PWPW
POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH

PODRĘCZNIK UŻYTKOWNIKA APLIKACJI SIGILLUM SIGN

WERSJA DOKUMENTU: 1.10
WERSJA OPROGRAMOWANIA: 1.10
DATA AKTUALIZACJI: 2023-10-19

Informacje prawne

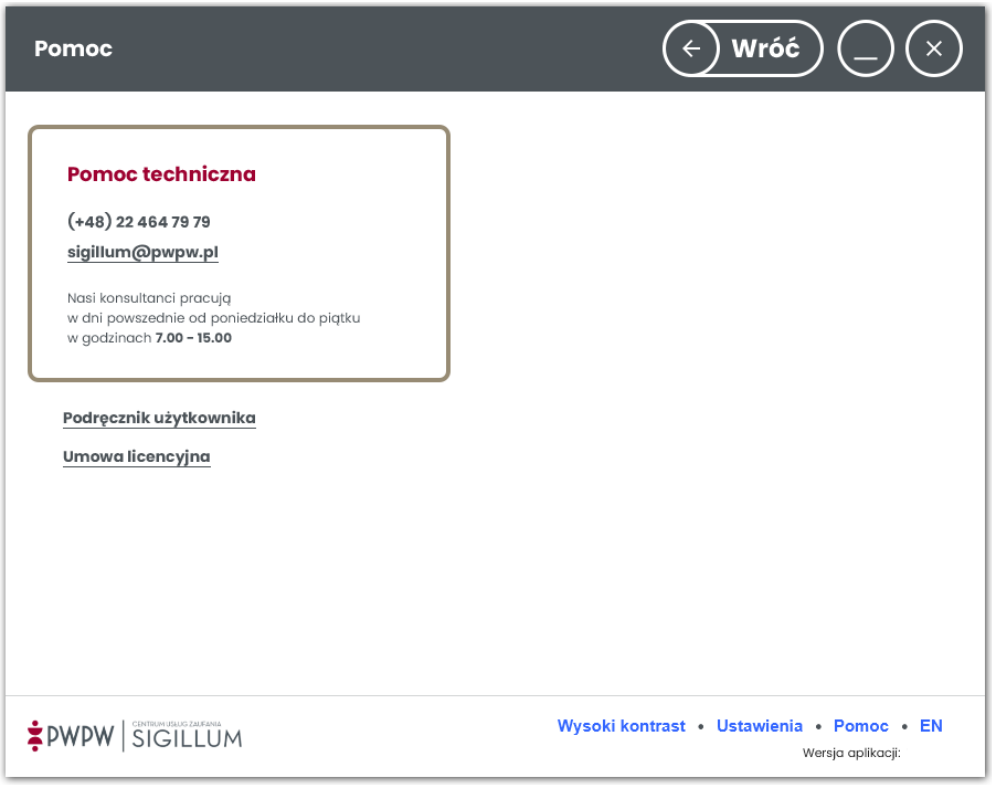
1 Spis treści

2 Wstęp

Niniejszy dokument jest wersją 1.10 Podręcznika użytkownika aplikacji „Sigillum Sign". Podręcznik użytkownika w obecnej postaci dotyczy wersji 1.10.

Celem niniejszego dokumentu jest zapoznanie użytkowników aplikacji z jej funkcjonalnością, sposobem instalacji i deinstalacji oraz przedstawienie ogólnych zagadnień związanych z podpisem elektronicznym, których znajomość jest niezbędna do świadomego oraz bezpiecznego korzystania z aplikacji.

Podręcznik jest dostępny z poziomu aplikacji, po wyświetleniu ekranu POMOC



3 Przeznaczenie aplikacji

Sigillum Sign jest aplikacją służącą do składania i weryfikacji podpisu elektronicznego na pliku, przeznaczoną do użytkowania na pojedynczym komputerze.

Ze względu na charakter aplikacji jej użytkownikami mogą być klienci indywidualni oraz klienci korporacyjni z sektora publicznego i biznesowego.

Aplikacja może podpisywać i szyfrować dowolny rodzaj danych, które są w postaci dowolnego pliku. Mogą to być zarówno dane binarne, tekstowe, multimedialne, XML itd. o dowolnym rozszerzeniu pliku zawierającego dane. Z powyższego wynika, że każdy plik, do którego mamy dostęp możemy podpisać elektronicznie lub zaszyfrować. Podpisowi nie podlegają meta dane pliku typu: nazwa, data utworzenia, właściciel itp. (zmianie ulega tylko data ostatniego użycia pliku, która jest zgodna z datą złożenia podpisu/zaszyfrowania). W procesie szyfrowania zmianie ulegają zarówno meta dane jak i zawartość pliku. Dane w postaci pliku, które są wskazane dla aplikacji, podczas jej działania ulegają przekształceniom, w wyniku których powstaje nowy plik zawierający podpis lub zaszyfrowane pliki z meta danymi. W przypadku odszyfrowania lub wyodrębnienia danych, wynikiem jest plik źródłowy.

Aplikacja obsługuje certyfikaty kwalifikowane i niekwalifikowane wydane przez PWPW S.A. oraz innych podmiotów usług certyfikacyjnych, tj.: Certum by Asseco, Enigma, Eurocert, Krajowa Izba Rozliczeniowa.

Aplikacja Sigillum Sign została przygotowana zgodnie z **Rozporządzeniem Parlamentu Europejskiego i Rady (UE)** NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

Sigillum Sign implementuje normy ETSI wykorzystując pakiet bibliotek „*Digital Signature Services*" w wersji 5-ej opublikowanych przez Connecting Europe Facility (CEF). Oprogramowanie umożliwia złożenie podpisu oraz jego weryfikację zgodnie z wymogami z Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. (eIDAS) oraz z towarzyszących mu aktów wykonawczych.

Sigillum Sign 1.8 korzysta z OpenJDK – wolnodostępnej i otwartej implementacji języka programowania Java rozwijanej na licencji GNU GPL.

Aplikacja współpracuje z czytnikami ekranu pozwalającymi osobom niewidomym oraz niedowidzącym korzystać z aplikacji.

3.1 Wymagania sprzętowe

Minimalne wymagania sprzętowe dla systemu operacyjnego użytkownika aplikacji:

- procesor o taktowaniu 2 gigaherc (GHz) lub szybszy,
- przynajmniej 4 gigabajt (GB) pamięci RAM,
- 970 megabajtów (MB) przestrzeni na dysku twardym,
- minimalna rozdzielczość: 1024x768px, 16bit,
- skonfigurowane połączenie internetowe,
- jeden port USB 2.0,
- czytnik kart elektronicznych USB.

Wymagania programowe dla stacji roboczej użytkownika aplikacji:

- MS Windows od wersji 10,
- Apple MacOS - dwie najnowsze stabilne wersje pośrednie (np. Ventura i Sonoma)
- sterowniki oraz oprogramowanie do obsługi czytnika/karty,
- aplikacja do odczytu dokumentów pdf.

Uwaga: w związku z zakończeniem świadczenia wsparcia przez firmę Microsoft dla wcześniejszych wersji systemów operacyjnych, nie gwarantujemy na nich bezpieczeństwa i poprawności działania aplikacji Sigillum Sign.

4 Słownik

W rozdziale tym zostały zdefiniowane podstawowe pojęcia (w kolejności alfabetycznej) związane z podpisem elektronicznym:

- **ASiC (ang. Associated Signature Containers)**

Jest to najnowszy format podpisu elektronicznego. Dedykowany do podpisywania danych, które następnie są umieszczane w kontenerze ZIP. Algorytm ZIP został wybrany ze względu na największą uniwersalność oraz rozpoznawalność przez różne systemy operacyjne. Plik ZIP formatu ASiC zawiera dwa foldery. Istnieją dwa typy formatu ASiC:

  - ***ASiCS (Simple)***

Służy do przechowywania jednego zestawu danych oraz kilku powiązanych z nim podpisów, przy czym podpisy te muszą zwierać się w jednej strukturze.

  - ***ASiCE (Extended)***

Może przechowywać kilka zestawów danych.

ASiC wspiera następujące formaty podpisu i znakowania czasem:
- CAdES baseline signatures (EN 319 122-1 [1]);
- XAdES baseline signatures (EN 319 132-1 [2]);
- RFC 3161 [3] time-stamp tokens; and
- RFC 4998 [8] or RFC 6283 [9] evidence records.

- **Kwalifikowany podpis elektroniczny (wg Rozporządzenia eIDAS)**

Jest to zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

- **CA (ang. certification authority)**

(więcej pod hasłem Urząd ds. Certyfikacji).

- **Certyfikacja (ang. certification)**

Pod pojęciem certyfikacji należy rozumieć:
- wydawanie certyfikatu elektronicznego przez urząd certyfikacji,
- wydawanie certyfikatu zgodności z obowiązującymi kryteriami oceny zabezpieczeń przez jednostkę certyfikującą działającą w ramach krajowego systemu certyfikacji zabezpieczeń.

- **Certyfikat elektroniczny (ang. Digital Certificate)**

Certyfikat elektroniczny, jest to cyfrowe zaświadczenie, za pomocą którego możliwe jest potwierdzenie tożsamości osoby lub firmy posługującej się nim. Certyfikat elektroniczny jest zwykle zaszyfrowanym plikiem zawierającym informacje o właścicielu certyfikatu (imię i nazwisko, firma, adres, PESEL lub NIP) oraz inne dane (wystawca certyfikatu, termin ważności, klucz prywatny, klucz publiczny, przeznaczenie certyfikatu, unikatowy numer seryjny). Certyfikat jest niezbędny do podpisywania, szyfrowania i odszyfrowywania danych, a także weryfikacji podpisu elektronicznego.

- **Certyfikat klucza publicznego (ang. public key certificate)**

Informacja o kluczu publicznym poświadczona przez urząd certyfikacji, potwierdzająca, że klucz publiczny należy do konkretnego podmiotu (osoby, firmy lub innej organizacji).

- **Certyfikat ROOT- certyfikat główny**

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

- **CAdES**

Format podpisu rozszerzającym standard CMS zawierające opcjonalne dodatkowe podpisane i niepodpisane atrybuty zgodne ze specyfikacją (Advanced Electronic Signature). Format CAdES jest analogiczny do formatu XAdES i występuje w wariantach (BES, T ,XL, A). Więcej informacji odnośnie poszczególnych wariantów podpisów można znaleźć w opisie formatu XAdES.

- **CMS (ang. Cryptographic Message Syntax)**

Formatem podpisu elektronicznego będący następcą standardu formatu PKCS#7 po wprowadzeniu poprawek ze specyfikacji RFC-2630 . Format ten umożliwia tworzenie kontrasygnat, czyli dołączanie podpisów kolejnych podmiotów do istniejących sygnatur.

