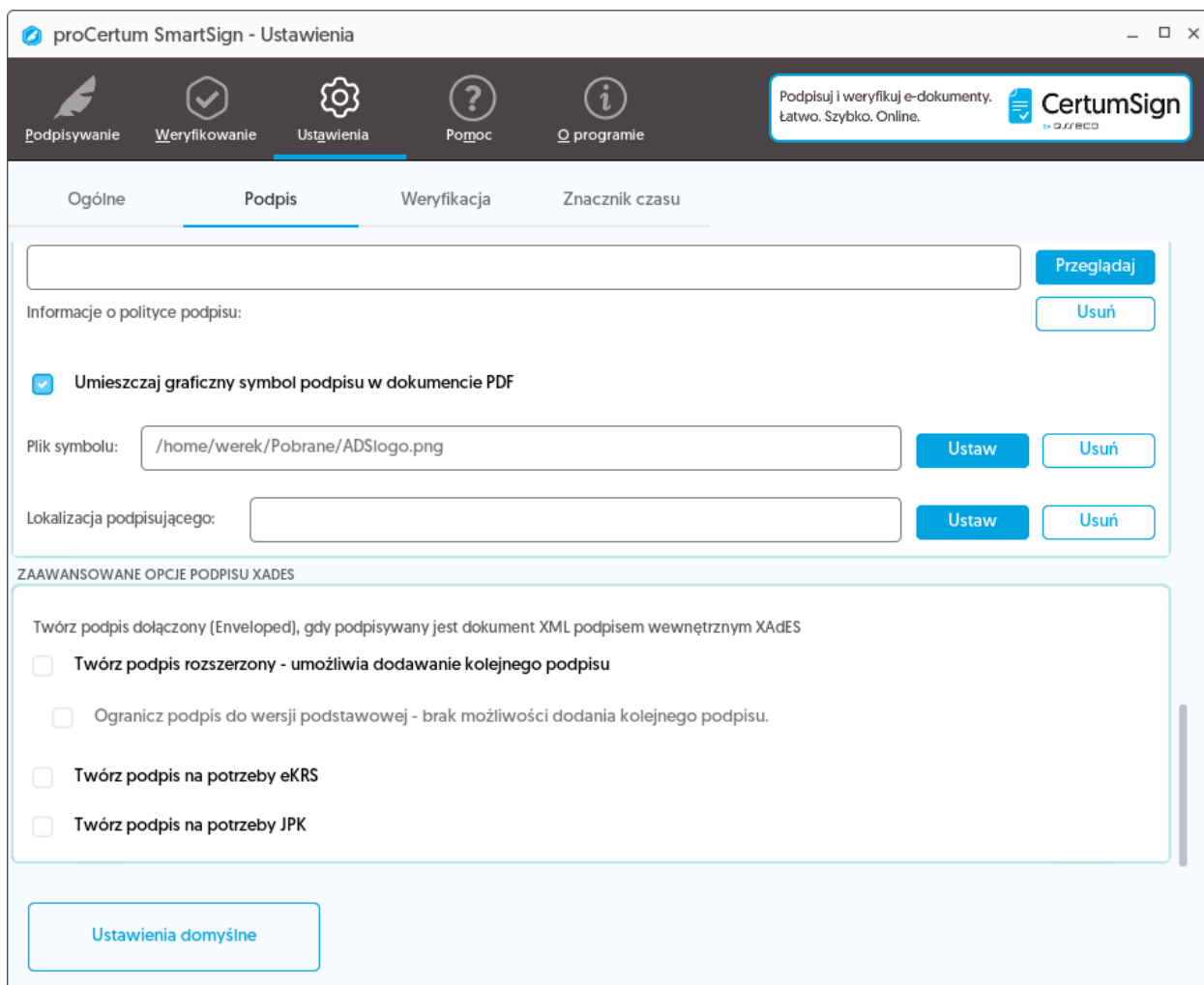
- Zaawansowane opcje podpisu ETSI/CADES
 - **Ścieżka do pliku polityki podpisu** – wskazuje na ścieżkę do pliku Polityki Podpisu definiującej kryteria składania i weryfikacji podpisu. Wybór odpowiedniej polityki podpisu dokonuje się przyciskiem **Przeglądaj**. Przycisk **Usuń** pozwala na usunięcie wybranej 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

- **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 input fields: "Kod pocztowy:" (Postal code), "Miejscowość:" (Locality), "Województwo:" (Voivodeship), and "Kraj:" (Country). At the bottom right are two buttons: "OK" and "Anuluj" (Cancel).

Rysunek 10: Zakładka Ustawienia – Podpis –Lokalizacja podpisującego



Screenshot of the "proCertum SmartSign - Ustawienia" (Settings) window. The "Podpis" (Signature) tab is selected. The interface includes a navigation bar with icons for "Podpisywanie" (Signing), "Weryfikowanie" (Verification), "Ustawienia" (Settings), "Pomoc" (Help), and "O programie" (About). A banner at the top right says "Podpisuj i weryfikuj e-dokumenty. Łatwo. Szybko. Online. CertumSign by ASSECO".

Under the "Podpis" tab, there are four sub-tabs: "Ogólne" (General), "Podpis" (Signature), "Weryfikacja" (Verification), and "Znacznik czasu" (Timestamp). The "Podpis" sub-tab is active.

Settings for the "Podpis" sub-tab include:

- A text input field for "Informacje o polityce podpisu:" (Information about the signing policy) with "Przeglądaj" (Browse) and "Usuń" (Delete) buttons.
- A checked checkbox "Umieszczaj graficzny symbol podpisu w dokumencie PDF" (Place graphical signature symbol in PDF document).
- A text input field for "Plik symbolu:" (Symbol file) showing "/home/werek/Pobrane/ADSIlogo.png" with "Ustaw" (Set) and "Usuń" (Delete) buttons.
- A text input field for "Lokalizacja podpisującego:" (Location of the signer) with "Ustaw" (Set) and "Usuń" (Delete) buttons.

Below these settings is a section titled "ZAAWANSOWANE OPCJE PODPISU XAdES" (Advanced XAdES Signature Options) with several unchecked checkboxes:

- "Twórz podpis dołączony (Enveloped), gdy podpisywany jest dokument XML podpisem wewnętrznym XAdES" (Create attached signature (Enveloped) when signing XML document with internal XAdES signature).
- "Twórz podpis rozszerzony - umożliwia dodawanie kolejnego podpisu" (Create extended signature - enables adding another signature).
- "Ogranicz podpis do wersji podstawowej - brak możliwości dodania kolejnego podpisu." (Limit signature to basic version - no possibility of adding another signature).
- "Twórz podpis na potrzeby eKRS" (Create signature for eKRS).
- "Twórz podpis na potrzeby JPK" (Create signature for JPK).

At the bottom left is a button labeled "Ustawienia domyślne" (Default settings).

Rysunek 11: Zakładka Ustawienia – Podpis – Zaawansowane opcje podpisu XAdES

- Zaawansowane opcje podpisu XAdES
 - **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

4.2.3. Ustawienia – Weryfikacja

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

The screenshot shows the 'Ustawienia' (Settings) window of the proCertum SmartSign application, specifically the 'Weryfikacja' (Verification) tab. The window has a dark header with navigation icons for 'Podpisywanie', 'Weryfikowanie', 'Ustawienia', 'Pomoc', and 'O programie'. A 'CertumSign' logo is also present. Below the header, there are four sub-tabs: 'Ogólne', 'Podpis', 'Weryfikacja' (selected), and 'Znacznik czasu'. The 'USTAWIENIA WERYFIKACJI' section contains two checked options: 'Weryfikacja podpisu kwalifikowanego' (with a list of criteria) and 'Eksportuj dane jeśli są zawarte w pliku podpisu'. Under the second option, 'Eksportuj do katalogu, w którym znajduje się podpis' is selected. The 'DODATKOWE OPCJE WERYFIKACJI' section shows 'Wariant weryfikacji' set to 'Dołącz znacznik czasu, certyfikaty i listy CRL (XL)'. At the bottom, there is a 'Ustawienia domyślne' button.

Rysunek 12: Zakładka Ustawienia - Weryfikacja

4.2.3.1. 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.

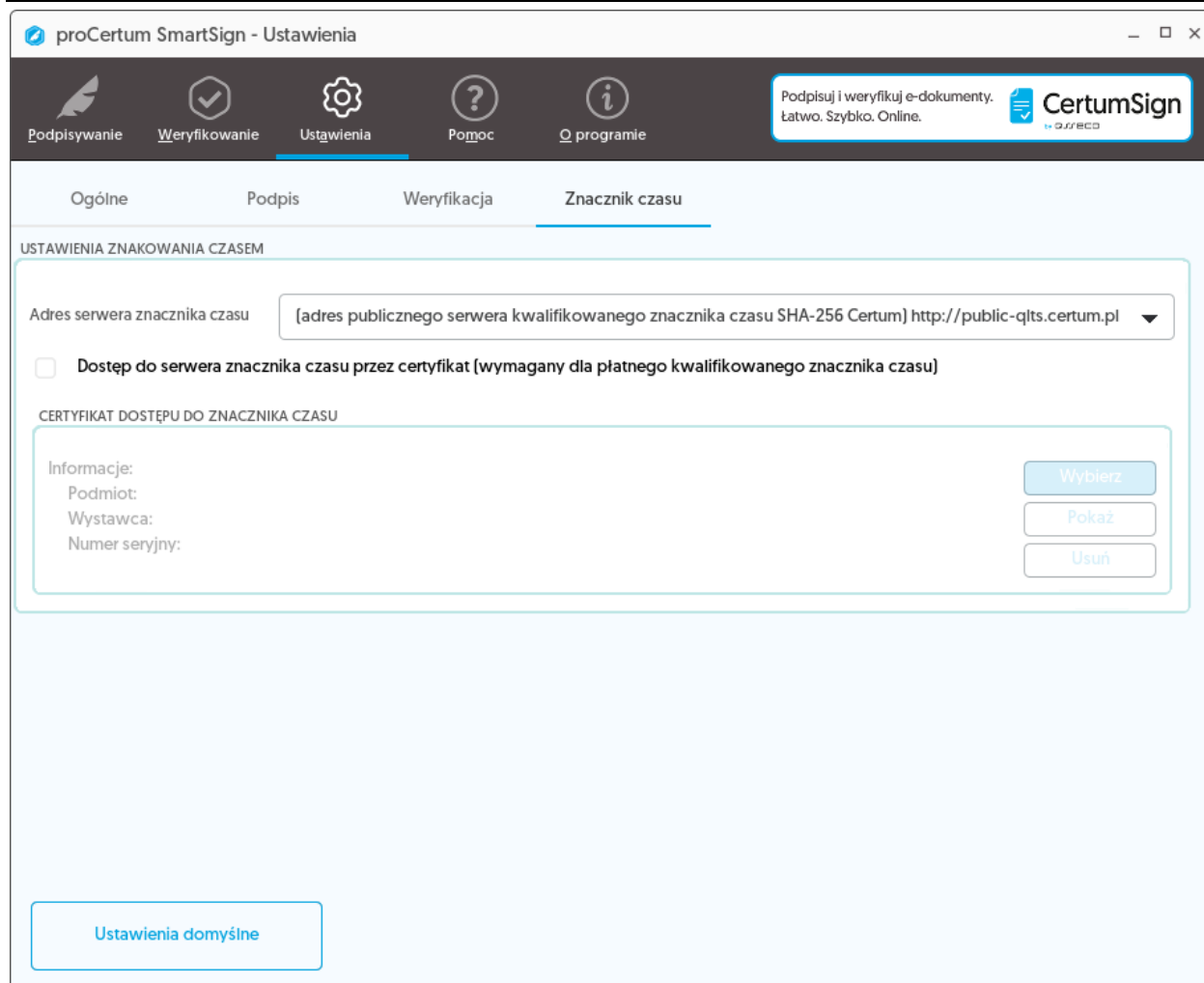
4.2.3.2. Dodatkowe opcje weryfikacji

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 podległa 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**;

4.2.4. Ustawienia – Znacznik czasu

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



Rysunek 13: Zakładka Ustawienia – Znacznik czasu

Możemy określić następujące parametry:

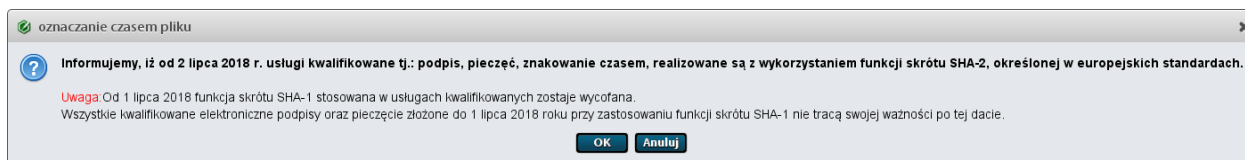
- **Adres serwera znacznika czasu** umożliwia włączenie znakowania pliku podpisu znacznikiem czasu – dostępne są następujące predefiniowane ustawienia:
 - adres publicznego serwera kwalifikowanego znacznika czasu SHA-256 Certum – publiczny kwalifikowany znacznik czasu, który nie wymaga posiadania certyfikatu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

Dodatkowo ręcznie można dodać następujące pozycje:

- <http://qlts.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!!!

W przypadku, gdy wybrany jest adres serwera znacznika czasu inny niż Certum SHA-256, w trakcie próby wykonania podpisu lub weryfikacji podpisu, aplikacja wyświetla ostrzeżenia o potencjalnym użyciu znacznika czasu stosującego algorytm SHA-1.



Rysunek 14: Zakładka Ustawienia – Znacznik czasu – ostrzeżenie o znaczniku czasu SHA-1

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.

4.3. 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.

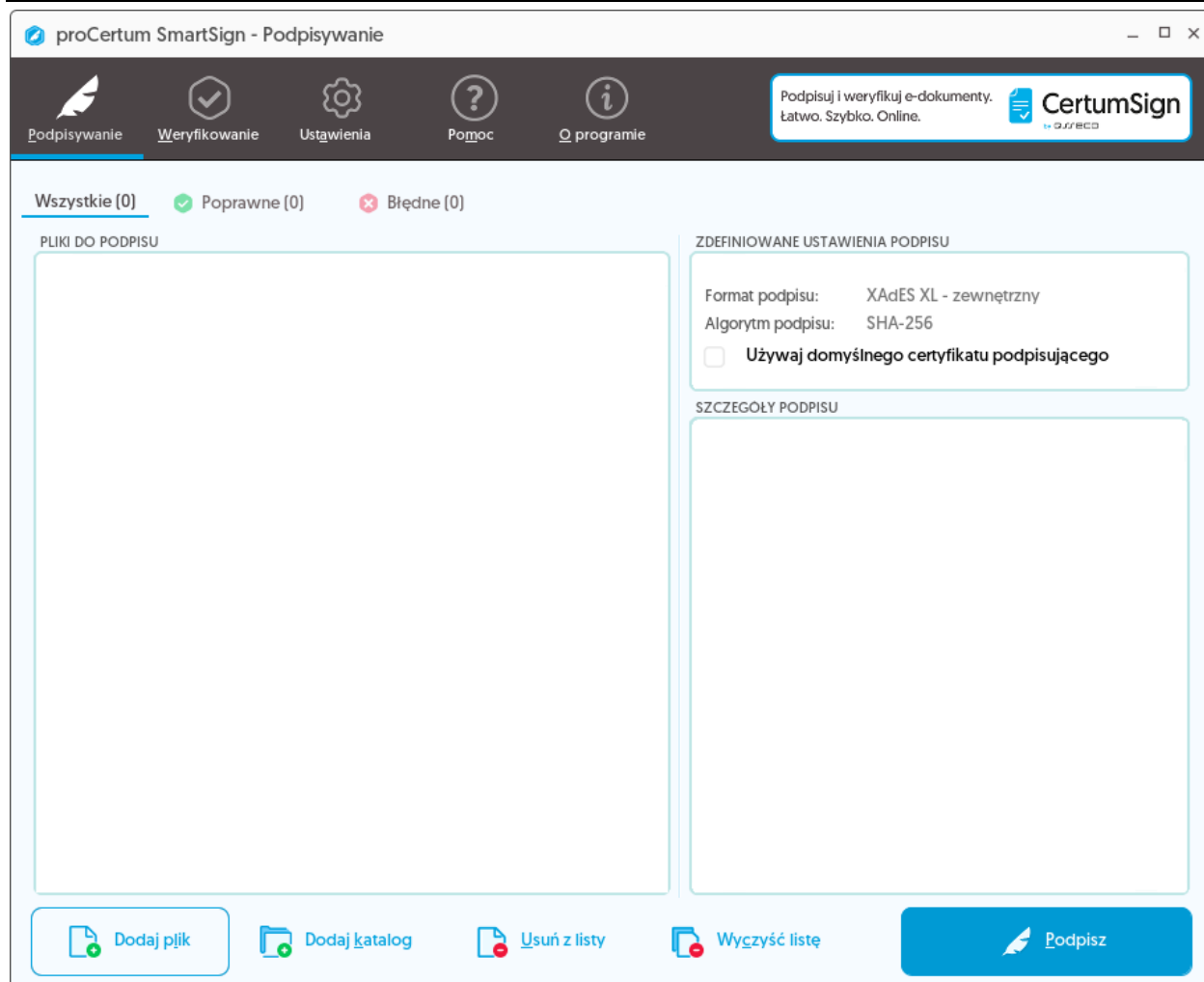
Niezależnie od posiadanej wersji oprogramowania jedyną rekomendowaną funkcją skrótu jest funkcja skrótu SHA2.