- **CRL (ang. Certificate Revocation List)**

Lista unieważnionych i zawieszonych certyfikatów, wydawana przez podmiot świadczący usługi certyfikacyjne, zawierająca numer kolejny listy, datę jej publikacji, przewidywany czas publikacji kolejnej listy, określenie podmiotu wydającego listę, numery seryjne unieważnionych i zawieszonych certyfikatów.

- **Dostawca usług zaufania**

Oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.

- **eIDAS**

Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

- **Klucz prywatny**

Klucz służący do wykonywania zastrzeżonej czynności. Jego rozpowszechnienie zagraża bezpieczeństwu systemu. Klucz prywatny może być w wyłącznym posiadaniu właściciela informacji. Najczęściej służy do odszyfrowywania i podpisywania informacji.

- **Klucz publiczny**

Klucz służący do wykonywania ogólnodostępnej czynności. Klucz publiczny może być rozpowszechniany wśród dowolnych osób. Najczęściej służy do szyfrowania informacji lub weryfikacji podpisu złożonego przez właściciela odpowiadającego mu klucza prywatnego.

- **Kontrasygnata**

Kontrasygnata, w przypadku podpisu elektronicznego, to dołączanie przez drugą osobę kolejnego podpisu elektronicznego do już istniejącego podpisu, potwierdzając w ten sposób jego ważność.

- **Kwalifikowany certyfikat podpisu elektronicznego (wg Rozporządzenia eIDAS)**

Certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I do Rozporządzenia eIDAS.

- **Kwalifikowany dostawca usług zaufania**

Oznacza dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru.

- **Kwalifikowana usługa zaufania**

Oznacza usługę zaufania, która spełnia stosowne wymogi określone w Rozporządzeniu eIDAS.

- **Kwalifikowane urządzenie do składania podpisu elektronicznego**

Oznacza urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II Rozporządzenia eIDAS.

- **Microsoft Root Certificate**

Program firmy Microsoft zawierający listę komercyjnych urzędów certyfikacyjnych (CA) potwierdzonych przez firmę Microsoft.

- **OCSP (ang. Online Certificate Status Protocol)**

Protokół informowania o statusie ważności certyfikatu w trybie połączeniowym (on-line).

- **PAdES**

Format podpisu elektronicznego pozwalający na dołączenie do dokumentów w formacie PDF podpisu cyfrowego posiadającego wszystkie właściwości zaawansowanego podpisu cyfrowego (Advanced Electronic Signature) takie jak znakowanie czasem lub dołączanie dodatkowych sygnatur.

- **Podpis elektroniczny**

Oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis.

- **PKCS#7: (Public-Key Cryptography Standard)**

Format podpisu opisany w specyfikacji RFC-2315, który definiuje dwa podstawowe typy: podpis cyfrowy i kopertę cyfrową. Podpis cyfrowy ma na celu zagwarantowanie, że dana wiadomość pochodzi od określonej osoby. Koperta cyfrowa gwarantuje poufność, dane są zaszyfrowane wraz z certyfikatem i kluczem publicznym, można je odczytać pod warunkiem posiadania klucza prywatnego zawartego w kopercie certyfikatu.

PKCS#7 udostępnia także dołączanie kluczy w większej ilości niż 1 (np. zaszyfrowanie wiadomości przeznaczonej dla wielu odbiorców).

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

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

- **Polityka certyfikacji (ang. certificate policy- CP)**

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

- **PROXY**

Serwer Proxy jest to usługa pośrednicząca w komunikacji między użytkownikiem, a docelowym systemem. Jego zadaniem może być m.in. zapamiętywanie odwiedzonych stron WWW w celu ich szybszego wyświetlenia w przypadku ponownego wywołania ich.

- **Root CA (ang. Root Certification Authority)**

Główny Urząd Certyfikacji pełniący rolę nadrzędną w stosunku do kwalifikowanej infrastruktury klucza publicznego. Posługuje się on tzw. certyfikatem samo podpisanym, tzn. podlegającym weryfikacji w urzędzie, który go wystawił. Pozostałe urzędy certyfikacji działają na podstawie certyfikatów wystawionych przez urzędy nadrzędne. Root CA są ujęte w wielu aplikacjach (np. Microsoft Root Certificate), a wystawione przez nie certyfikaty są domyślnie zaufane.

- **Ścieżka certyfikacji**

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

- **Urząd ds. Certyfikacji - CA (ang. Certification Authority)**

Centrum certyfikacji wystawiające certyfikaty elektroniczne.
Urząd realizujący usługę wydawania i zarządzania certyfikatami. Potoczne nazwy to Urząd Certyfikacji lub Centrum Certyfikacji najbardziej typowego urzędu certyfikacyjnego realizującego podstawową usługę certyfikacyjną w ramach PKI - certyfikację kluczy publicznych.

- **Unieważnienie certyfikatu**

Urząd, który wystawił certyfikat ma prawo unieważnić go, jeśli:

  - został on wydany na podstawie nieprawdziwych lub nieaktualnych danych osoby lub podmiotu, dla którego został wystawiony,
  - podmiot świadczący usługi certyfikacyjne nie dopełnił obowiązków określonych w ustawie,
  - osoba składająca podpis elektroniczny weryfikowany na podstawie tego certyfikatu nie dopełniła ustawowego obowiązku przechowywania danych służących do składania podpisu elektronicznego w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem w okresie ważności certyfikatu służącego do weryfikacji tych podpisów,
  - podmiot świadczący usługi certyfikacyjne zaprzestaje tej działalności, a jego praw i obowiązków nie przejmuje inny kwalifikowany podmiot,
  - zażąda tego osoba składająca podpis elektroniczny lub osoba trzecia wskazana w certyfikacie,
  - zażąda tego Minister właściwy do spraw gospodarki,
  - osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych.

Certyfikat, który został unieważniony, nie może być ponownie uznany za ważny.

- **Urząd Rejestracji, Urząd ds. Rejestracji (ang. Registration Authority (RA))**
  Organ odpowiedzialny za weryfikację tożsamości subskrybenta oraz przekazanie odpowiednich informacji do urzędu certyfikacji zgodnie z procedurą rejestracji stosowaną w celu wydania certyfikatu.

- **Urządzenie służące do składania podpisu elektronicznego**
  Oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania podpisu elektronicznego.

- **Usługi zaufania**
  Oznacza usługi elektroniczne zazwyczaj świadczone za wynagrodzeniem i obejmujące:

a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub
b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych;
lub
c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

- **Uouzoie (Ustawa o usługach zaufania oraz identyfikacji elektronicznej)**

Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dziennik Ustaw 2016 poz. 1579), określająca:

- krajową infrastrukturę zaufania;
- działalność dostawców usług zaufania, w tym zawieszanie certyfikatów podpisów elektronicznych i pieczęci elektronicznych;
- tryb notyfikacji krajowego systemu identyfikacji elektronicznej;
- nadzór nad dostawcami usług zaufania;
- krajowy schemat identyfikacji elektronicznej;
- nadzór nad krajowym schematem identyfikacji elektronicznej;
- zasady określania i wykorzystywania standardu usługi rejestrowanego doręczenia elektronicznego.

- **Uwierzytelnienie (ang. authentication)**

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

- **Urząd Znacznika Czasu - UZC (ang. Time Stamping Authority - TSA)**

Urząd realizujący usługę certyfikacyjną oznaczania czasem przedstawionego skrótu dokumentu elektronicznego.

- **Walidacja kwalifikowanych podpisów elektronicznych**

Proces walidacji kwalifikowanego podpisu elektronicznego potwierdza ważność kwalifikowanego podpisu elektronicznego, pod warunkiem że:

a) certyfikat, który towarzyszy podpisowi, był w momencie składania podpisu kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I Rozporządzenia eIDAS;
b) kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu;
c) dane służące do walidacji podpisu odpowiadają danym dostarczonym stronie ufającej;
d) unikalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie jest prawidłowo dostarczony stronie ufającej;
e) jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane stronie ufającej;
f) podpis elektroniczny został złożony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego;
g) integralność podpisanych danych nie została naruszona;

h) wymogi przewidziane w art. 26 Rozporządzenia eIDAS zostały spełnione w momencie składania podpisu.

System wykorzystany do walidacji kwalifikowanego podpisu elektronicznego zapewnia stronie ufającej prawidłowy wynik procesu walidacji i umożliwia stronie ufającej wykrycie wszelkich problemów związanych z bezpieczeństwem.

- **XADES (XML Advanced Electronic Signature) format podpisu elektronicznego oparty na standardzie XML. Warianty podpisu XAdES:**

1. XAdES-BES – (Basic Electronic Signature) –zgodnie z nazwą jest to podstawowy format podpisu XAdES, który powstał, jako rozwinięcie formatu XML-DSig, do którego dodano takie informacje jak: czas lokalny, miejsce, rola osoby składającej podpis, ścieżka certyfikacji, znaczniki czasowe oraz możliwość stosowania dodatkowych podpisów (podpis wielokrotny, kontrasygnata);
2. XAdES-T – (Time Stamp) – format ten dodaje do podpisu typu XAdES-BES znacznik czasowy wystawiony przez Urząd Znakowania Czasem, co umożliwia określenie ważności podpisu w ustalonym momencie czasowym;
3. XAdES-C – (Complete) – format umożliwia dodanie do powyższych formatów elementów wskazujących na certyfikaty użyte podczas tworzenia podpisu oraz elementów pozwalających na sprawdzenie ważności użytych do podpisu certyfikatów;
4. XAdES-X – (Extended) – format dodaje znacznik czasu na elementach, o które został uzupełniony podpis podczas tworzenia XAdES-C;
5. XAdES-XL – (Extended Long Term) – format umożliwia dodanie do powyższych formatów dodatkowych certyfikatów (poza certyfikatem osoby podpisującej). Ponadto zawiera informacje pobrane z serwerów CRL lub OCSP. Podpis w tym formacie szczegółowo określa warunki, w jakich został złożony. Zapewnia on, że certyfikat osoby podpisującej w chwili podpisania pliku był ważny;
6. XAdES-A – (Archival) – format ten umożliwia dodawanie znaczników czasowych wystawianych przez Urząd Znakowania Czasem. Jest on stosowany m.in. w celu konserwacji podpisu (przedłużenia jego ważności). Dzięki niemu, właściciel podpisanego pliku może dodawać nowe zaświadczenia certyfikacyjne UZC przed upływem terminu ważności poprzedniego.

- **XMLDsig (ang. XML signature)**

Jeden z formatów podpisu elektronicznego dla XML. Jako jego rozwinięcie powstał format XAdES-BES. Najważniejsze cechy tego formatu to: tworzenie podpisu w oddzielnym pliku oraz możliwość podpisania wielu plików jednocześnie. Brak w nim jest elementów wymaganych dla podpisu kwalifikowanego.