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

- **lista elementów do podpisania** – 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 15: Zakładka Podpisywanie

4.3.1. Dodawanie elementów do listy

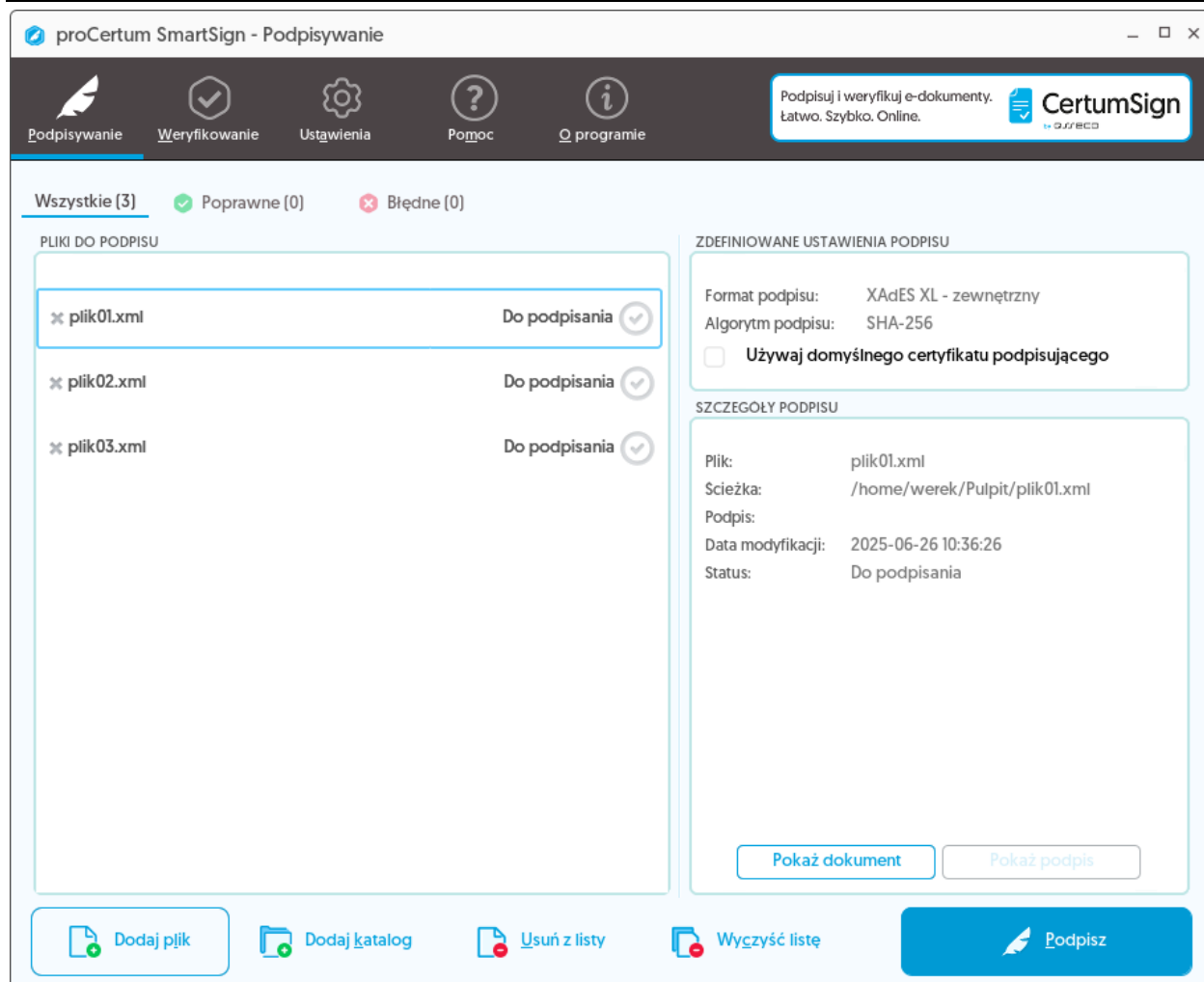
Operację podpisu elektronicznego można wykonać na dwa sposoby:

- 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**.

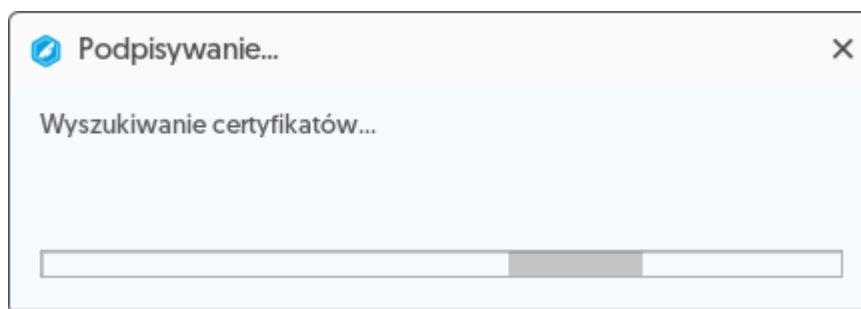
4.3.2. Operacja podpisu

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



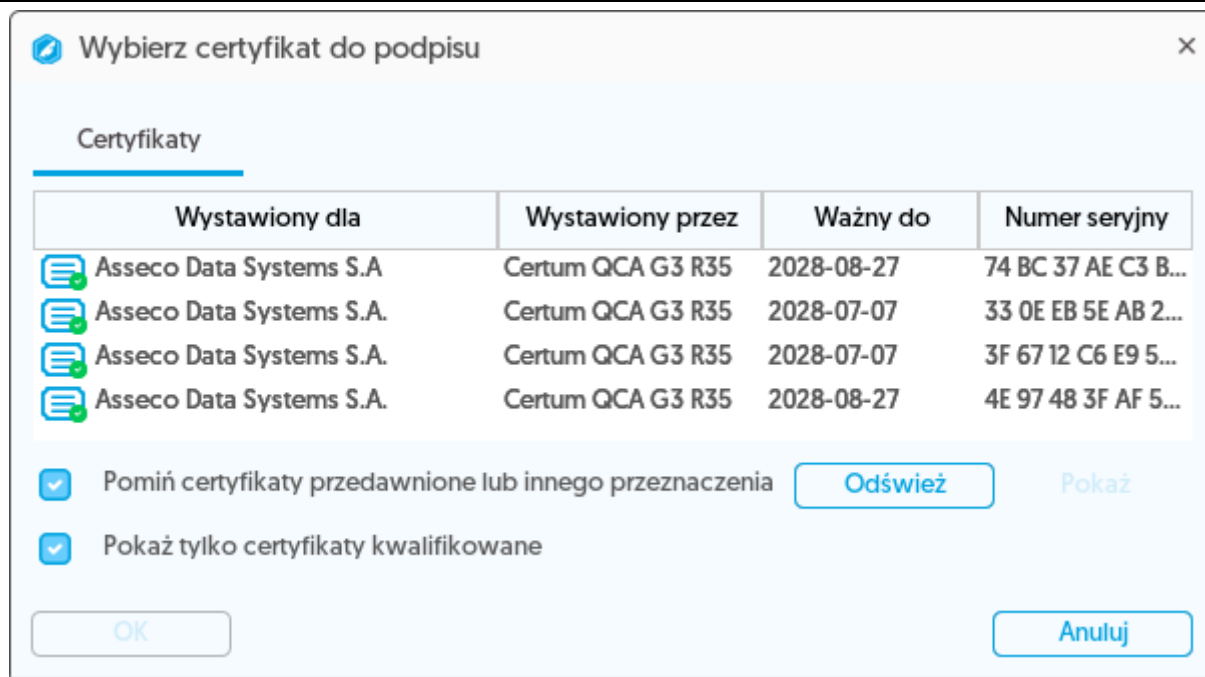
Rysunek 16: Zakładka Podpisywanie – Lista elementów do podpisania

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



Rysunek 17: Wyszukiwanie certyfikatów

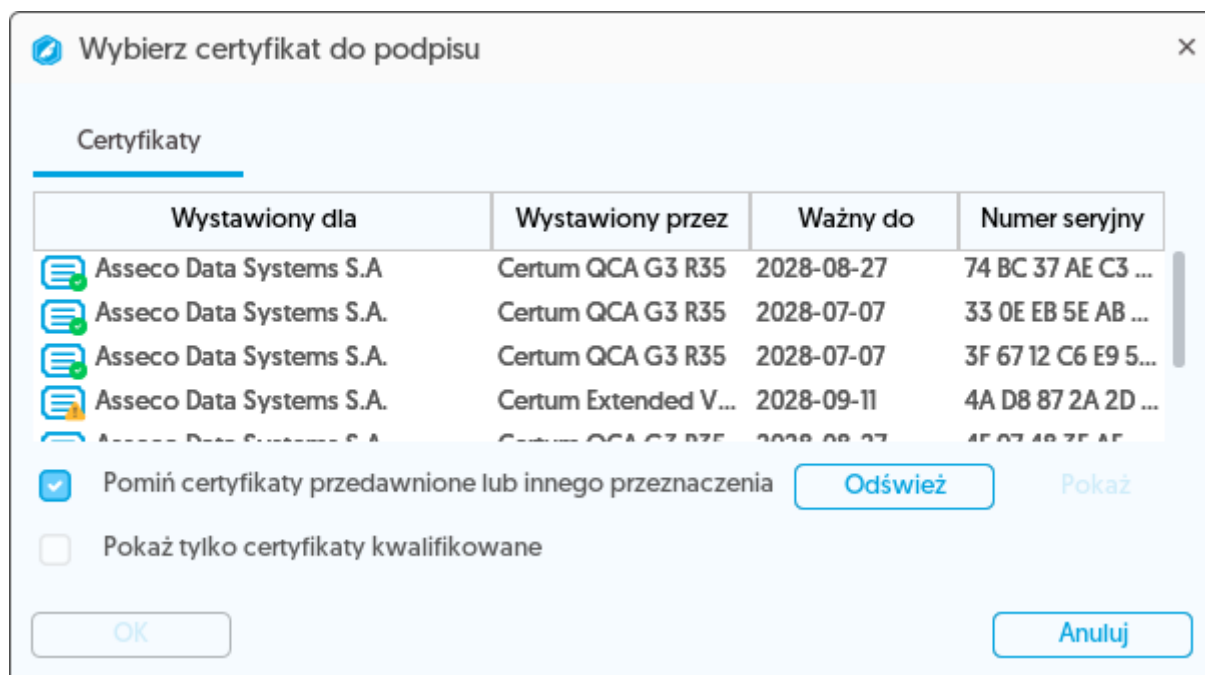
Po zakończeniu wyszukiwania zostaną wyświetlone certyfikaty. W przypadku gdy została zaznaczona opcja **Używaj domyślnego certyfikatu podpisującego** krok wyboru certyfikatów zostanie pominięty.



Rysunek 18: Lista certyfikatów kwalifikowanych

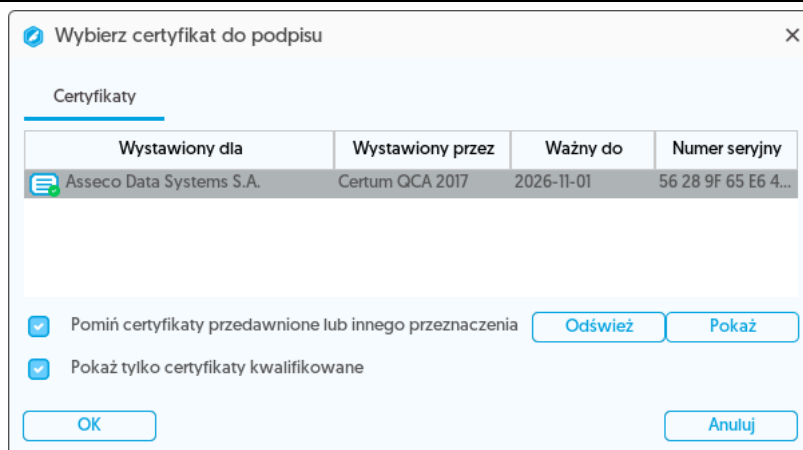
Uwaga!

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



Rysunek 19: Lista certyfikatów kwalifikowanych i niekwalifikowanych

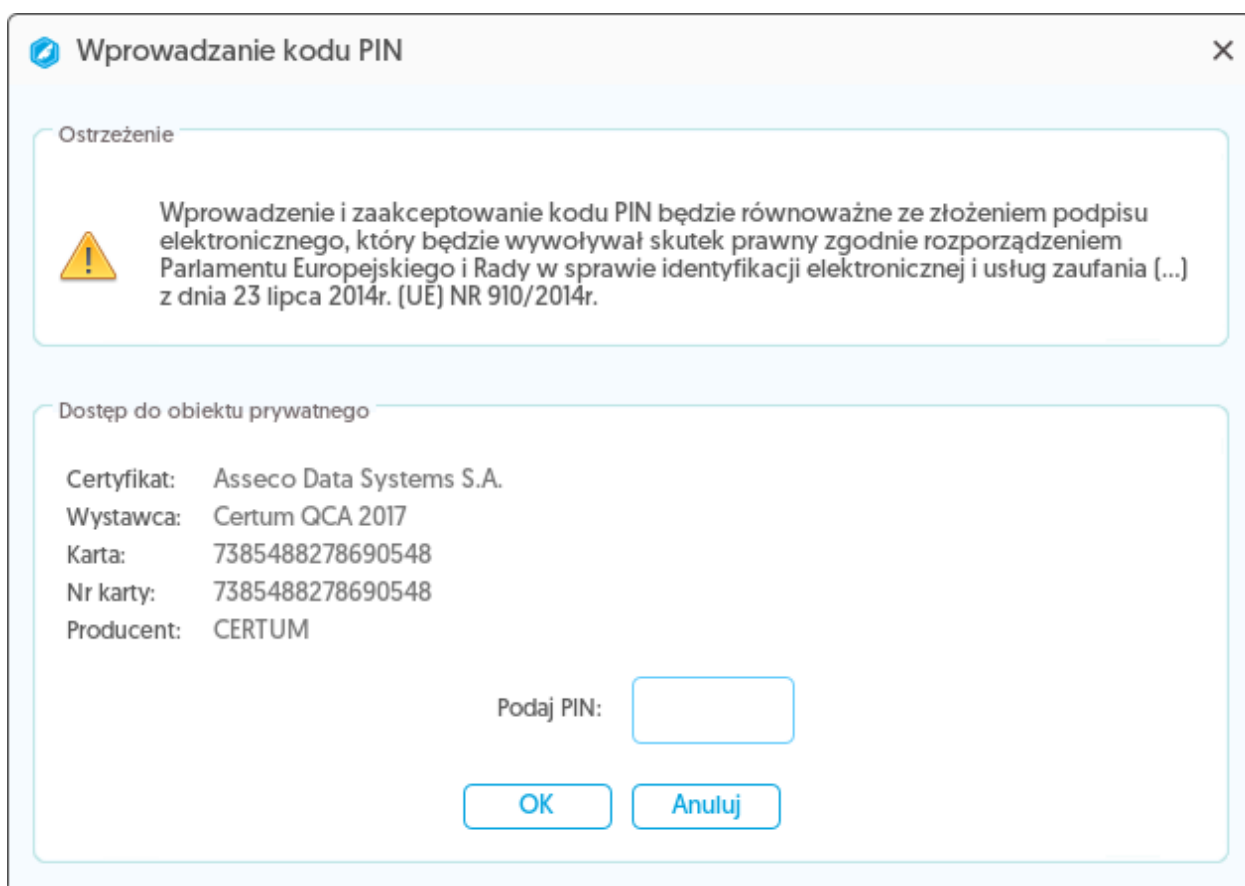
Należy wskazać certyfikat dla wykonania operacji podpisu i nacisnąć przycisk **OK**.



Rysunek 20: Wybór certyfikatu dla operacji podpisu

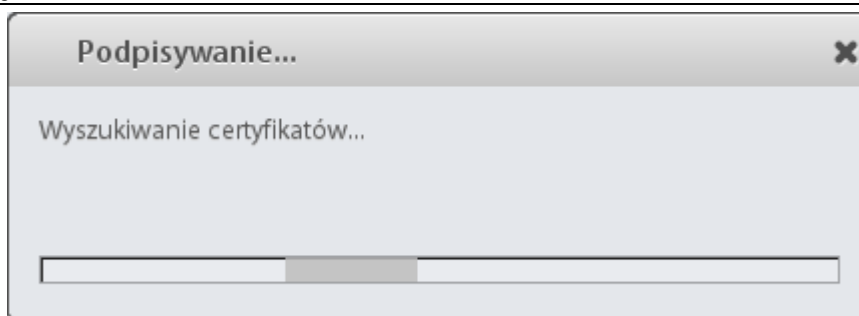
Jeżeli użytkownik dla operacji podpisu cyfrowego wybrał certyfikat kwalifikowany to wyświetlona zostanie prośba o wprowadzenie kodu uwierzytelniającego PIN. Należy wprowadzić PIN i nacisnąć przycisk **OK**.

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).

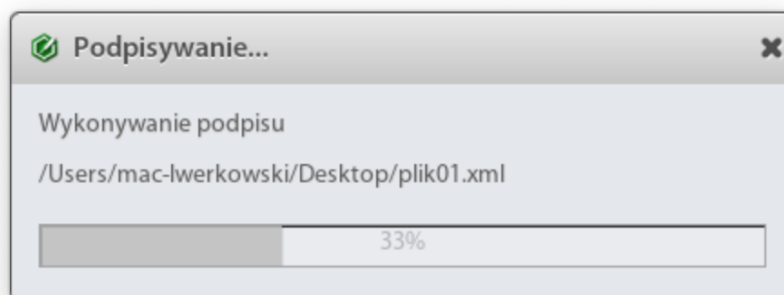


Rysunek 21: Prośba o wprowadzenie kodu PIN

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

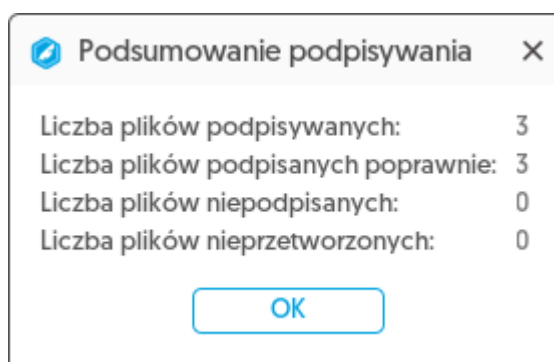


Rysunek 22: Podpisywanie... - Wyszukiwanie kluczy



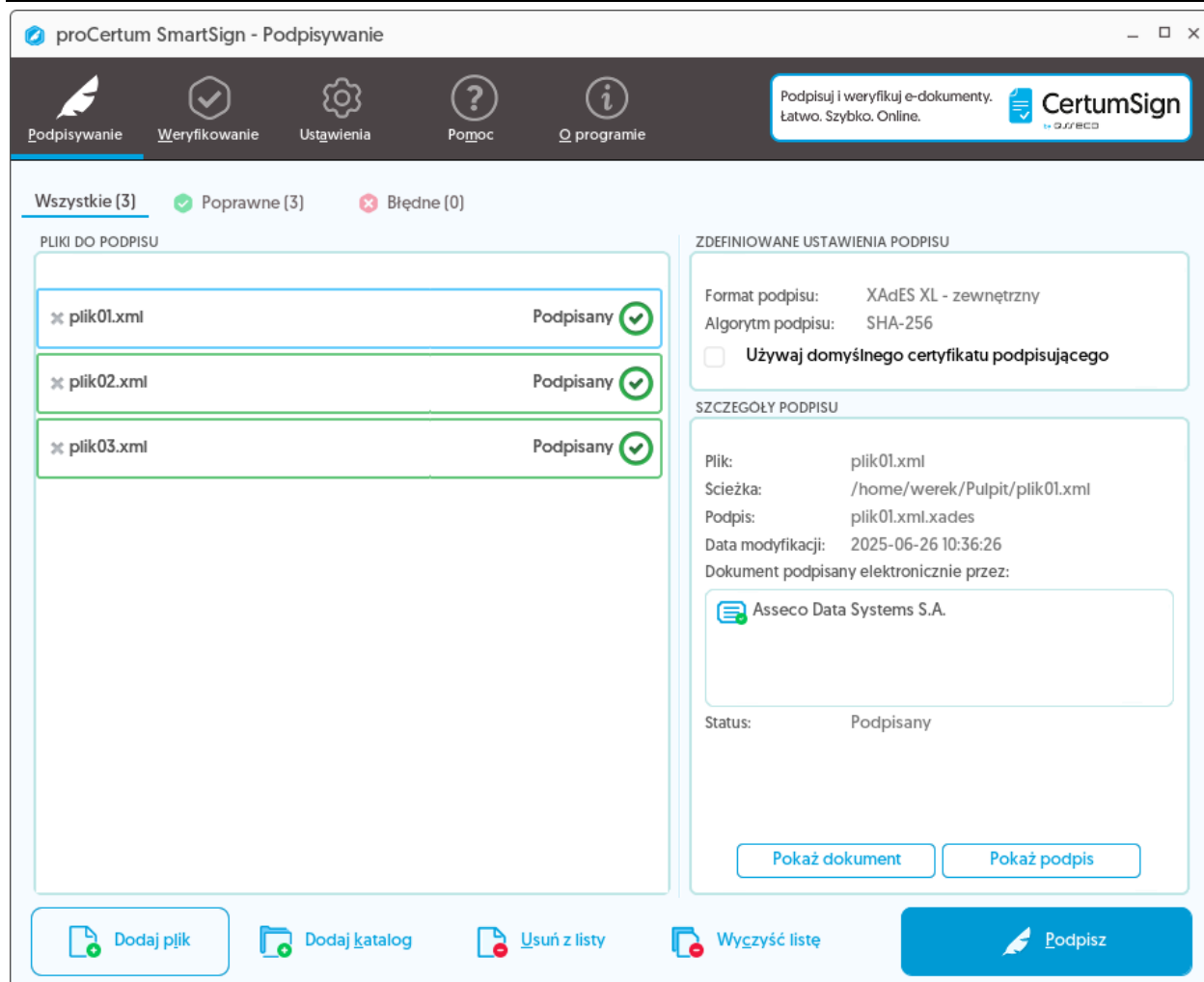
Rysunek 23: Podpisywanie... - Wykonywanie podpisu

Po zakończeniu procesu składania podpisu elektronicznego zostanie wyświetlone podsumowanie.



Rysunek 24: Podsumowanie podpisywania

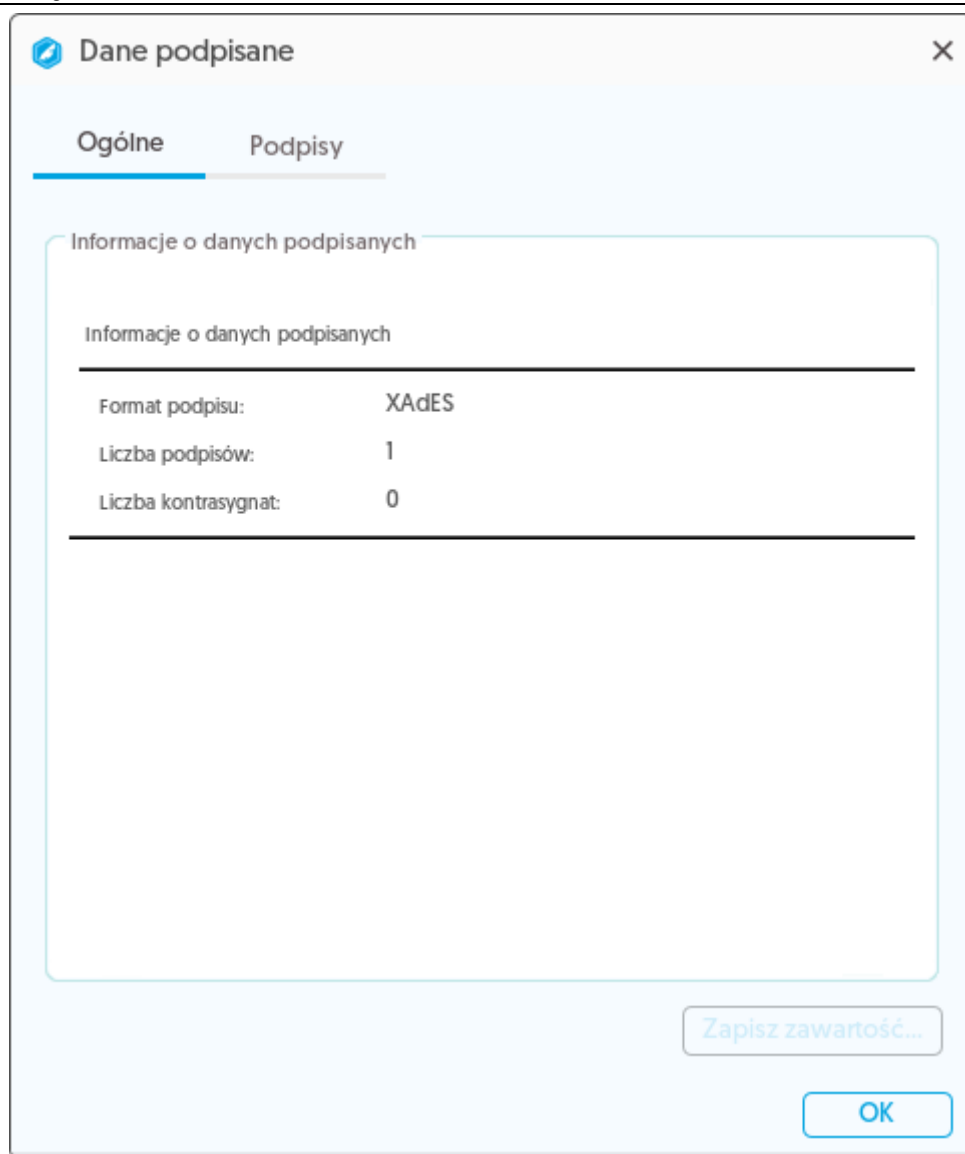
Sekcja **Szczegóły podpisu** na zakładce **Podpisywanie** zostanie uaktualniona o informacje dotyczące pliku podpisu oraz podpisującego (pole **Dokument podpisany przez**).



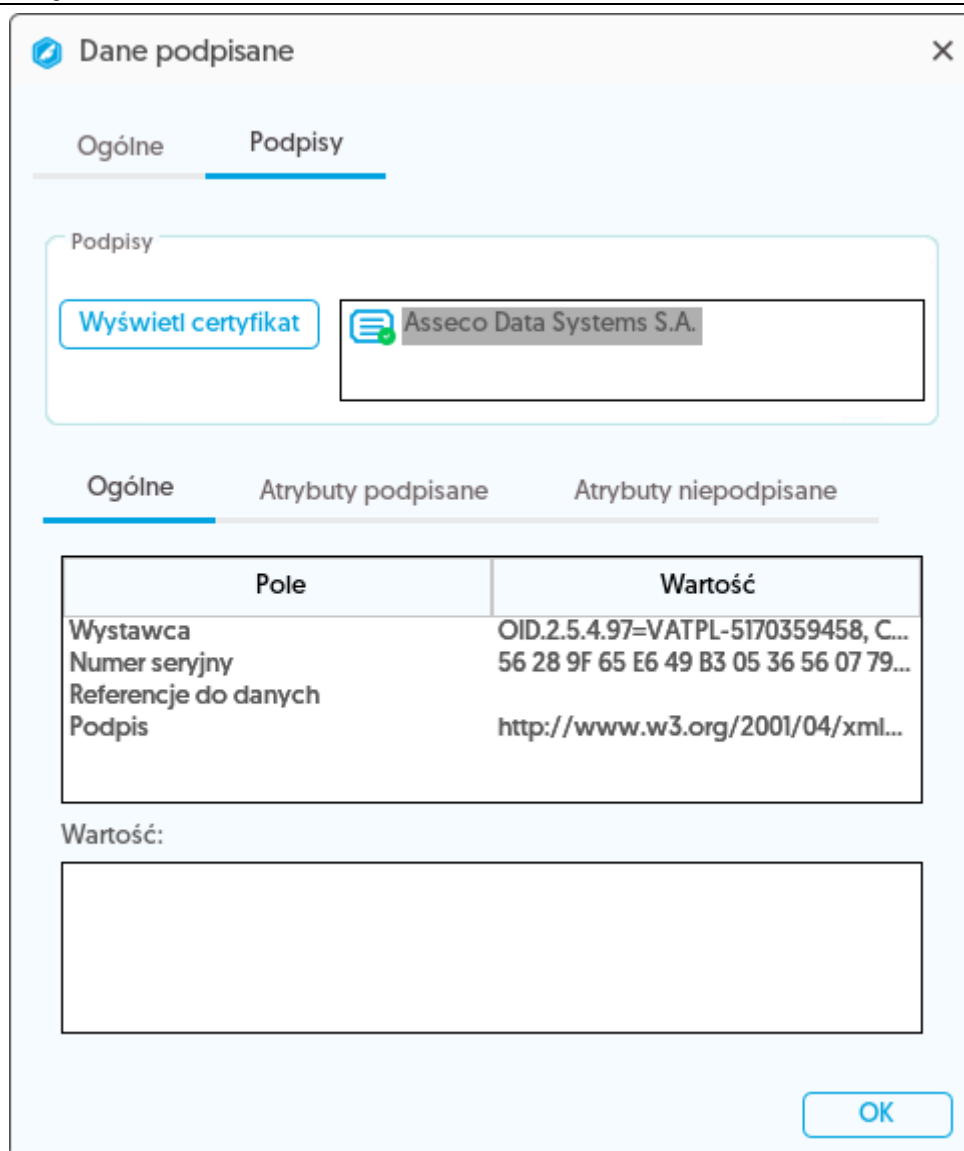
Rysunek 25: Zakładka Podpisywanie – wykonany podpis