- **Zaawansowany podpis elektroniczny**

Zaawansowany podpis elektroniczny oznacza podpis elektroniczny, który spełnia następujące wymogi:

a) jest unikalnie przyporządkowany podpisującemu;
b) umożliwia ustalenie tożsamości podpisującego;
c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz

d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

- **Zawieszenie certyfikatu**

W przypadku istnienia podejrzenia uprawniających do unieważnienia certyfikatu, wystawca certyfikatu zobowiązany jest go zawiesić. Jednocześnie zostają podjęte działania wyjaśniające powstałe wątpliwości. Urząd certyfikacji ma 7 dni na ich wyjaśnienie. Po upływie tego okresu lub w przypadku braku możliwości wyjaśnienia wątpliwości certyfikat zostaje unieważniony.

- **Usługa elektronicznego znacznika czasu**

Usługa polegająca na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z plikami opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę.

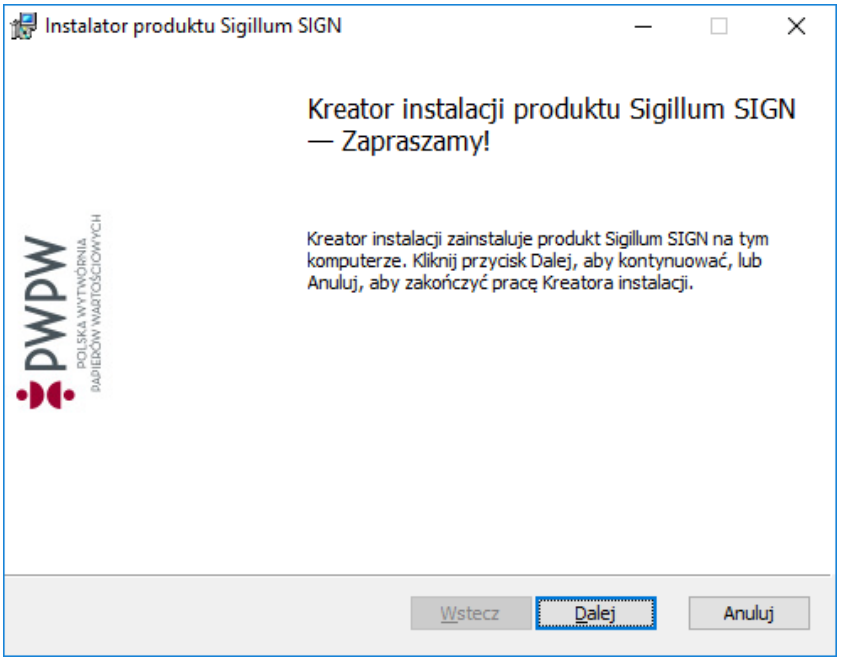
- **Zaświadczenie certyfikacyjne**

Elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub „organu" - kwalifikowanego podmiotu świadczącego usługi certyfikacyjne, umożliwiające identyfikację tego podmiotu lub organu.

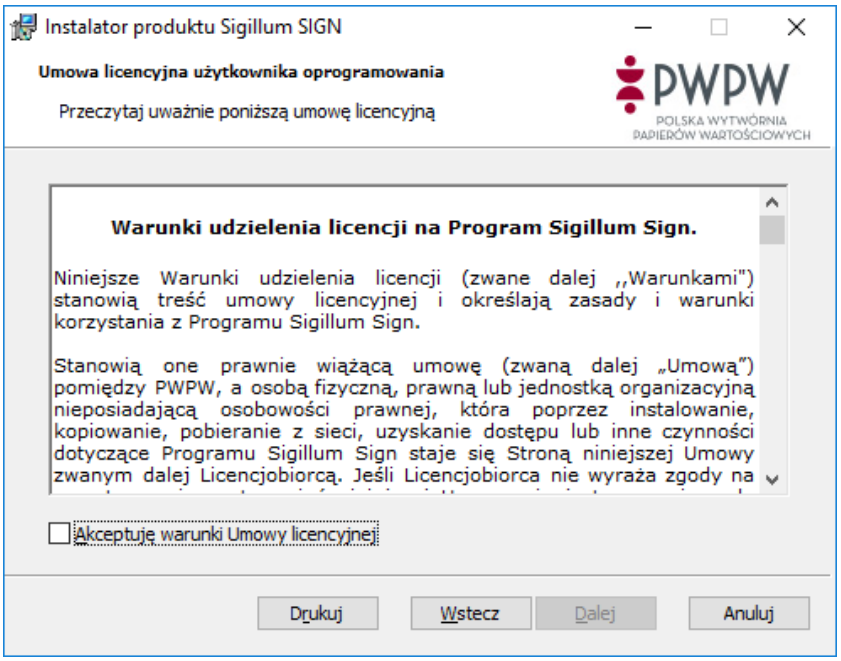
5 Instalacja aplikacji

5.1 Instalacja na systemach operacyjnych Microsoft Windows

Po uruchomieniu instalatora pojawia się okno informacyjne z przyciskami nawigacyjnymi:



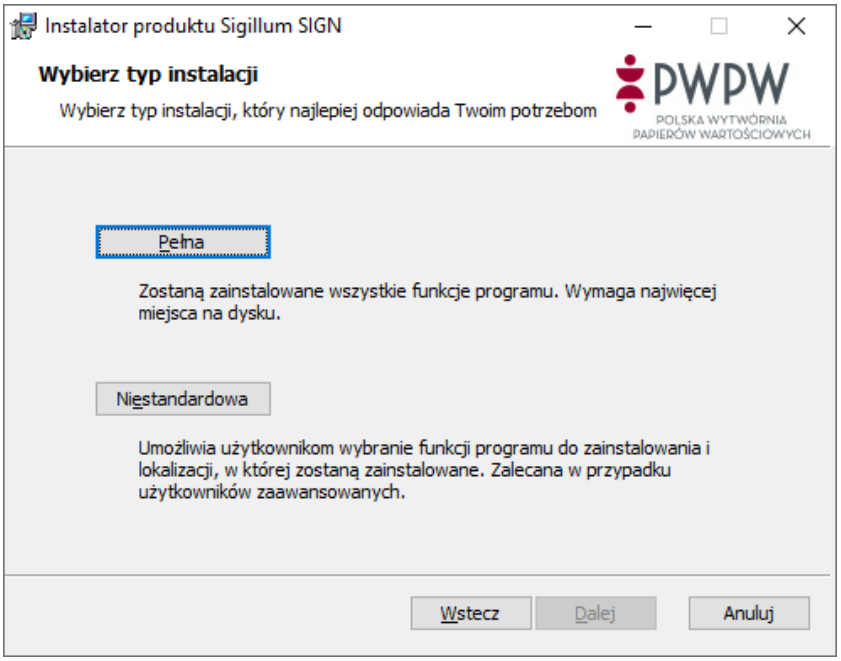
Kliknięcie przycisku *Dalej* powoduje wyświetlenie ekranu z Umową licencyjną:



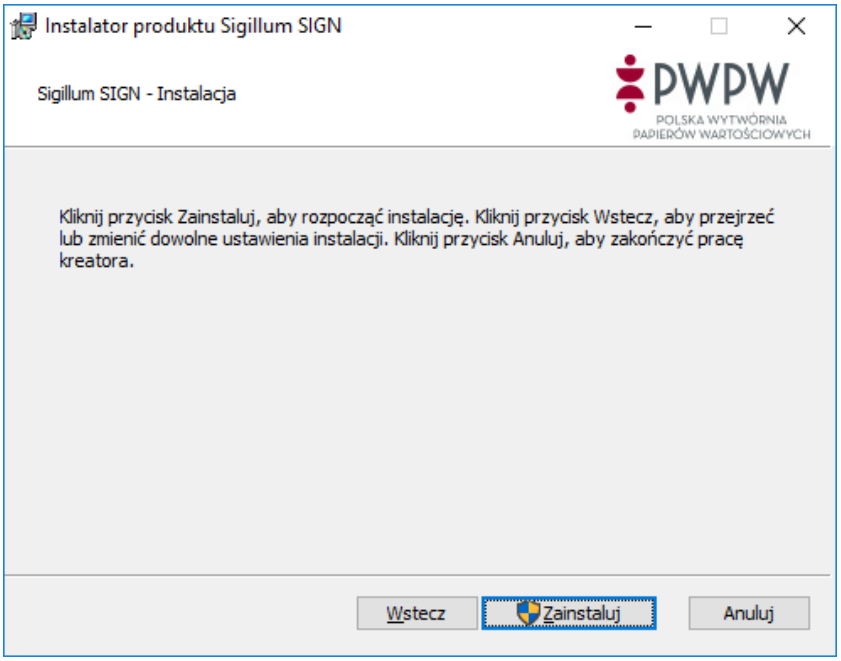
Po przeczytaniu umowy i zaznaczeniu akceptacji jej warunków, przycisk *Dalej* umożliwia przejście do kolejnego kroku.

Następnie pojawi się okno z możliwością wyboru, które ze składników aplikacji zostaną zainstalowane. Użytkownik ma do wyboru dwie opcje:

- *Pełna* – instaluje wszystkie funkcje programu.
- *Niestandardowa* – umożliwia użytkownikowi wybranie funkcji programu do zainstalowania i lokalizacji, w której zostaną zainstalowane,

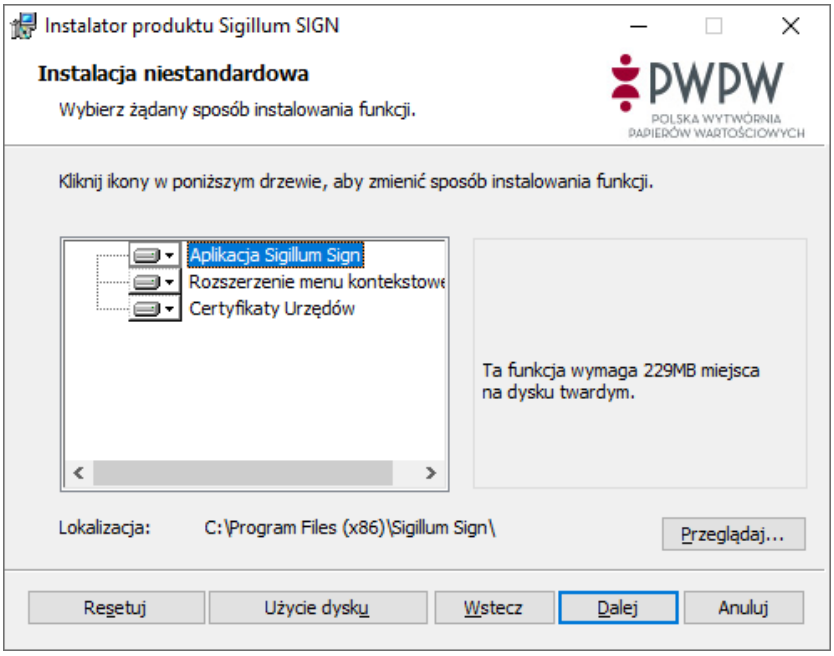


Po wybraniu opcji Pełna, instalator wyświetla okno potwierdzenia instalacji.