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 26: Dane podpisane – zakładka ogólna



Rysunek 27: Dane podpisane - zakładka podpis

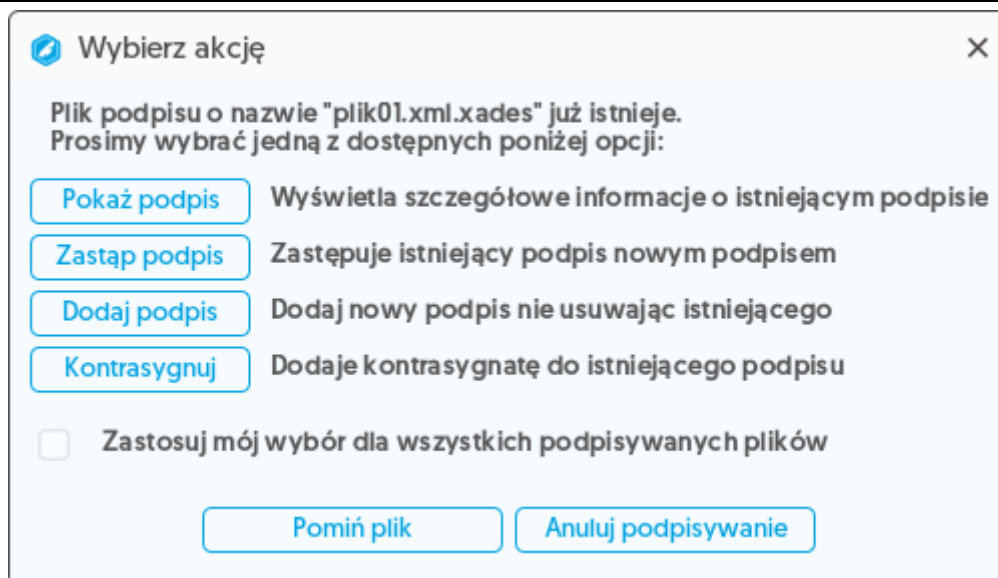
4.3.3. Podpis wielokrotny

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!!!

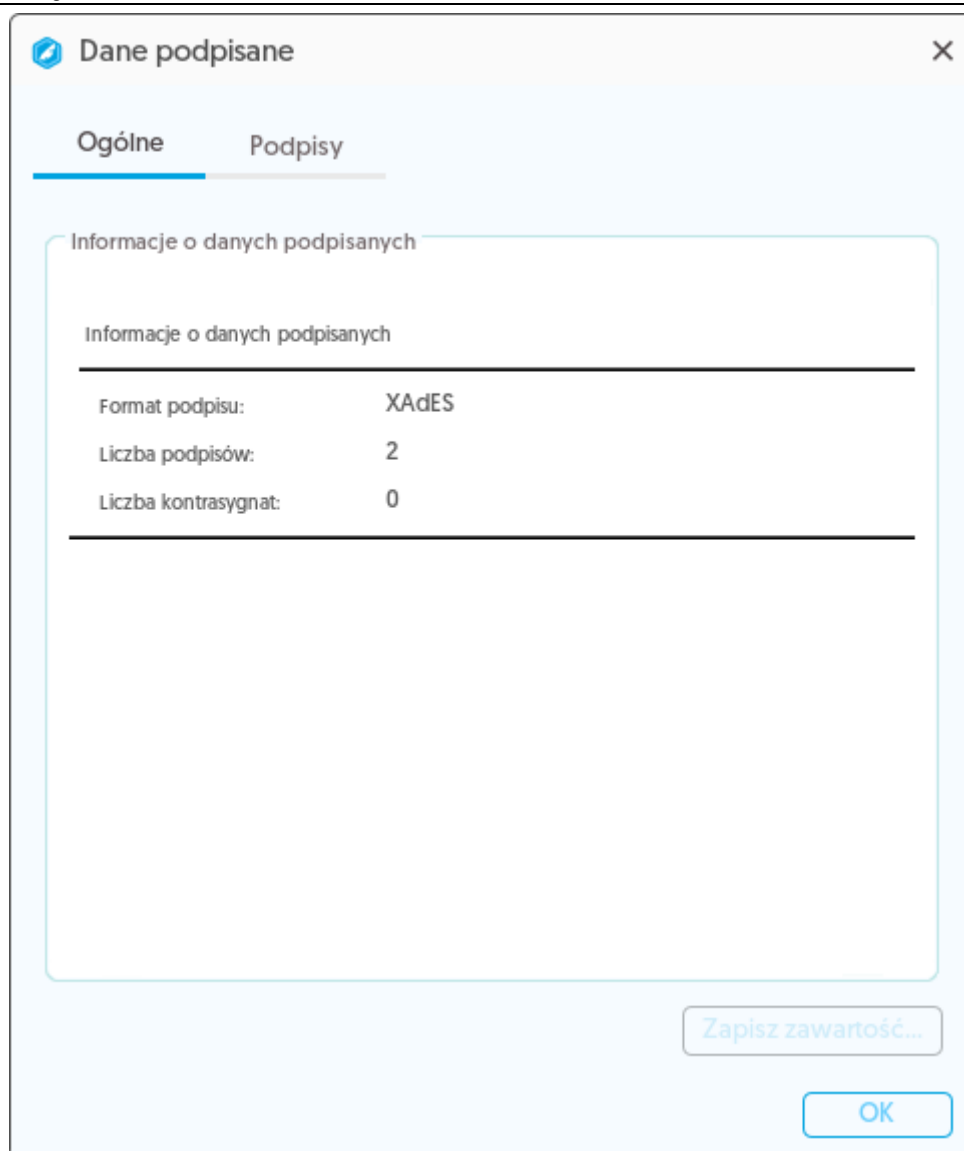
Przy tworzeniu podpisu wielokrotnych nie ma możliwości składania podpisów „mieszanych” tzn. aplikacja ignoruje wszelkie ustawienia dot. formatów podpisu i wykonuje podpis w takim trybie, w jakim złożony jest pierwszy podpis na dokumencie.

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

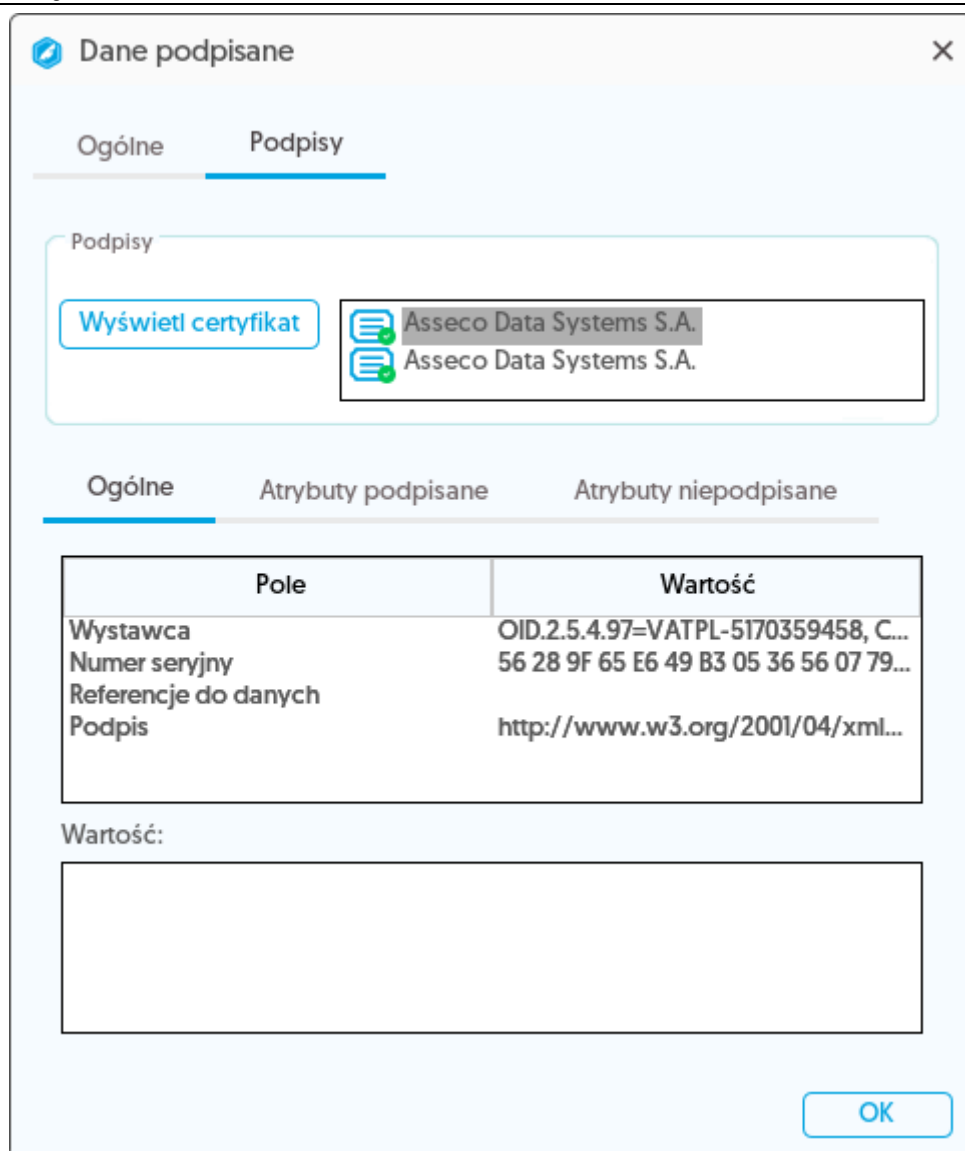


Rysunek 28: Okno wyboru akcji przy obecnym już co najmniej jednym podpisie

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 29: Dane podpisane - zakładka ogólna dla podpisu wielokrotnego

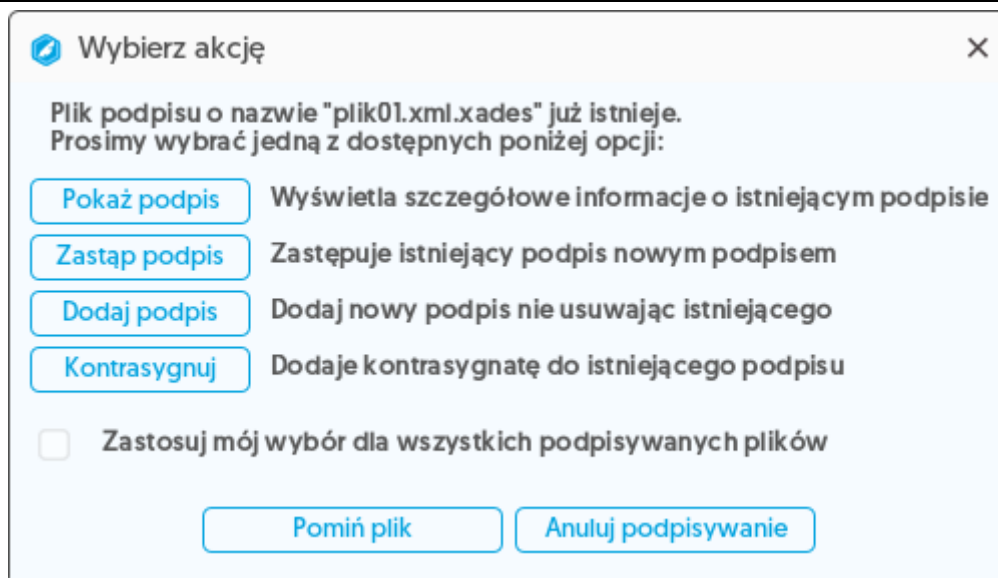


Rysunek 30: Dane podpisane - zakładka podpis dla podpisu wielokrotnego

4.3.4. Kontrasygndata

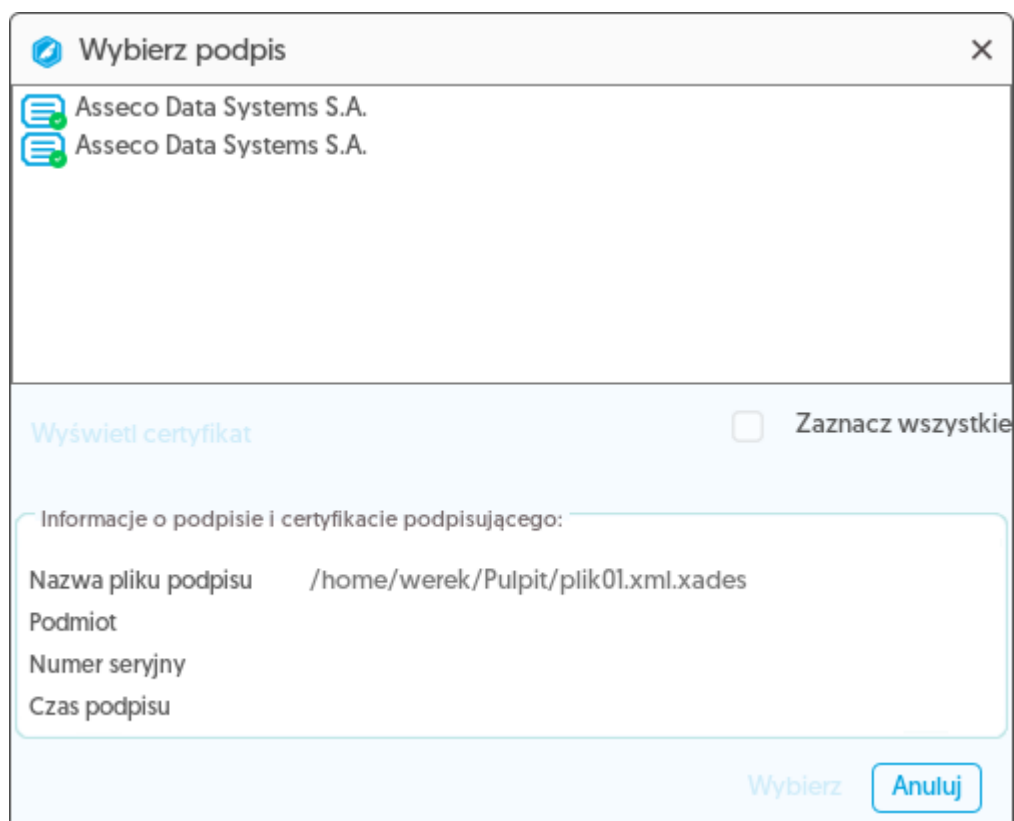
W celu wykonania **kontrasygnaty**, należy wybrać plik, który został już wcześniej podpisany. Wskazać można zarówno oryginalny plik, jak również plik podpisu. Domyślnie okno wyboru pliku pozwala wybierać wszystkie pliki, oprócz plików podpisu. Jeśli chcemy skorzystać z opcji wskazywania pliku podpisu, 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:



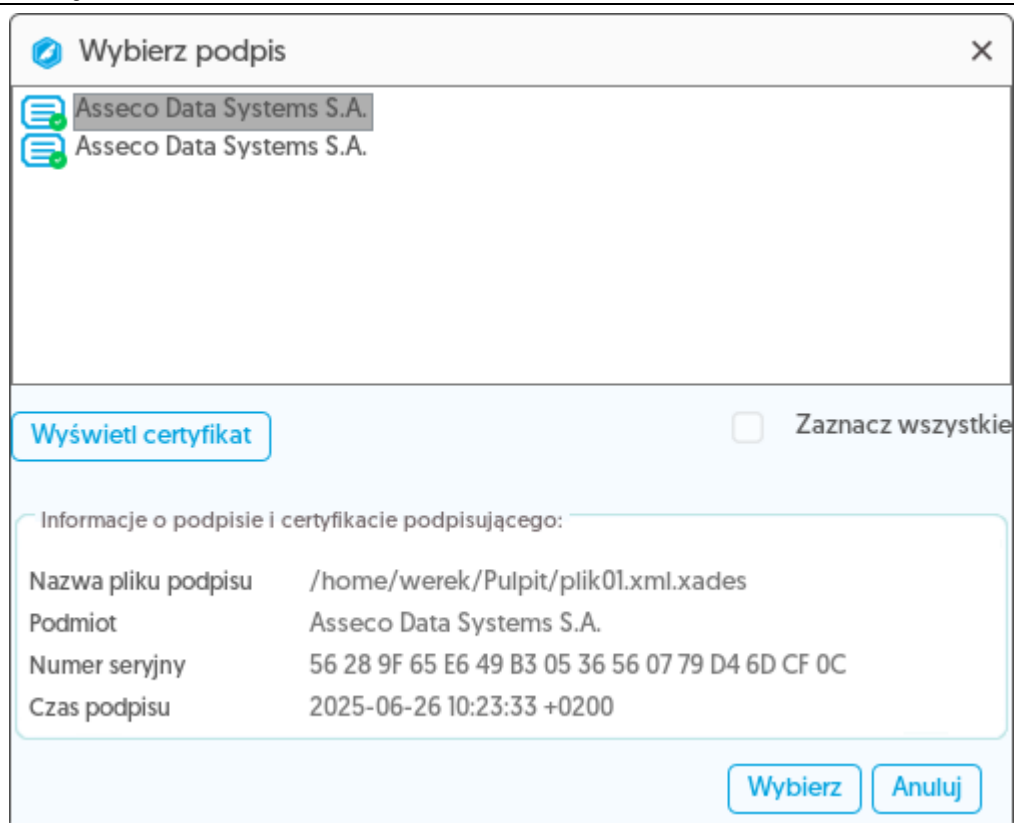
Rysunek 31: Okno wyboru akcji przy obecnym już co najmniej jednym podpisie

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:



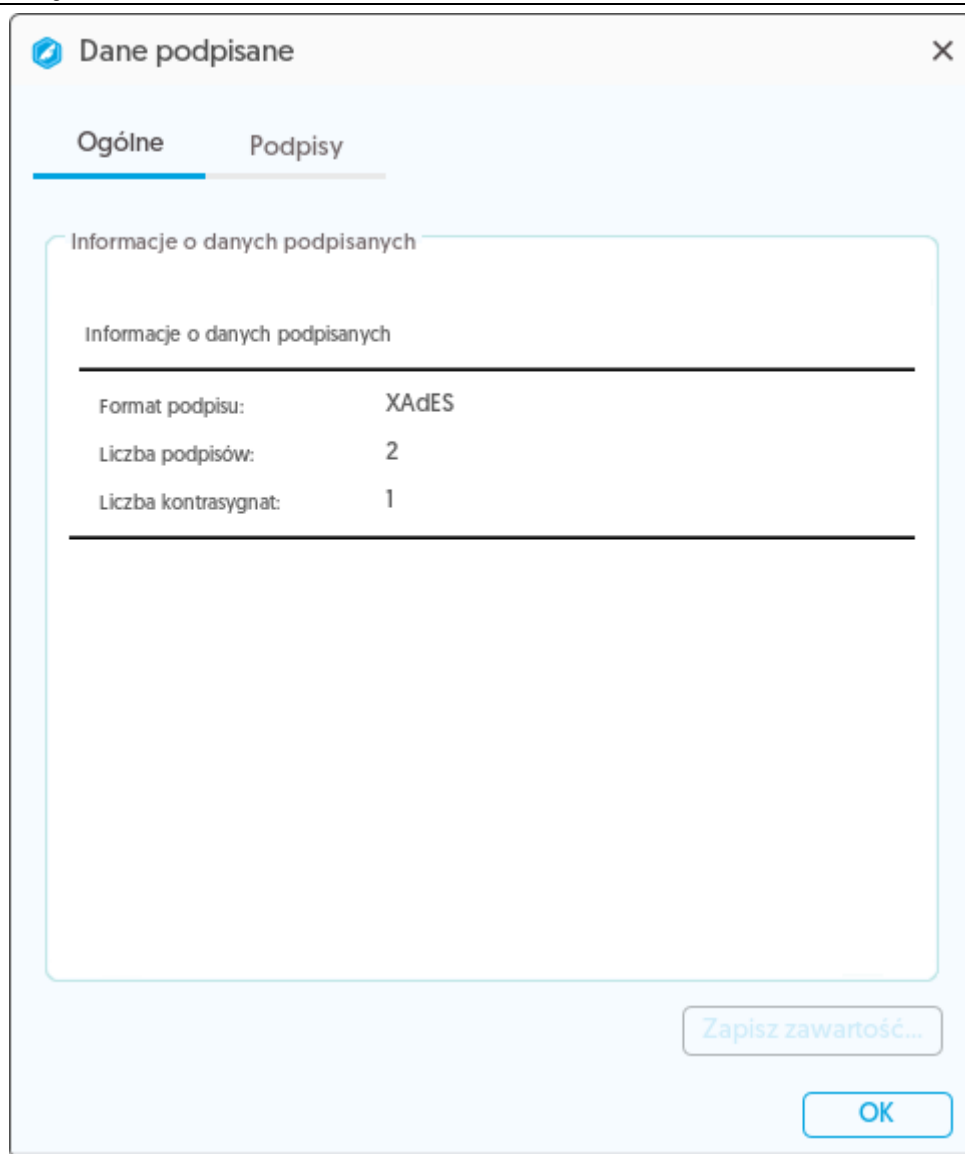
Rysunek 32: Okno wyboru podpisu, który chcemy kontrasygnować

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

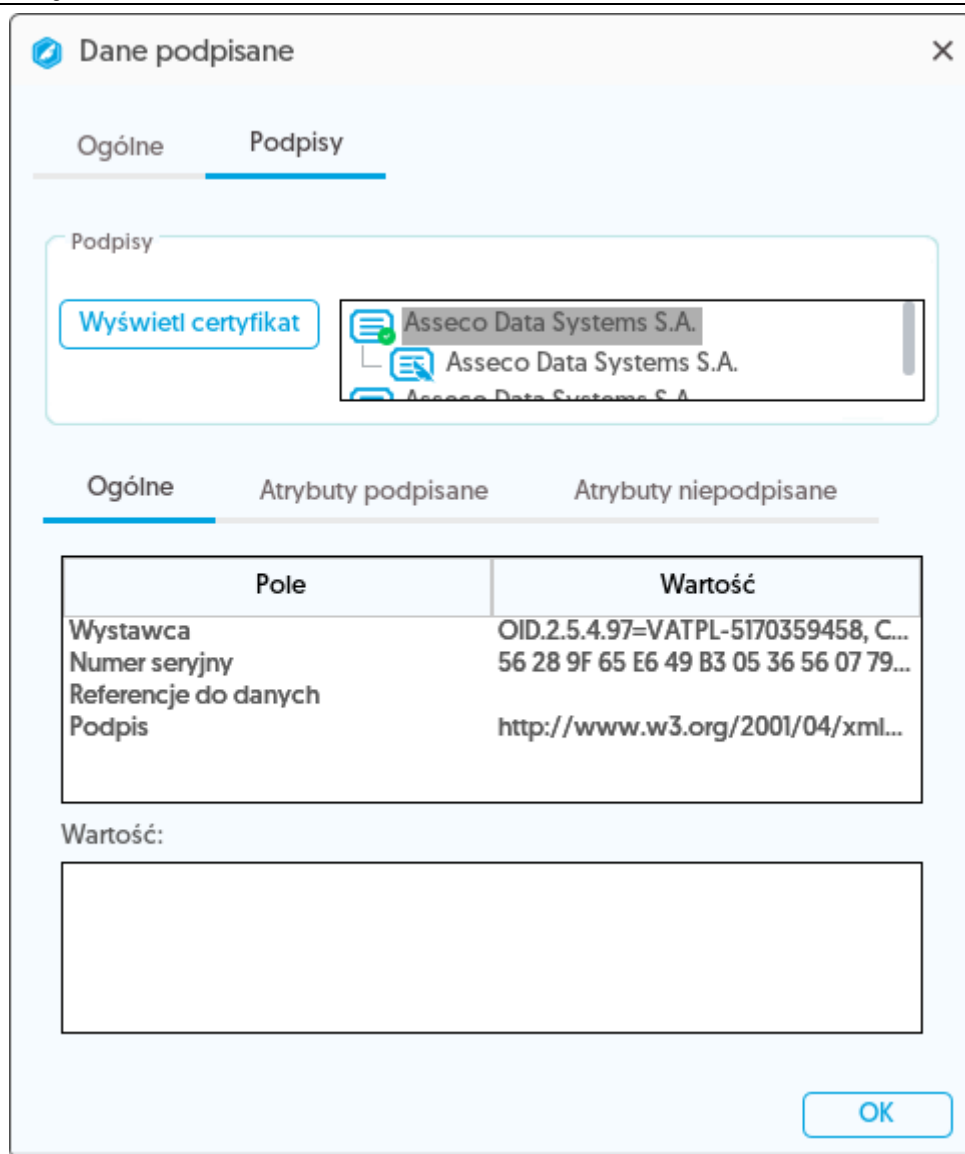


Rysunek 33: Okno wyboru podpisu, gdy wybrano wszystkie podpisy do kontrasygnowania

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



Rysunek 34 Dane podpisane - zakładka ogólna dla kontrasygnaty



Rysunek 35 Dane podpisane - zakładka podpis dla kontrasygnaty

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

4.3.5. 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.

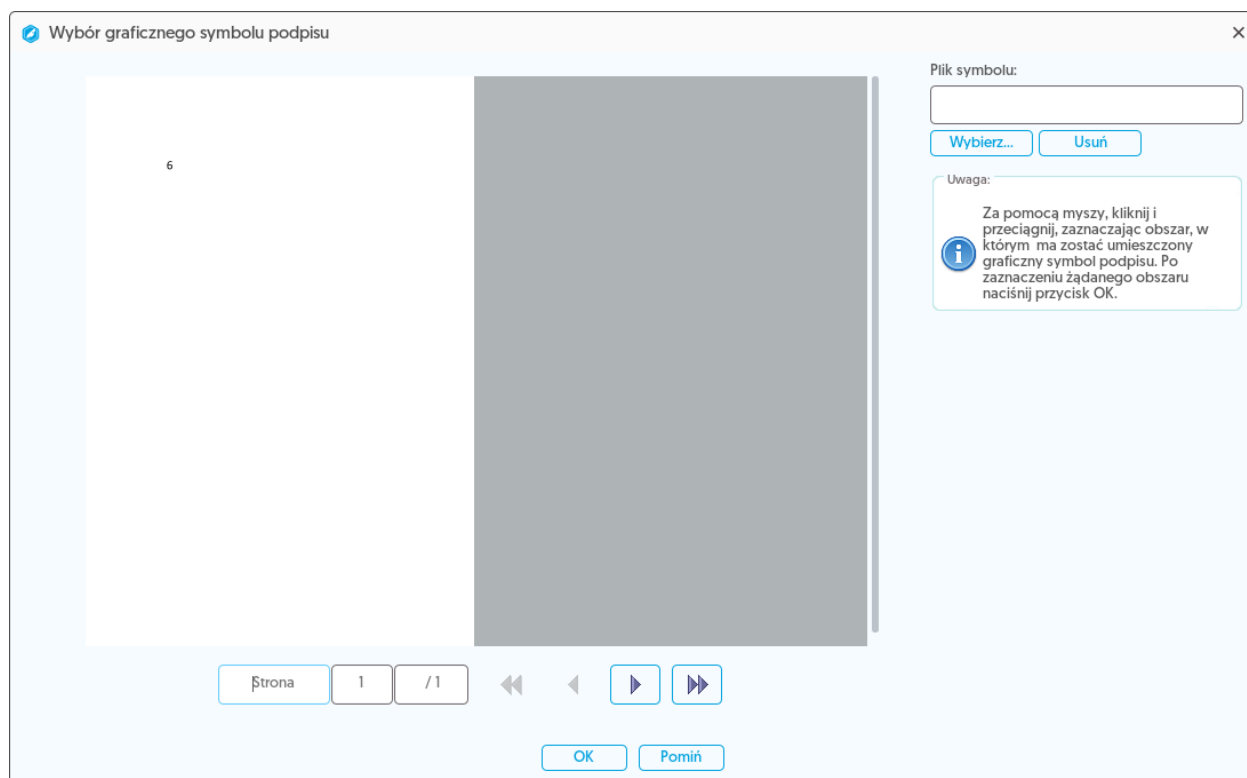
UWAGA!!!

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

4.3.5.1. Dodawanie graficznego symbolu podpisu

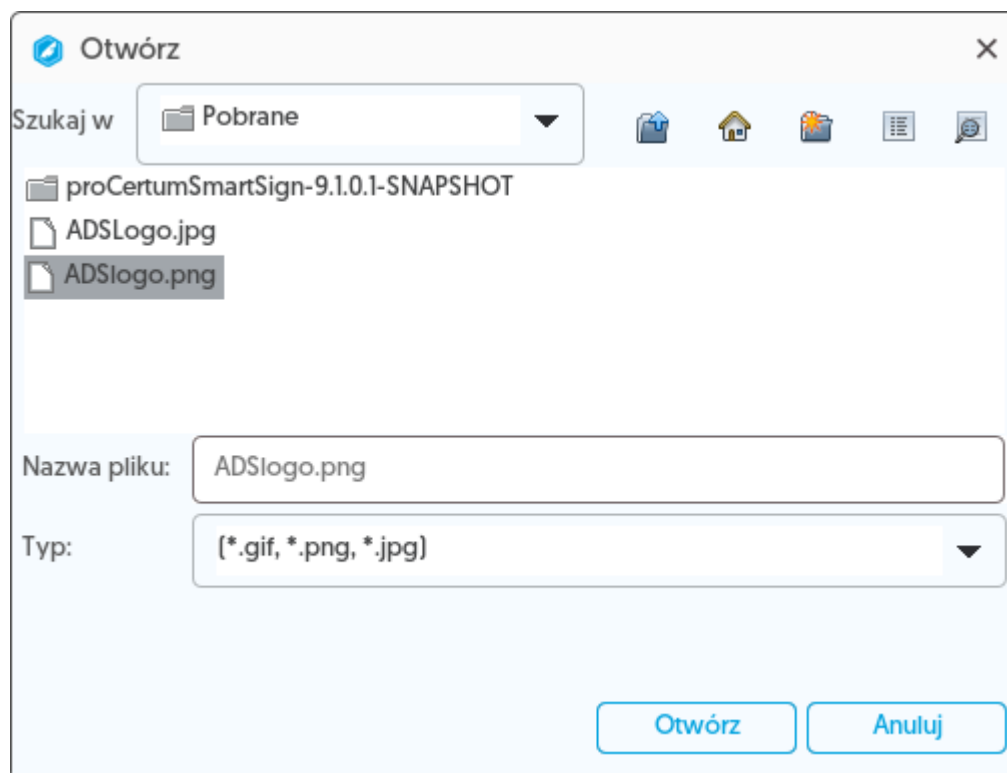
Jeśli w zaawansowanych opcjach podpisu PDF/PAdES zaznaczona jest opcja **Umieszczaj graficzny symbol podpisu w dokumencie PDF** to w trakcie podpisywania plików PDF, po wybraniu certyfikatu podpisującego umożliwiające zostanie wybranie pliku graficznego symbolu podpisu. W przypadku seryjnego podpisywania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

definiowanie osobnego symbolu.