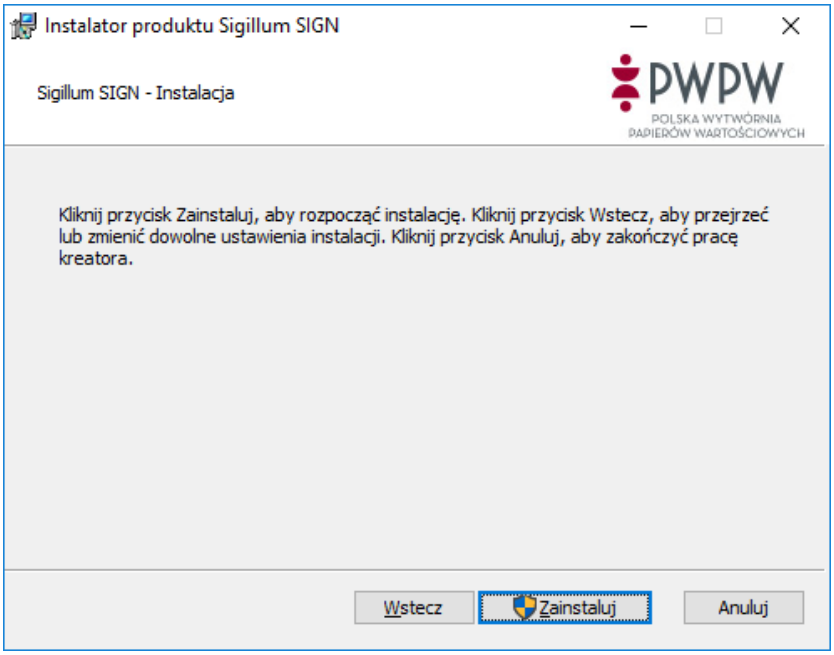


W przypadku, gdy zostanie wybrana opcja *Niestandardowa*, instalator wyświetli okno, w którym należy wybrać, które ze składników aplikacji zostaną zainstalowane.

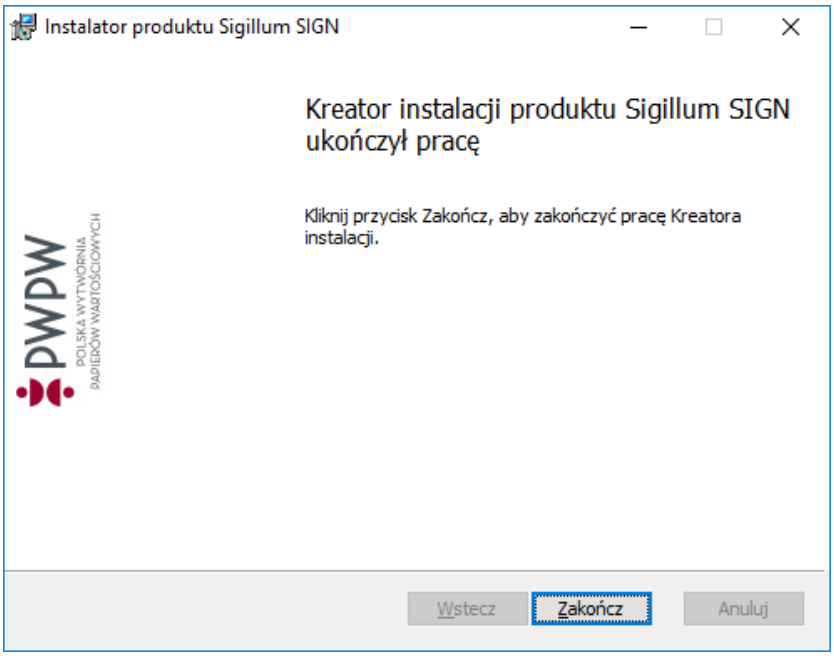
Można też wskazać miejsce na dysku, w którym aplikacja zostanie zainstalowana.



Po wyborze składników oraz miejsca zainstalowania, instalator wyświetla okno potwierdzenia instalacji.

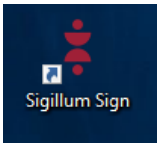


Po zakończeniu procesu instalacji, pojawia się okno potwierdzające pomyślną instalację aplikacji:



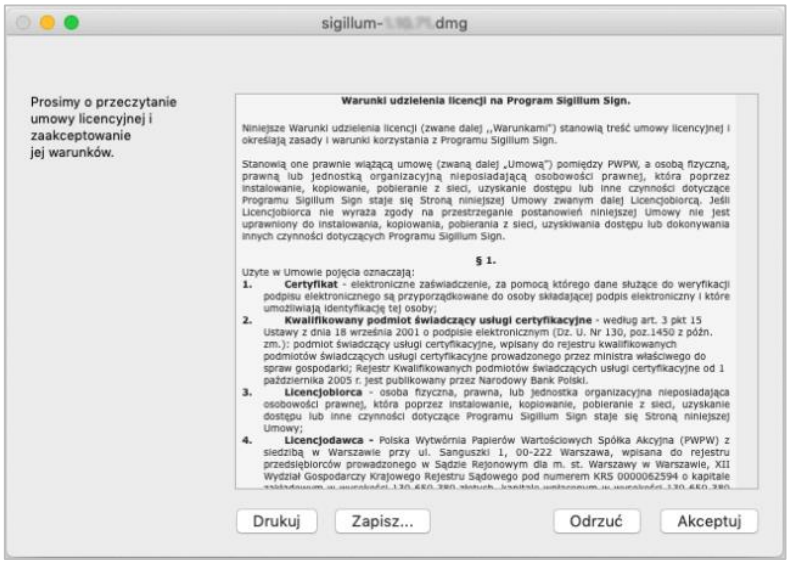
Kliknięcie przycisku *Zakończ* kończy proces instalacji.

Można otworzyć aplikację z poziomu paska narzędzi i/lub używając skrótu na pulpicie.



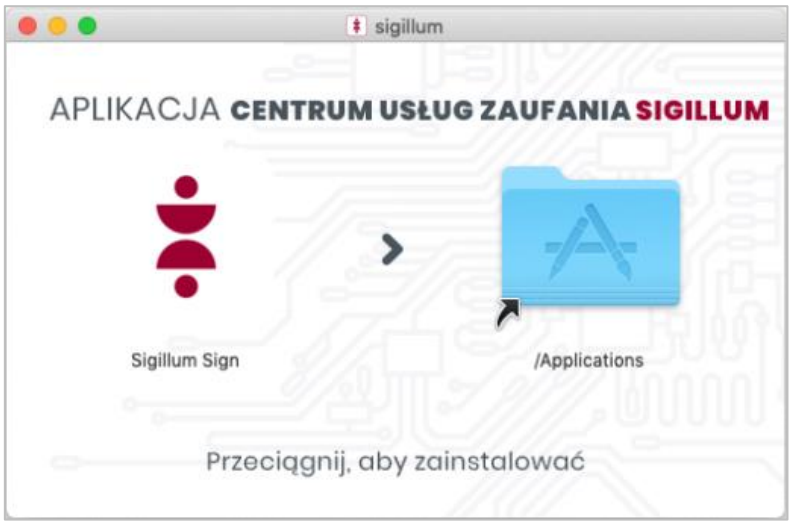
5.2 Instalacja na systemach operacyjnych MacOS

Po uruchomieniu instalatora wyświetlony zostaje ekran z umową licencyjną:



Po przeczytaniu umowy należy kliknąć przycisk *Akceptuj*.

Następnie pojawi się poniższe okno, w którym należy przeciągnąć ikonę aplikacji do folderu Applications (Aplikacje).



Aplikacja zostaje zainstalowana.

Po pomyślnej instalacji należy zamknąć powyższe okno.

Aplikację można uruchomić z listy aplikacji poprzez kliknięcie ikony:

5.3 Informacja o aktualizacji

Przy uruchamianiu aplikacji (domyślnie codziennie), sprawdzany jest serwer aktualizacji. Jeśli istnieje dostępna aktualizacja, zostanie wyświetlony komunikat jak na obrazie poniżej.

Jeśli podczas uruchamiania aplikacja nie ma dostępu do serwera aktualizacji wyświetlony zostanie następujący komunikat.

6 Obsługa aplikacji

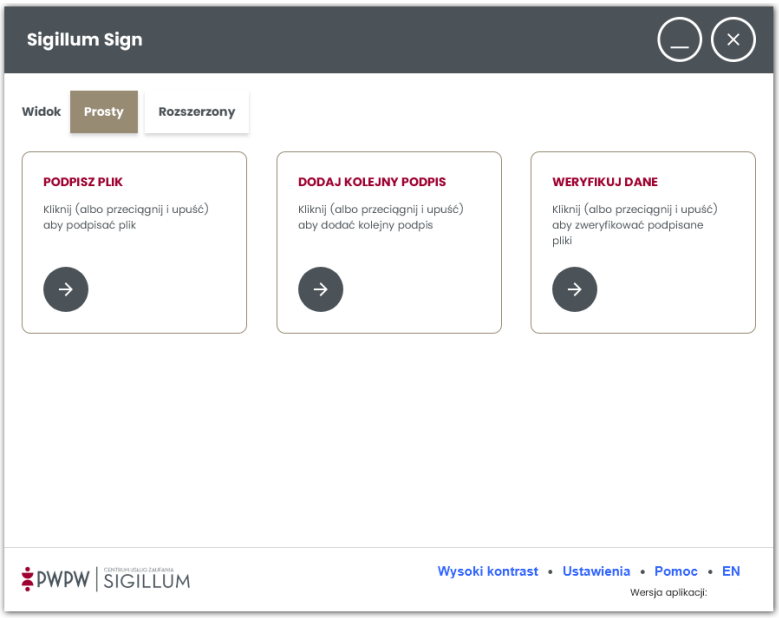
6.1 Strona główna – widok prosty

Po uruchomieniu aplikacji, otwiera się strona główna (domyślna) złożona z trzech kafelków:

Podpisz plik – rozpoczyna proces podpisywania plików.

Dodaj kolejny podpis – otwiera proces dodawania kolejnego podpisu do pliku

Weryfikuj dane – otwiera proces weryfikacji.