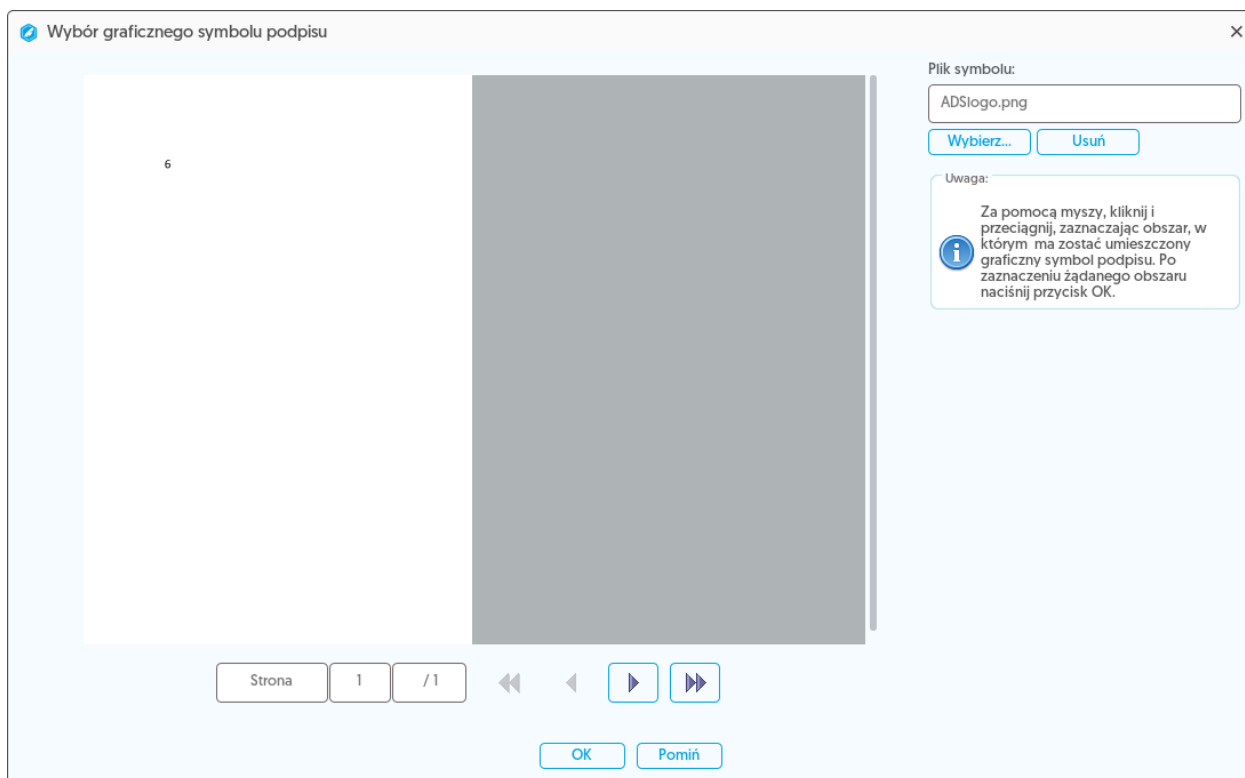
Rysunek 36 Dodawanie graficznego symbolu podpisu – okno główne

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



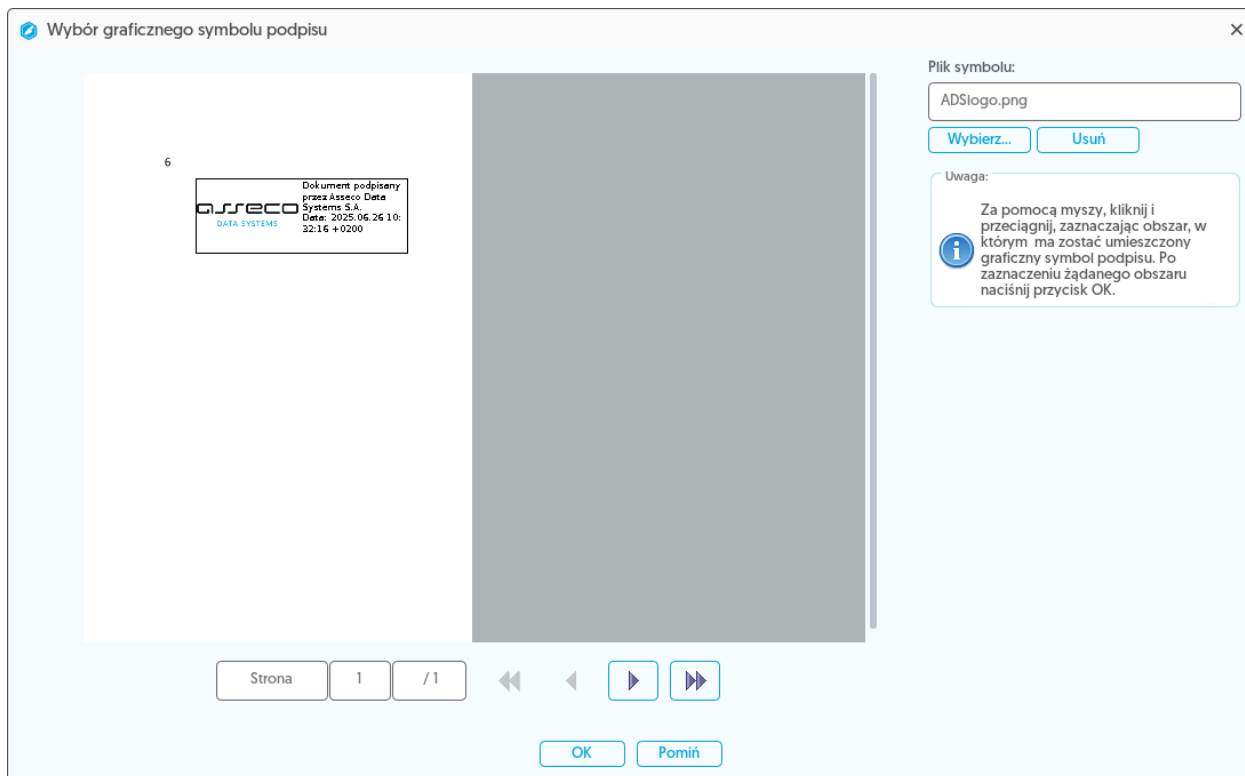
Rysunek 37 Dodawanie graficznego symbolu podpisu – wskazanie pliku graficznego

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



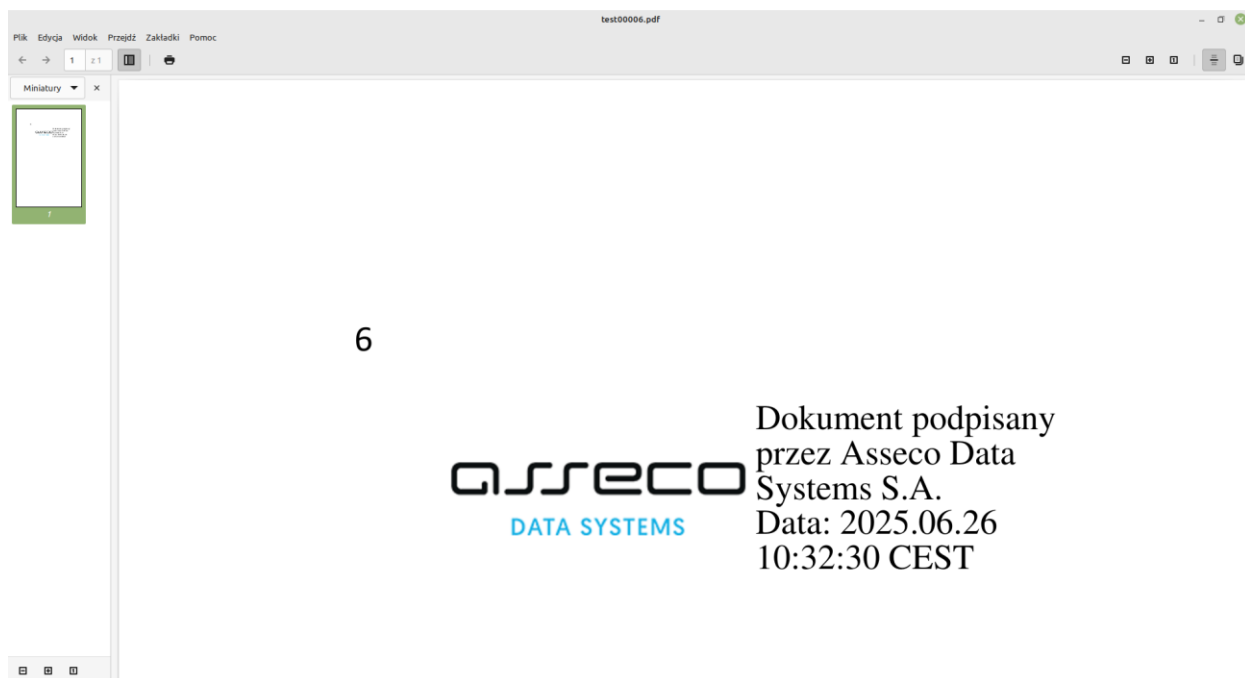
Rysunek 38 Dodawanie graficznego symbolu podpisu – wybrany plik graficzny

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 39 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 40 Dodawanie graficznego symbolu podpisu – podpisany plik z umieszczonym graficznym symbolem podpisu

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

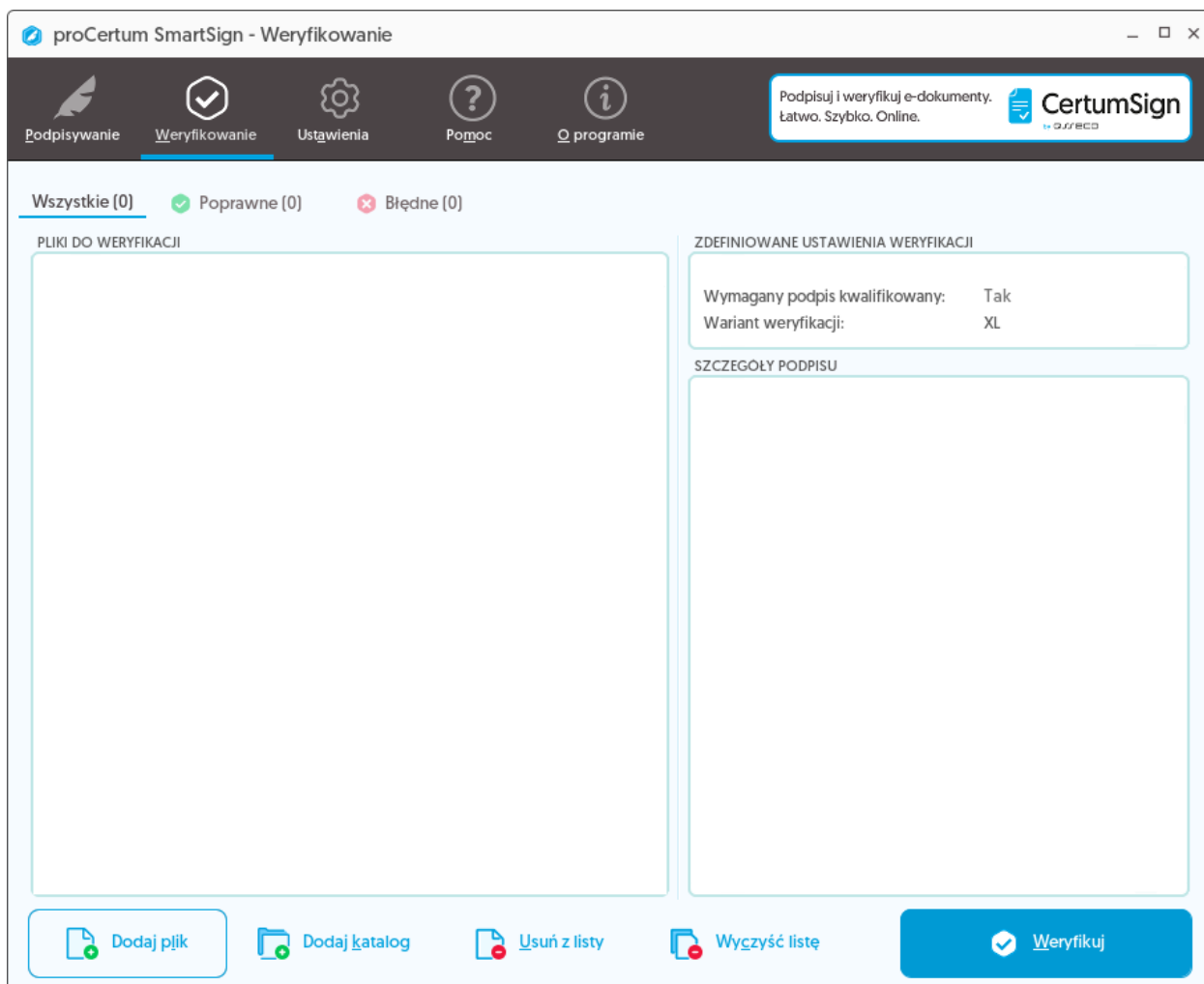


Rysunek 41 Dodawanie graficznego symbolu podpisu – podpisywanie wielu plików

4.4. Weryfikowanie podpisów

Zakładka **Weryfikowanie** umożliwia weryfikację podpisu elektronicznego. Składają 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 42: Zakładka Weryfikowanie

4.4.1. Dodawanie elementów do listy

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

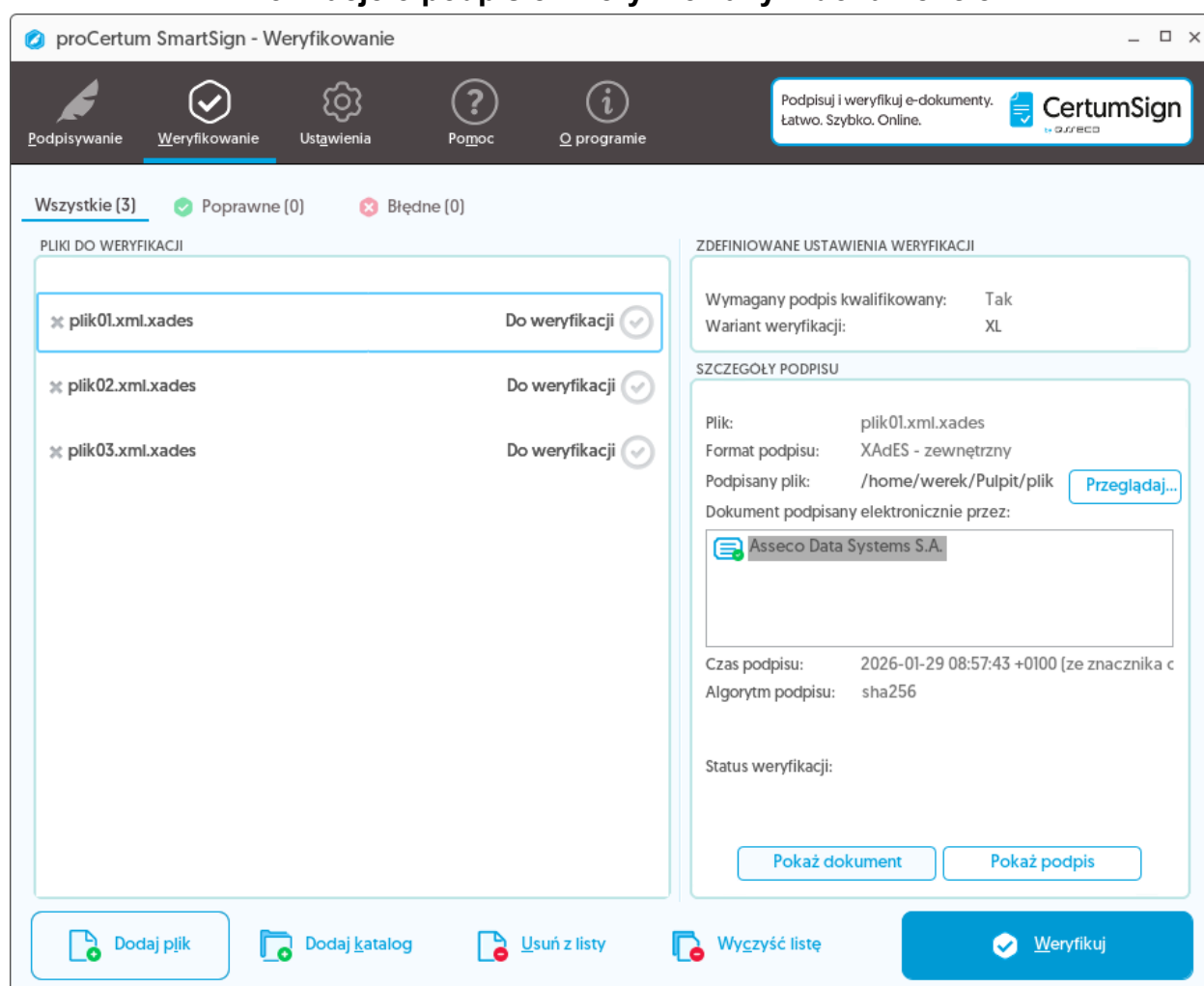
- na pojedynczym pliku – poprzez wskazanie pliku za pomocą przycisku **Dodaj plik**,
- na grupie plików – poprzez wielokrotny wybór plików za pomocą przycisku **Dodaj plik** lub poprzez dodanie katalogu za pomocą przycisku **Dodaj katalog**.

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!

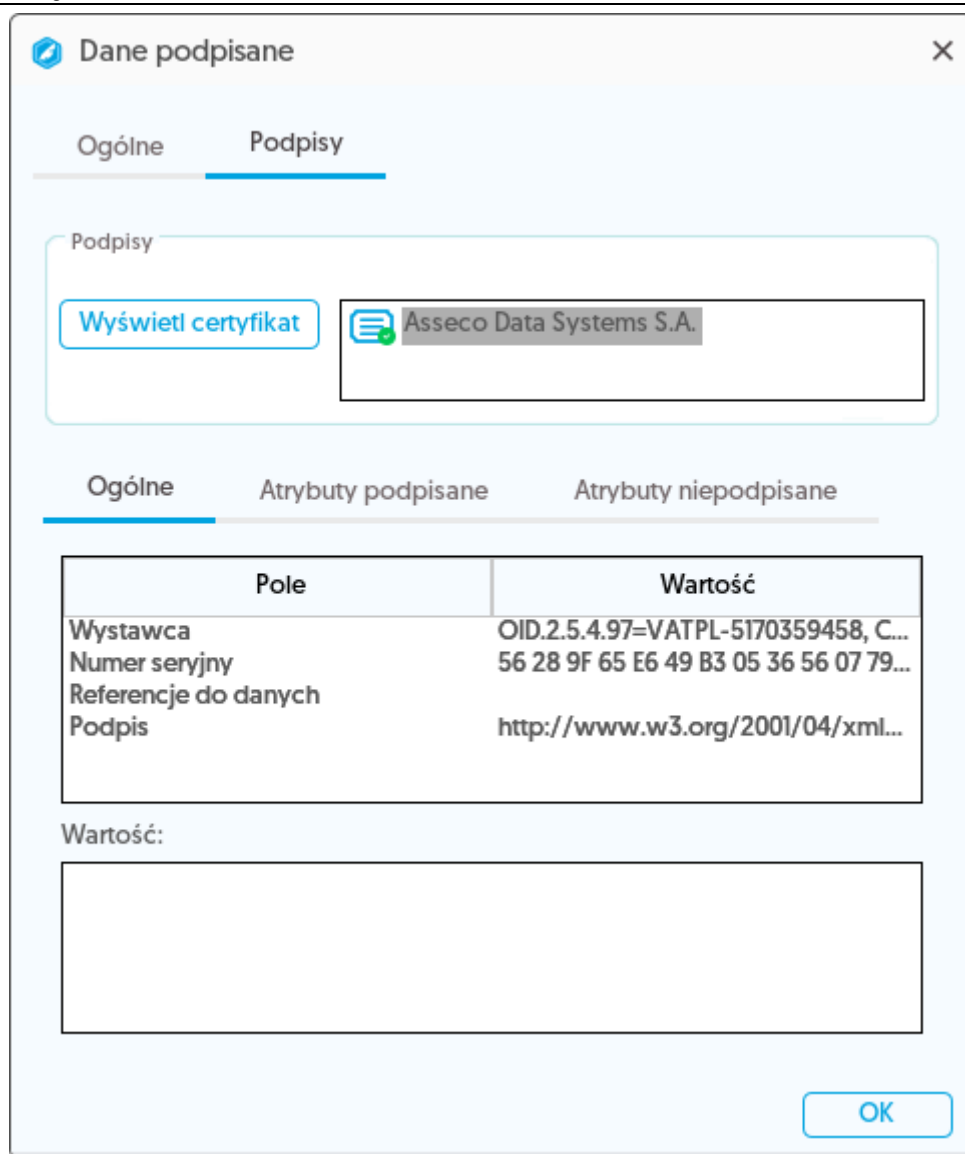
Na liście elementów do weryfikacji mogą figurować pliki z wewnętrznym bądź zewnętrznym podpisem (informacja o typie podpisu znajduje się w sekcji **Szczegóły podpisu**). Jeżeli wybrany element jest podpisem zewnętrznym i program nie odnalazł pliku podpisanego w katalogu pliku podpisu, to w sekcji **Szczegóły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

4.4.2. Informacje o podpisie i weryfikowanym dokumencie



Rysunek 43: Zakładka Weryfikowanie – Lista elementów do weryfikacji

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



Rysunek 44: 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.;

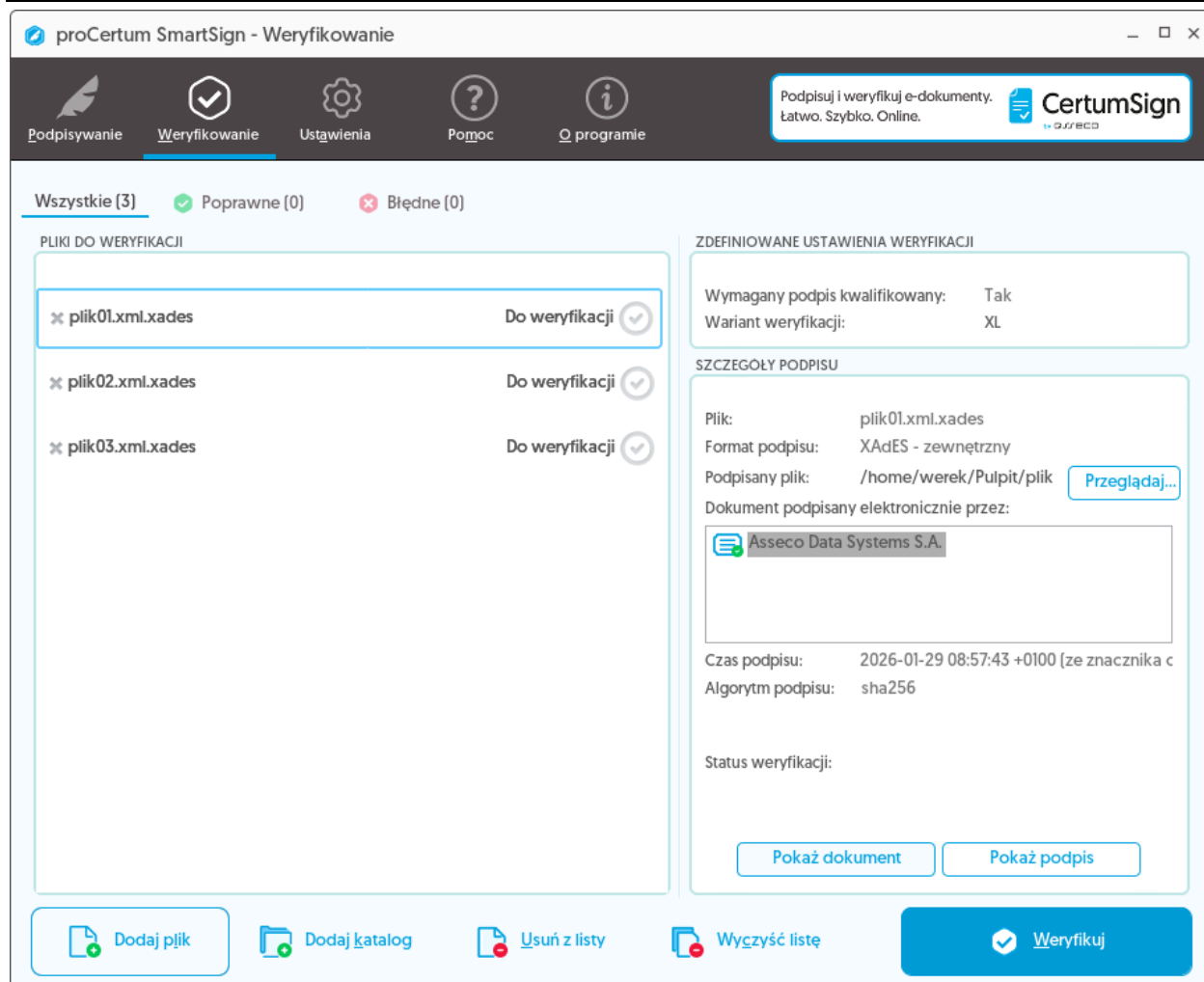
Aby wyświetlić weryfikowany dokument należy nacisnąć przycisk **Pokaż dokument**.

Uwaga!

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

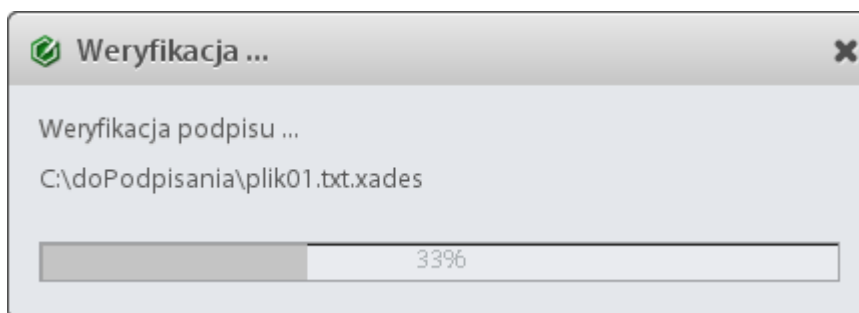
4.4.3. Operacja weryfikacji

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



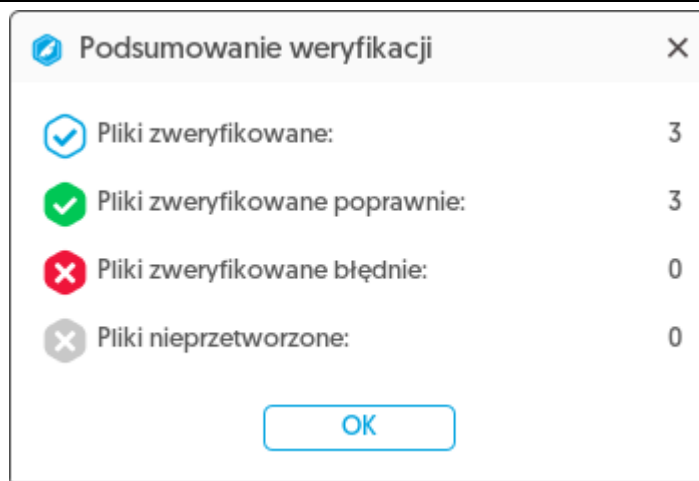
Rysunek 45: Zakładka Weryfikowanie – Lista elementów do weryfikacji

Rozpocznie się proces weryfikacji podpisu.



Rysunek 46: Weryfikacja...

Po zakończeniu procesu weryfikacji podpisu elektronicznego zostanie wyświetlone podsumowanie.