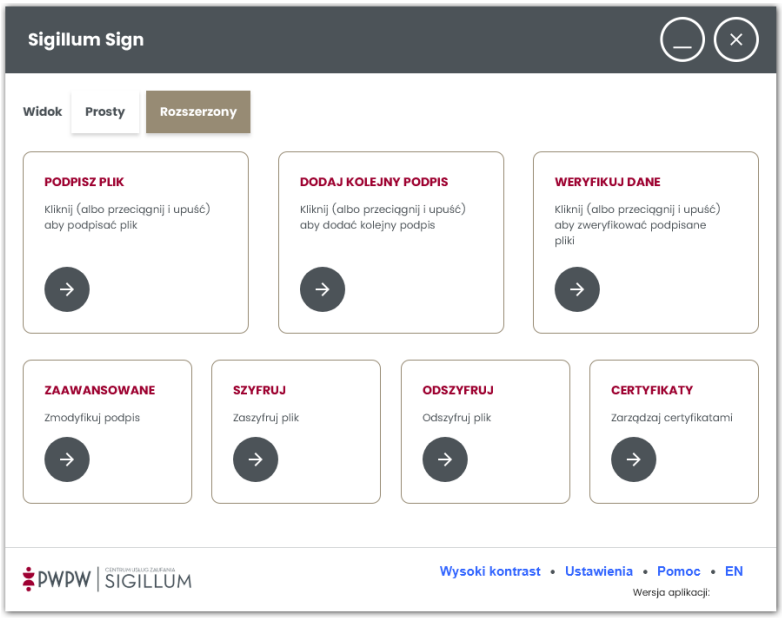


Po prawej stronie dolnego paska umieszczone są polecenia aplikacji tj. ***Wysoki/Normalny kontrast***, ***Ustawienia***, ***Pomoc*** oraz skrót ***PL/EN*** umożliwiający przełączanie języka**.**

Kliknięcie przycisku ***Rozszerzony*** powoduje przełączenie na widok zawierający dodatkowe funkcjonalności.

6.2 Strona główna – widok rozszerzony

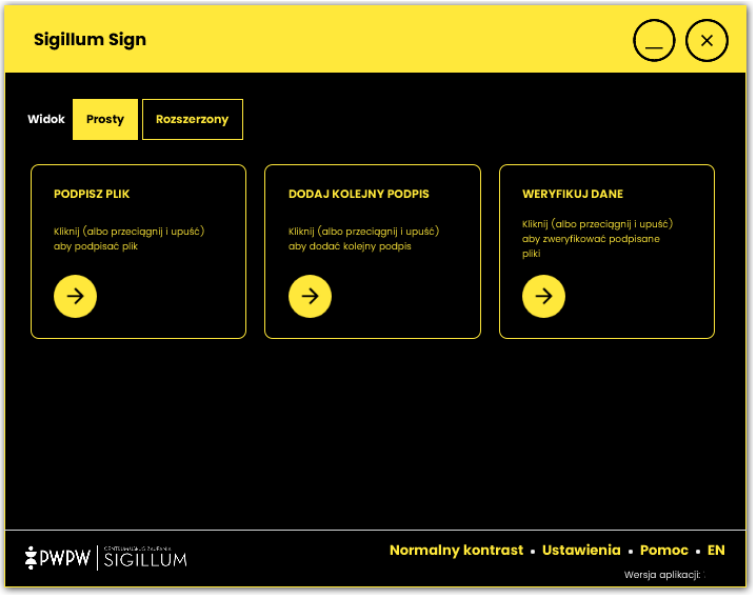
Poza kafelkami ***Podpisz plik***, ***Dodaj kolejny podpis*** oraz ***Weryfikuj dane***, *dostępne* są jeszcze ***Zaawansowane, Szyfruj***, ***Odszyfruj*** oraz ***Certyfikaty***.



Podpisz plik	– rozpoczyna proces składania podpisu na pliku/ach,
Dodaj kolejny podpis	– rozpoczyna proces dodawania kolejnego podpisu do pliku,
Weryfikuj dane	– start procesu weryfikacji podpisu,
Zaawansowane	– odpowiada za operacje: zastąpienia, rozszerzenia, dodania kontrasygnaty lub znacznika czasu,
Szyfruj	– otwiera proces szyfrowania,
Odszyfruj	– rozpoczyna proces deszyfrowania,
Certyfikaty	– opcja zarządzania certyfikatami, które wykorzystywane są przy realizacji powyższych zadań.

6.3 Wysoki kontrast

Wersja kontrastowa przeznaczona jest dla osób niedowidzących. Po kliknięciu w link *Wysoki kontrast* na dolnym pasku aplikacji, zmieniony zostaje kontrast ekranu aplikacji. Po kliknięciu w link *Normalny kontrast* na dolnym pasku aplikacji, kontrast ekranu zostaje przywrócony.



Domyślnie przy uruchomieniu aplikacji ustawiany jest kontrast, który można skonfigurować w Ustawieniach (6.5.8).

6.4 Współpraca z czytnikami ekranu

Jeśli w systemie Windows uruchomiono aplikację czytnika ekranu (np. NVDA), uruchomienie aplikacji Sigillum Sign odbędzie się w trybie współpracy z czytnikiem ekranu.

Używanie klawiatury w trybie współpracy z czytnikiem:

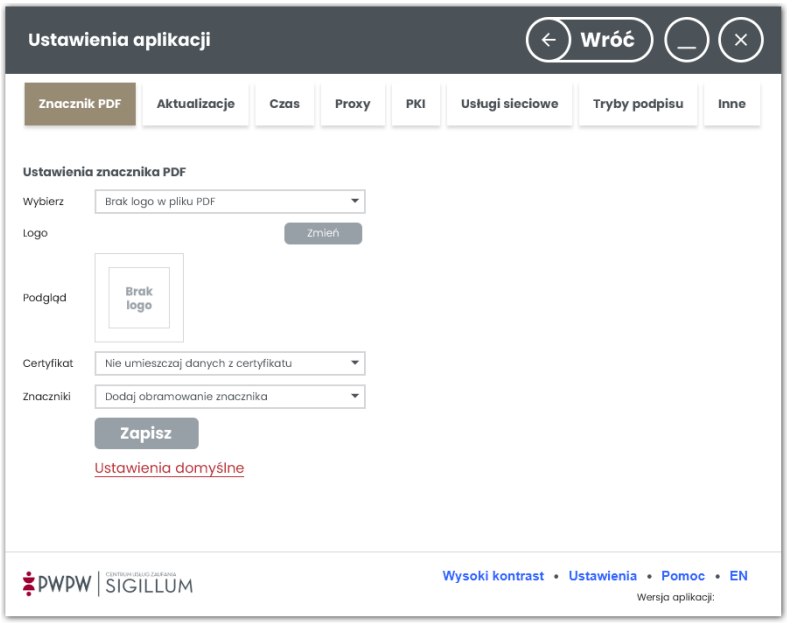
- **TAB** (tabulator) – przechodzenie po między elementami interfejsu graficznego „do przodu”,
- **Shift + TAB** – przechodzenie po między elementami interfejsu graficznego „do tyłu”,
- **ENTER** – naciśnięcie przycisku ekranowego lub kliknięcie pola tekstowego otwierającego okno wyboru,
- **strzałka w dół** – rozwinięcie listy wyboru,
- **SPACJA** – zaznaczenie checkboxa lub radiobuttona.

Dodatkowo, w trybie współpracy z czytnikiem ekranu, aplikacja umożliwia odczytanie wyniku weryfikacji podpisu (przycisk **Czytaj wynik** na ekranie Weryfikacji podpisu elektronicznego).

Tryb współpracy z czytnikiem nie jest obsługiwany na ekranie autoryzacji proxy po starcie aplikacji.

6.5 Ustawienia

Po kliknięciu w link *Ustawienia* na dolnym pasku aplikacji, prezentowane jest okno aplikacji:

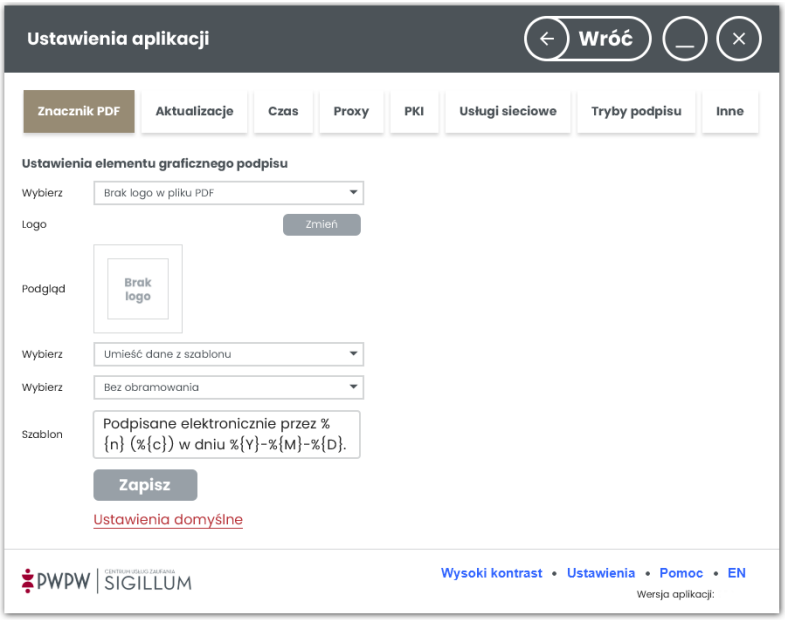


W tym widoku użytkownik może dokonywać zmian oraz zarządzać ustawieniami aplikacji prezentowanymi w poszczególnych zakładkach.

Ustawienia w aplikacji (prezentowane, jako zakładki) podzielone są na:

Znacznik PDF	Możliwość umieszczenia oraz pozycjonowania elementu graficznego podpisu w dokumencie typu PDF.
Aktualizacje	Możliwość ustawienia interwału czasowego, z jakim ma odbywać się sprawdzenie czy wykorzystywana wersja jest wersją aktualną.
Czas	Wybór źródła pobierania czasu przez aplikację.
Proxy	Włączenie tej opcji spowoduje, że użytkownik będzie mógł skonfigurować ustawienia proxy.
PKI	Dotyczą ustawień certyfikatów, profili podpisu, algorytmu szyfrowania oraz polityki certyfikacji.
Usługi sieciowe	Umożliwiają zarządzanie serwerami CRL, TSP, NTP.
Tryby podpisu	Umożliwiają ustawienie domyślnych: Typu zobowiązania, Wariantu i Funkcji skrótu dla kolejnego podpisu oraz kontrasygnaty.
Inne	Umożliwia ustawienie kontrastu, rozszerzeń podpisanych plików, języka oraz folderu, z którego wybierane są pliki.