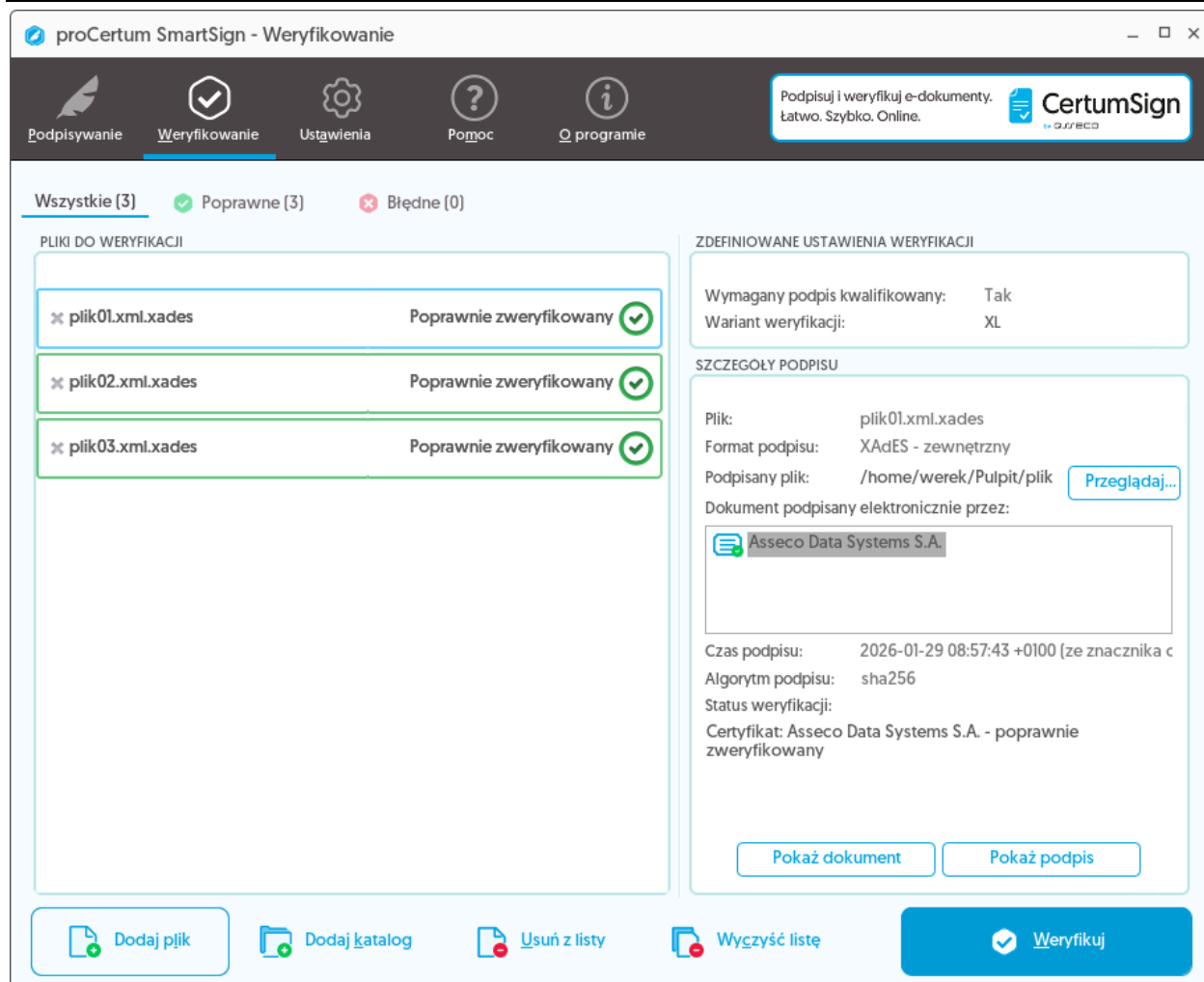
Rysunek 47: Podsumowanie weryfikacji

4.4.4. Status weryfikacji

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

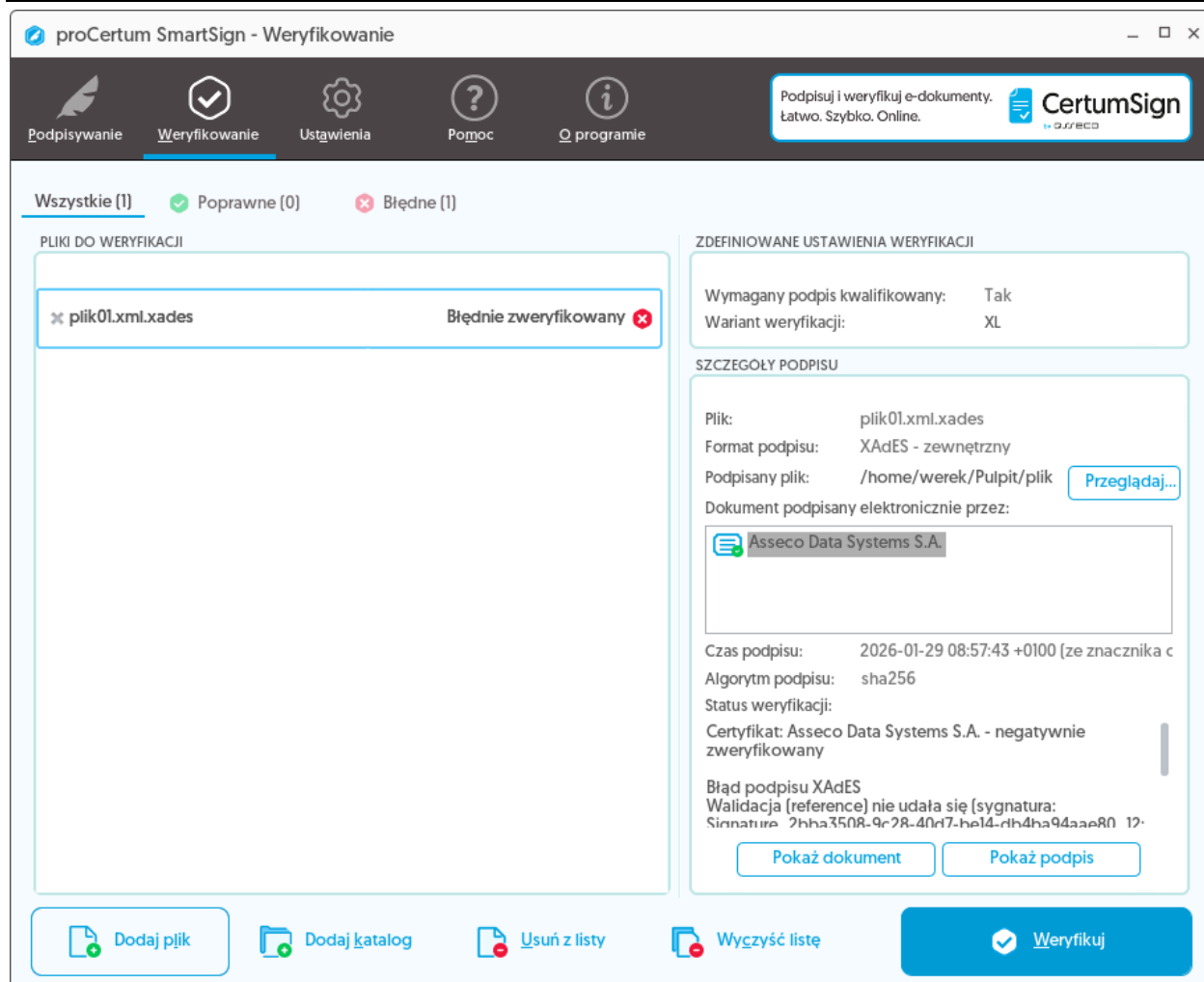
- **Poprawnie zweryfikowany;**
- **Błędnie zweryfikowany.**

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



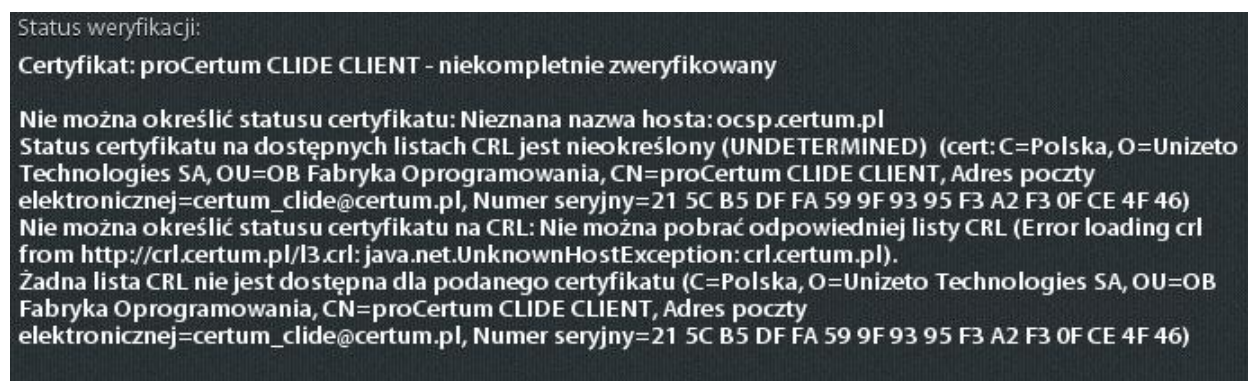
Rysunek 48: Status weryfikacji: Poprawnie zweryfikowany

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 49: 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 50: 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 51: Nieprawidłowa wartość podpisu

Status weryfikacji:
Certyfikat: MARUA - negatywnie zweryfikowany
Nie znaleziono certyfikatu (CN=LEVEL, OU=LEVEL, O=LEVEL,
L=Szczecin, ST=Zachodniopomorskie, C=PL)

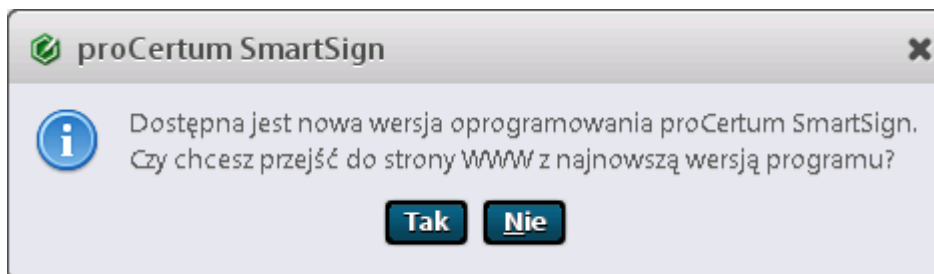
Rysunek 52: Nieprawidłowy certyfikat

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 53: Błąd przy weryfikacji certyfikatu niekwalifikowanego

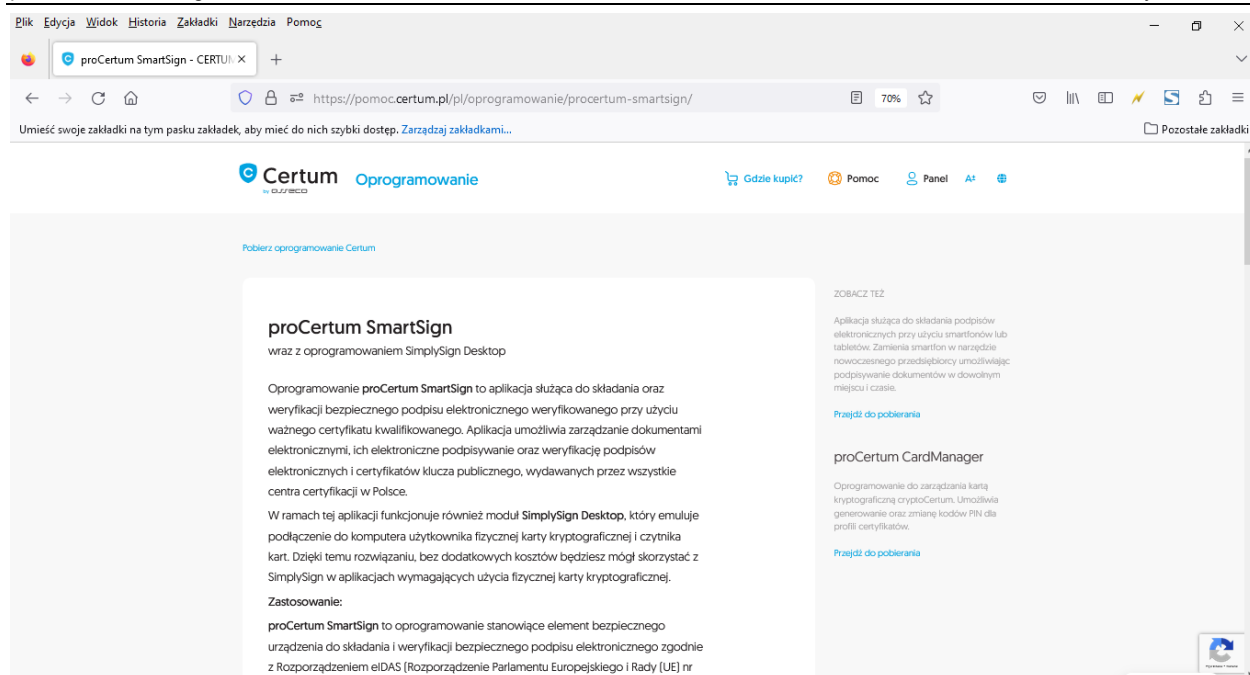
4.5. Powiadamianie o aktualizacji.

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 54: 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 55: Strona WWW z nową wersją proCertum SmartSign**

5. Spis rysunków

Rysunek 1: Okno główne aplikacji proCertum SmartSign	7
Rysunek 2: Informacje o systemie– Zakładka Środowisko Java	8
Rysunek 3: Zakładka Pomoc	9
Rysunek 4: Zakładka Pomoc strona WWW	10
Rysunek 5: Zakładka - Ustawienia	11
Rysunek 6: Zakładka Ustawienia – Ogólne	12
Rysunek 7: Zakładka Ustawienia – Podpis – część dotycząca Formatu podpisu, Typu podpisu i ustawień Archiwizacji	13
Rysunek 8: Zakładka Ustawienia – Podpis – część dotycząca Domyślnego certyfikatu i dodatkowych opcji podpisu	14
Rysunek 9: Zakładka Ustawienia – Podpis – część dotycząca zaawansowanych opcji podpisu	16
Rysunek 10: Zakładka Ustawienia – Podpis –Lokalizacja podpisującego	17
Rysunek 11: Zakładka Ustawienia – Podpis – Zaawansowane opcje podpisu XAdES	17
Rysunek 12: Zakładka Ustawienia - Weryfikacja	18
Rysunek 13: Zakładka Ustawienia – Znacznik czasu	20
Rysunek 14: Zakładka Ustawienia – Znacznik czasu – ostrzeżenie o znaczniku czasu SHA-1	21
Rysunek 15: Zakładka Podpisywanie	22
Rysunek 16: Zakładka Podpisywanie – Lista elementów do podpisania	23
Rysunek 17: Wyszukiwanie certyfikatów	23
Rysunek 18: Lista certyfikatów kwalifikowanych	24
Rysunek 19: Lista certyfikatów kwalifikowanych i niekwalifikowanych	24
Rysunek 20: Wybór certyfikatu dla operacji podpisu	25
Rysunek 21: Prośba o wprowadzenie kodu PIN	25
Rysunek 22: Podpisywanie... - Wyszukiwanie kluczy	26
Rysunek 23: Podpisywanie... - Wykonywanie podpisu	26
Rysunek 24: Podsumowanie podpisywania	26
Rysunek 25: Zakładka Podpisywanie – wykonany podpis	27
Rysunek 26: Dane podpisane – zakładka ogólne	28
Rysunek 27: Dane podpisane - zakładka podpis	29
Rysunek 28: Okno wyboru akcji przy obecnym już co najmniej jednym podpisie	30
Rysunek 29: Dane podpisane - zakładka ogólne dla podpisu wielokrotnego	31
Rysunek 30: Dane podpisane - zakładka podpis dla podpisu wielokrotnego	32
Rysunek 31: Okno wyboru akcji przy obecnym już co najmniej jednym podpisie	33
Rysunek 32: Okno wyboru podpisu, który chcemy kontrasygnować	33
Rysunek 33: Okno wyboru podpisu, gdy wybrano wszystkie podpisy do kontrasygnowania	34
Rysunek 34 Dane podpisane - zakładka ogólne dla kontrasygnaty	35
Rysunek 35 Dane podpisane - zakładka podpis dla kontrasygnaty	36
Rysunek 36 Dodawanie graficznego symbolu podpisu – okno główne	37
Rysunek 37 Dodawanie graficznego symbolu podpisu – wskazanie pliku graficznego	37
Rysunek 38 Dodawanie graficznego symbolu podpisu – wybrany plik graficzny	38
Rysunek 39 Dodawanie graficznego symbolu podpisu – symbol graficzny dodany do dokumentu	39
Rysunek 40 Dodawanie graficznego symbolu podpisu – podpisany plik z umieszczonym graficznym symbolem podpisu	39
Rysunek 41 Dodawanie graficznego symbolu podpisu – podpisywanie wielu plików	40
Rysunek 42: Zakładka Weryfikowanie	40
Rysunek 43: Zakładka Weryfikowanie – Lista elementów do weryfikacji	41

Rysunek 44: Dane podpisane	42
Rysunek 45: Zakładka Weryfikowanie – Lista elementów do weryfikacji	43
Rysunek 46: Weryfikacja... ..	43
Rysunek 47: Podsumowanie weryfikacji	44
Rysunek 48: Status weryfikacji: Poprawnie zweryfikowany	45
Rysunek 49: Status weryfikacji: Błędnie zweryfikowany	46
Rysunek 50: Brak certyfikatu wystawcy lub niemożliwość pobrania aktualnych list CRL	46
Rysunek 51: Nieprawidłowa wartość podpisu	47
Rysunek 52: Nieprawidłowy certyfikat	47
Rysunek 53: Błąd przy weryfikacji certyfikatu niekwalifikowanego	47
Rysunek 54: Powiadomienie o aktualizacji.....	47
Rysunek 55: Strona WWW z nową wersją proCertum SmartSign	48