6.5.1 Znacznik PDF



Menu tej zakładki umożliwia zarządzanie ustawieniami elementu graficznego podpisu:

- Lista wyboru „**Wybierz**" – opcja umożliwia umieszczenie zdefiniowanego logo w pliku PDF,
- **Logo** – przycisk **Zmień** umożliwia wybór/zmianę pliku graficznego,
- **Podgląd** – tu wyświetlana jest miniatura wybranego pliku graficznego,
- lista wyboru „**Wybierz**" – umożliwia umieszczenie danych z szablonu w elemencie graficznym podpisu,
- lista wyboru „**Wybierz**" – umożliwia umieszczenie obramowania wstawianego elementu graficznego podpisu,
- **Szablon** – pole tekstowe pozwalające dowolnie skonfigurować tekst wstawiany w dokumencie PDF dla każdej wersji językowej aplikacji odrębnie, można użyć następujących tagów:
  - **%{n}** – common name certyfikatu np. "Jan Maria Kowalski",
  - **%{c}** – typ certyfikatu np. "Certyfikat kwalifikowany",
  - **%{Y}** - bieżąca data, rok w formacie YYYY, np. 2022,
  - **%{M}** - bieżąca data, miesiąc w formacie MM, np. 06,
  - **%{D}** - bieżąca data, dzień w formacie DD, np. 08,
  - **%{h}** - bieżący czas lokalny, godzina w formacie hh, np. 12,
  - **%{m}** - bieżący czas lokalny, minuta w formacie mm, np. 00,

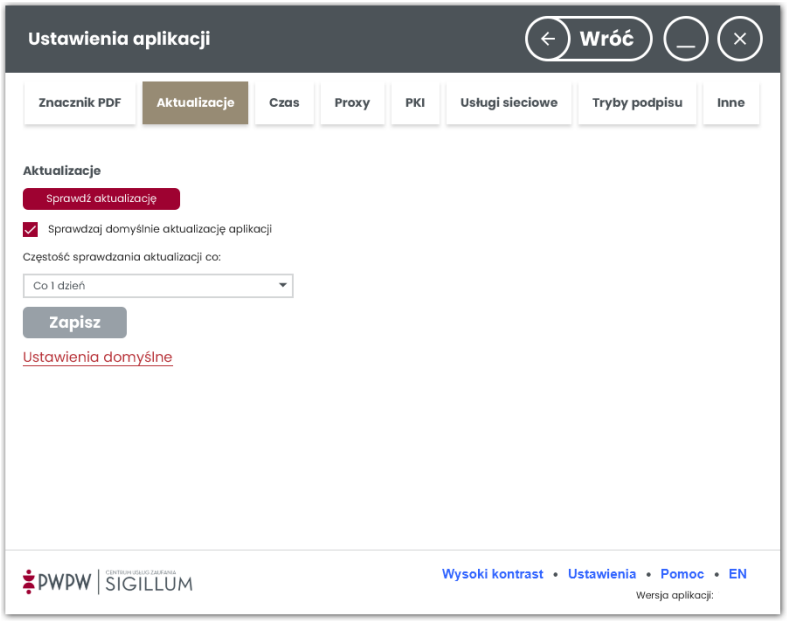
- **%{s}** - bieżący czas lokalny, sekunda w formacie ss, np. 00,
- **%{z}** - bieżący czas lokalny, przesunięcie względem czasu UTC w formacie [+/-]hh:mm, np. +02:00.

Domyślnie proponowana treść w polu Szablon dla polskiej wersji językowej aplikacji to: "Podpisane elektronicznie przez %{n} (%{c}) w dniu %{Y}-%{M}-%{D}."

System umożliwia umieszczenie elementu graficznego podpisu na dowolnej stronie dokumentu, zgodnie z wolą Użytkownika.

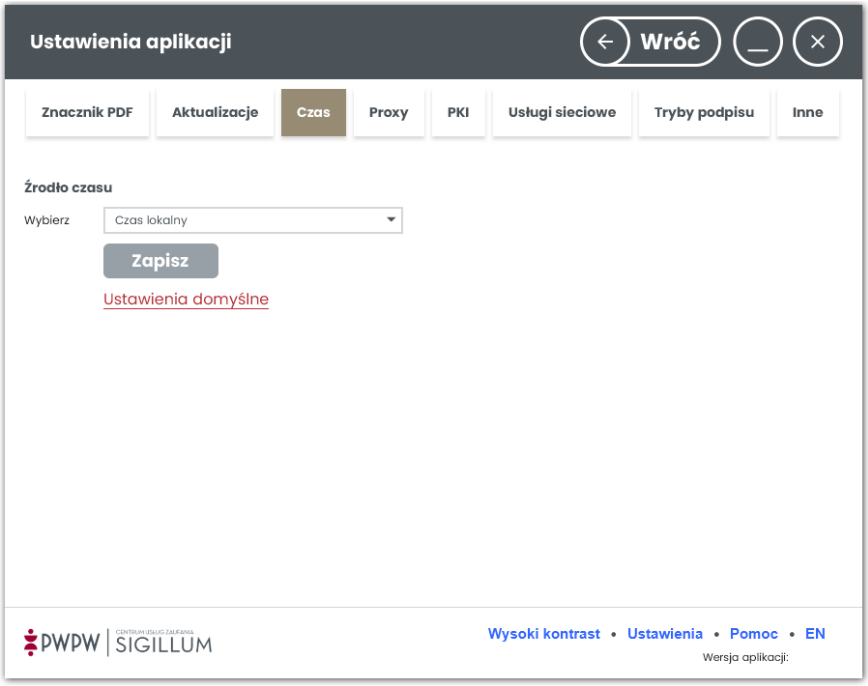
Szczegółowy opis składania podpisu na dokumentach PDF z użyciem elementu graficznego podpisu opisany został w punkcie 7.1.5 niniejszej instrukcji.

6.5.2 Aktualizacje



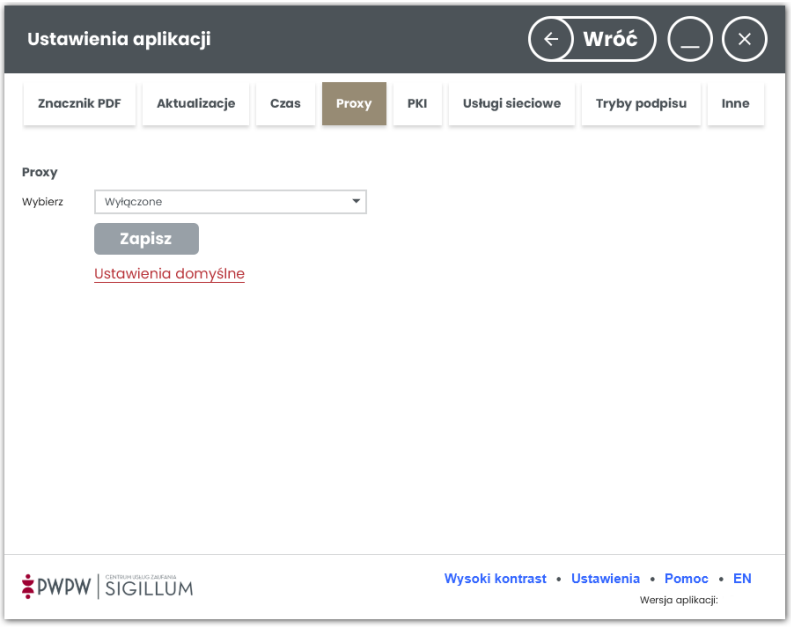
W zakładce ***Aktualizacje*** można sprawdzić aktualizacje klikając przycisk **Sprawdź aktualizacje**, można też zaznaczyć opcję ***Sprawdzaj aktualizacje automatycznie***, by aplikacja sprawdzała dostępność nowej wersji cyklicznie. Przy zaznaczonej opcji ***Sprawdzaj aktualizacje automatycznie*** użytkownik może wskazać częstotliwość sprawdzania (1, 2, 7, 14, 31 dni). Jeśli aktualizacja zostanie znaleziona, zostanie wyświetlony komunikat po uruchomieniu aplikacji.

6.5.3 Czas



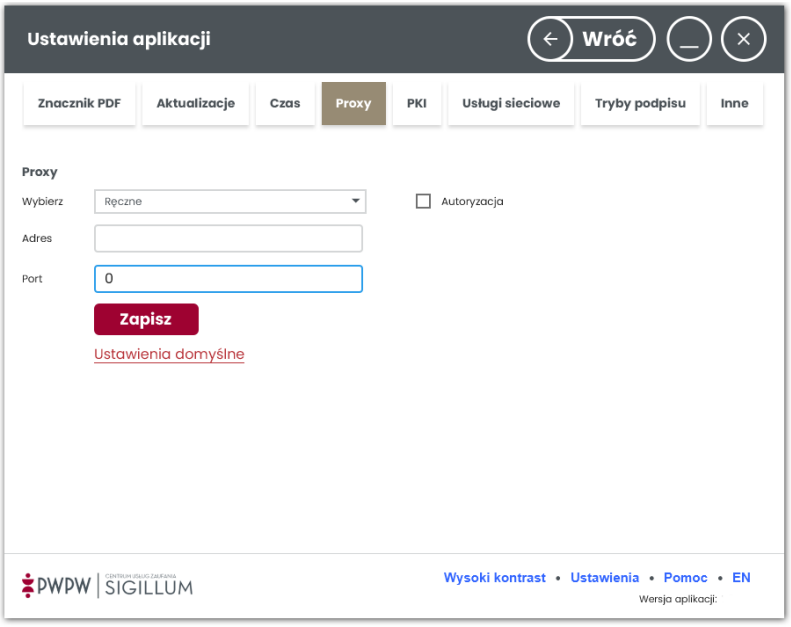
W zakładce ustawień źródła czasu aplikacji można wybrać między czasem lokalnym (komputer), a źródłem czasu NTP (dedykowany serwer czasu). Wskazanie dedykowanego serwera czasu jest możliwie z poziomu zakładki ***Usługi sieciowe / Serwery NTP***.

6.5.4 Proxy



Zakładka ***Proxy*** domyślnie posiada pole ***Proxy*** ustawione na wartość Wyłączone.

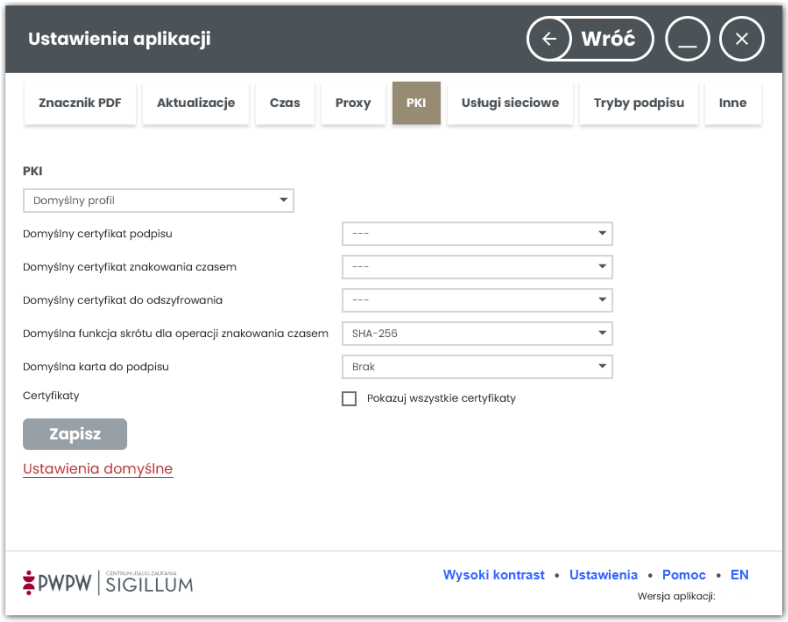
Po wyborze w polu ***Proxy*** wartości ***Ręczne***, wyświetlone zostaną szczegóły konfiguracji.



Należy uzupełnić pola ***Adres, Port***, które dotyczą serwera proxy.

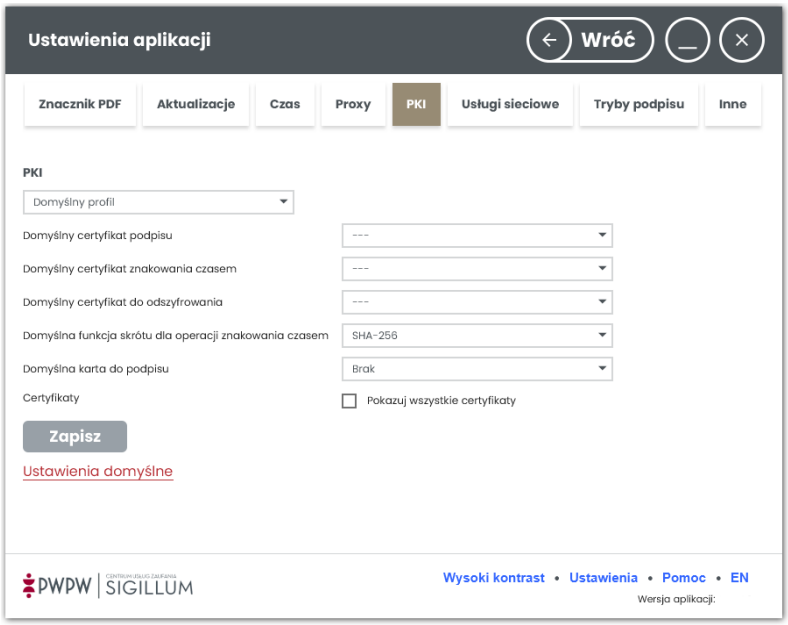
Jeśli dodatkowo serwer proxy wymaga autoryzacji, wówczas należy zaznaczyć checkbox ***Autoryzacja*** oraz wypełnić pola: ***Użytkownik, Hasło, Domena*** oraz wybrać typ autentykacji (BASIC lub NTLM). Jeśli zaznaczone zostanie pole ***Autoryzacja podczas startu***, przy uruchamianiu aplikacji trzeba będzie podać dane autoryzacyjne do serwera proxy.

6.5.5 PKI



Z uwagi na mnogość opcji zakładka ***PKI*** posiada własne menu (lista rozwijalna PKI), w skład którego wchodzą następujące opcje: ***Domyślny profil***, ***Profil podpisu***, ***Domyślny algorytm***, ***Polityka certyfikacji***.

6.5.5.1 Domyślny profil



Po wybraniu opcji ***Domyślny profil,*** istnieje możliwość wskazania domyślnych certyfikatów dla operacji:

- podpisu,
- znakowania czasem,

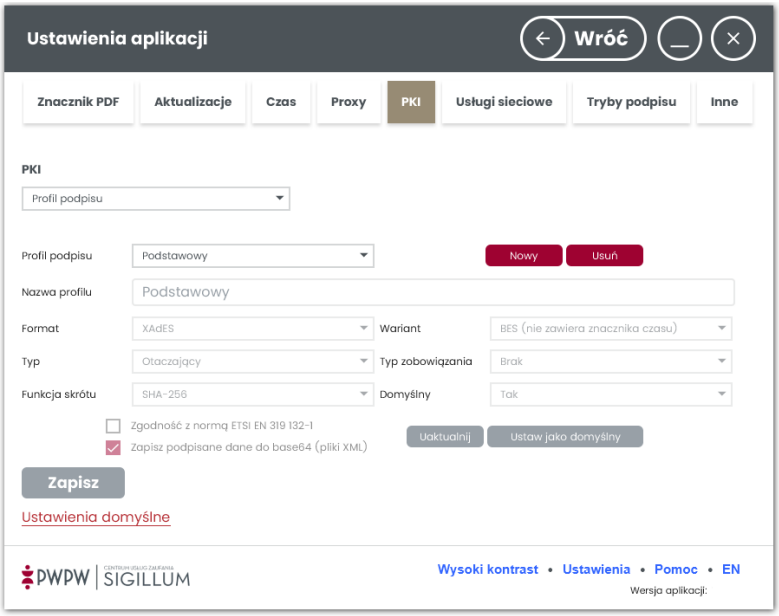
- odszyfrowania,

, oraz wyboru:

- domyślnej funkcji skrótu dla operacji znakowania czasem,
- domyślnej karty do podpisu,

Pokazuj wszystkie certyfikaty - jeśli opcja jest zaznaczona, wszystkie certyfikaty przy pomocy których można wykonać daną operację, są wyświetlane na liście wyboru certyfikatu. Jeśli opcja jest odznaczona na liście do wyboru certyfikatu pojawią się tylko te certyfikaty, dla których dostępny jest certyfikat CA. Certyfikaty CA pobierane są wyłącznie z listy TSL lub z keystore aplikacji.

6.5.5.2 Profil podpisu



Zakładka ***Profil podpisu*** służy do przygotowania dedykowanych profili użytkownika.

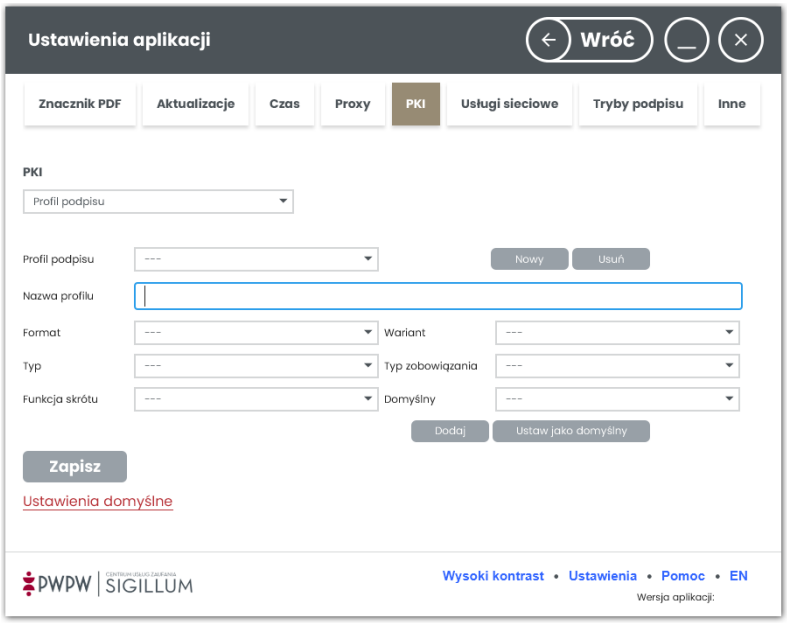
Profile są wykorzystane przy podpisywaniu plików. Dzięki ustawieniu profilu, użytkownik nie musi za każdym razem określać *Formatu, Wariantu, Typu, Funkcji skrótu i Typu zobowiązania* w trakcie procesu podpisywania. Te ustawienia przechowywane są w profilu.

W ustawieniach można zarządzać profilami podpisu (dodawać, edytować, usuwać).

Aby stworzyć własny profil należy:

1. Wybrać opcję ***Nowy***

2. Odblokowane zostaną pola do stworzenia nowego profilu



3. Po dodaniu nazwy profilu należy ustawić szczegóły profilu, które dotyczą pól:
   - *Nazwa profilu* – nazwa, pod jaką prezentowany będzie profil podczas podpisu,
   - *Format* – do wyboru: XAdES,, PAdES, CAdES, ASiCE, ASiCS,
   - *Wariant* – do wyboru w zależności od wskazanego wcześniej *Formatu* (BES, T),
   - *Typ* – do wyboru w zależności od wskazanego wcześniej *Formatu* (*Otoczony, Otaczający, Zewnętrzny*),
   - *Typ zobowiązania* – opcja dostępna dla wszystkich formatów,
   - *Zgodność z normą ETSI EN 319 132-1* – opcję można włączyć, jeśli wybrano *Format* XAdES,
   - *Zapisz podpisane dane do base64 (pliki XML)* - opcja dostępna tylko dla XAdES Otaczający.
4. Formaty podpisu
   - XAdES – najpopularniejszy i najnowszy format podpisu (oparty o język XML), znajdujący najszersze zastosowanie.
   - PAdES – format umożliwiający składanie i prezentację podpisu na dokumentach PDF.
   - CAdES – format stanowiący rozwinięcie formatu CMS.
   - ASiCS – tworzy strukturę kontenera pliku podpisywanego oraz podpisu
   - ASiCE – tworzy rozszerzoną strukturę kontenera pliku podpisywanego oraz podpisu
5. Warianty podpisu

- BES – podstawowy wariant podpisu,
- T – w tym wariancie do podpisu dołączany jest znacznik czasu, który przechowuje informacje o dacie złożenia podpisu elektronicznego.

W aplikacji możliwe jest zastosowanie możliwych wariantów:

- dla XAdES: BES, T,
- dla PAdES: BES, T,
- dla CAdES: BES, T,
- dla ASiCE, ASiCS: BES, T.

Wyjątkiem jest profil "Podpis długoterminowy", który dla każdego z formatów ustawia wariant A oraz "Podpis rozszerzony", który dla każdego z formatów ustawia wariant XL.

6. Typ
   - Zewnętrzny – oddzielne pliki dla dokumentu i podpisu. W takim przypadku przy weryfikacji należy dysponować wszystkimi plikami.
   - Otoczony – struktura podpisu jest dołączona do dokumentu. Wówczas plik z podpisem zawiera treść dokumentu oraz podpis.
   - Otaczający – Struktura podpisu zawiera dokument, który uległ podpisaniu.

   W aplikacji możliwe jest zastosowanie ustawień dla poniższych typów:

   - dla XAdES: Zewnętrzny, Otaczający, Otoczony,
   - dla PAdES: Otoczony,
   - dla CAdES: Zewnętrzny, Otaczający,
   - dla ASiCE, ASiCS: Otoczony.

7. Typ zobowiązania – z listy rozwijalnej użytkownik może wybrać typ zobowiązania, dla jakiego tworzony jest podpis. Dostępne są wartości:
   - Dowód pochodzenia
   - Potwierdzenie odbioru
   - Dowód dostawy
   - Dowód nadawcy
   - Formalne potwierdzenie

- Potwierdzenie utworzenia

W aplikacji możliwe jest zastosowanie każdego z wymienionych zobowiązań dla każdego *Formatu* podpisu.

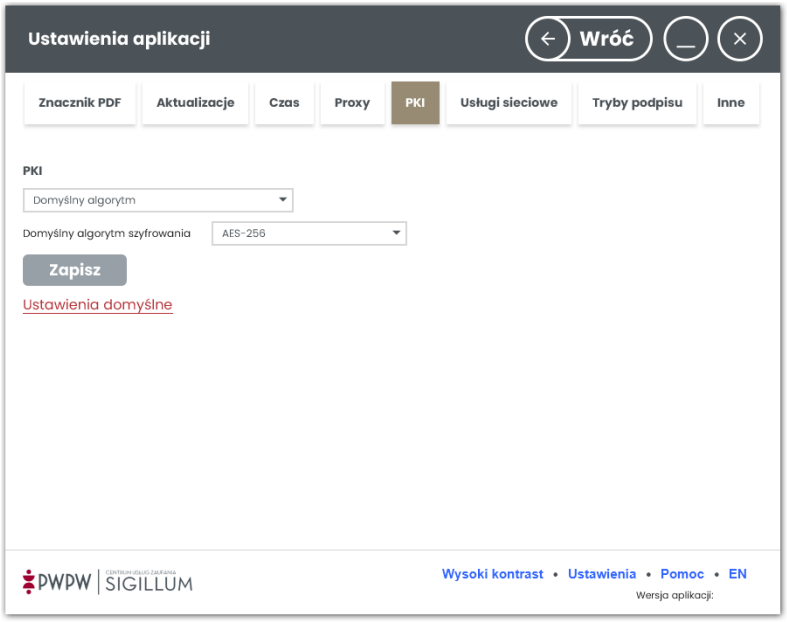
8. Funkcja skrótu
   - SHA-256 – następca SHA-1. Rozmiar skrótu to maks. 256 bitów.
   - SHA-384 – następca SHA-1. Rozmiar skrótu to maks. 384 bity.
   - SHA-512 – następca SHA-1. Rozmiar skrótu to mak. 512 bitów.

W aplikacji możliwe jest zastosowanie każdej z wymienionych *Funkcji skrótu* dla każdego *Formatu* podpisu.

Po uzupełnieniu wymaganych danych, należy użyć przycisku „Dodaj" a następnie kliknąć przycisk „Zapisz" by zapisać dany profil podpisu.

By stworzony profil podpisu był podpisem domyślnym, należy użyć przycisku *„Ustaw jako domyślny"* a następnie również użyć przycisku „Zapisz" do zapisania dokonanego wyboru.

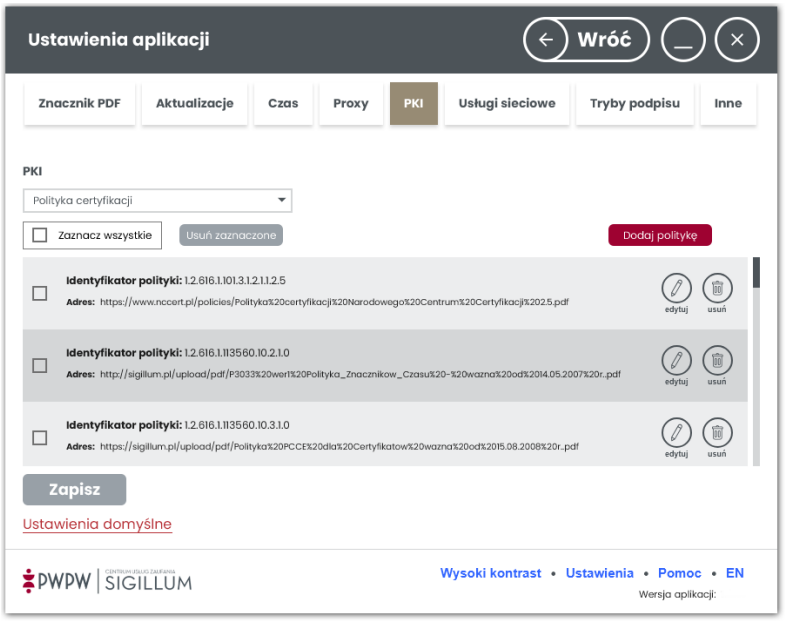
6.5.5.3 Domyślny algorytm (szyfrowania)



Użytkownik z listy rozwijalnej wybiera typ algorytmu:

- DES – algorytm szyfrujący z blokami o długości 64 bitów. Najstarszy typ spośród dostępnych,
- 3DES – nowszy niż DES. Wykorzystuje do szyfrowania i deszyfrowania trzy klucze,
- AES-128 – nowszy standard szyfrowania. Szyfruje kluczem o długości 128 bitów,
- AES-256 – domyślny, szyfruje kluczem o długości 256 bitów.

6.5.5.4 Polityka certyfikacji

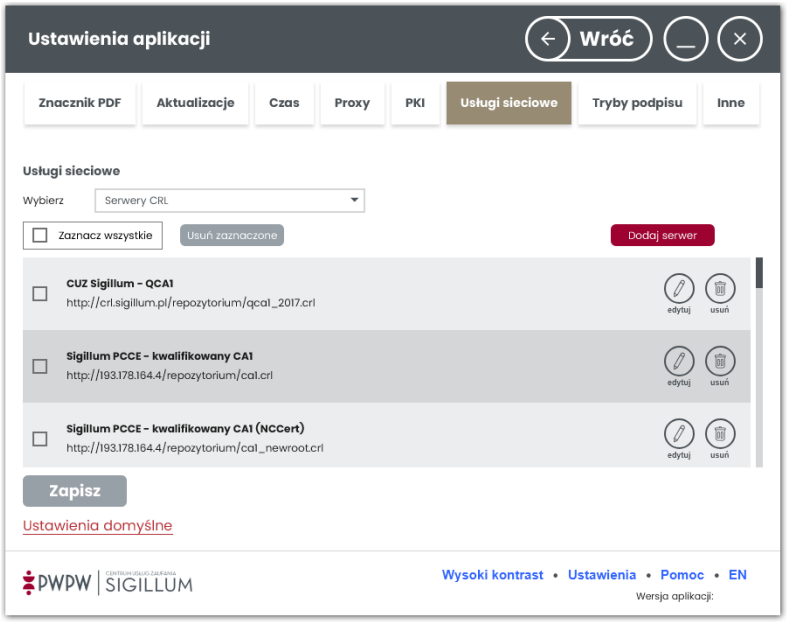


W zakładce ***Polityka certyfikacji*** wyświetlane są nazwy Polityki certyfikacji oraz ich adresy.

Dostępne akcje:

- przycisk **Dodaj politykę** – otwiera się okno dodania serwera,
- ikona kosza (Usuń) – powoduje usunięcie serwera z listy,
- ikona ołówka (Edytuj) – otwiera się okno edycji danych serwera.

6.5.6 Usługi sieciowe



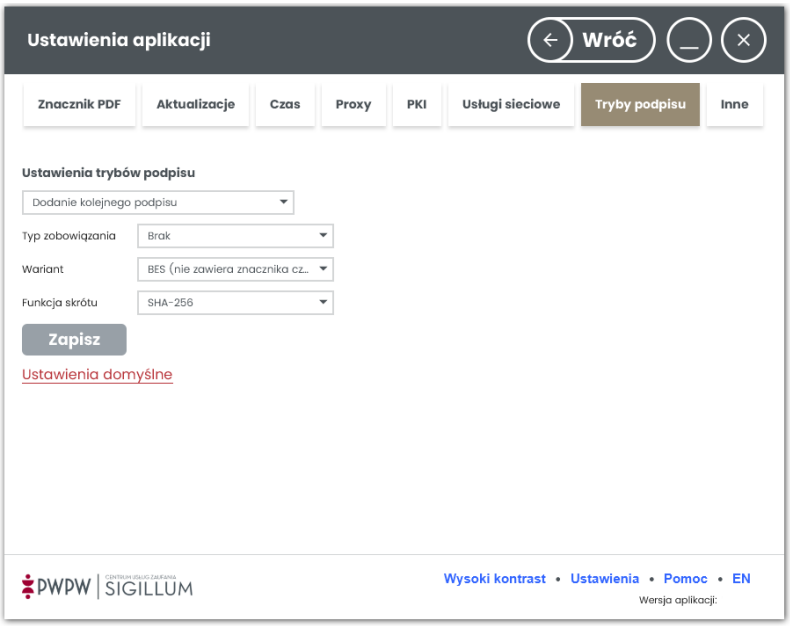
Menu tej zakładki umożliwia zarządzanie serwerami:

1. CRL – lista unieważnionych i zawieszonych certyfikatów. Publikowana przez wystawcę certyfikatów.
2. TSP – protokół kryptograficzny poświadczający znaczniki czasu przy użyciu certyfikatów X.509. Usługa znakowania czasem. Możliwa jest konfiguracja serwera TSP: bez autoryzacji, z podpisem żądania o znacznik czasu oraz z loginem i hasłem.
3. NTP – protokół komunikacyjny umożliwiający precyzyjną synchronizację czasu pomiędzy komputerami. Wzorcowy czas UTC może pochodzić bezpośrednio z zegarów atomowych lub pośrednio ze specjalizowanych serwerów czasu.

Aplikacja potrzebuje dostępu do list CRL lub usługi OCSP, dostępu do list TSL, aby móc weryfikować certyfikat używany do podpisywania.

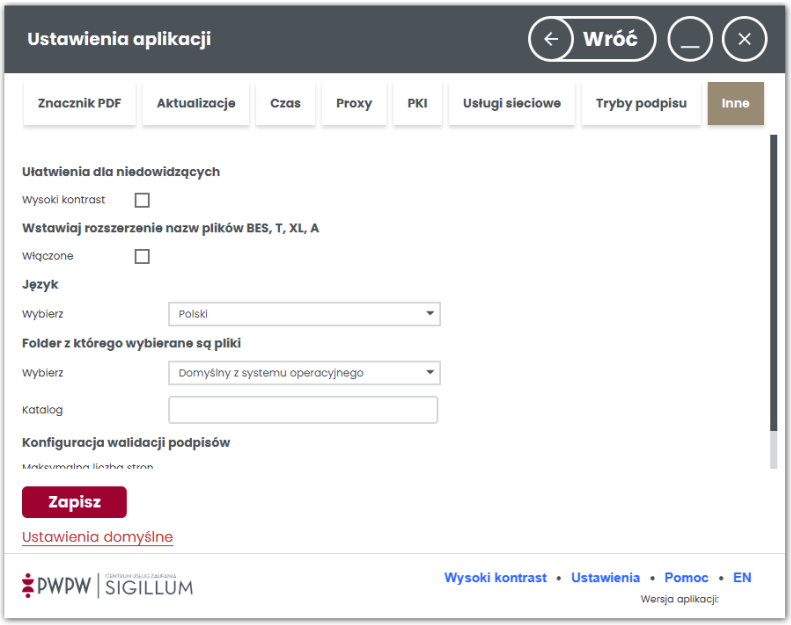
Brak dostępu jest komunikowany przy składaniu oraz weryfikacji podpisu.

6.5.7 Tryby podpisu



Menu zakładki umożliwia zarządzanie domyślnymi ustawieniami Typu zobowiązania, Wariantu i Funkcji skrótu dla kolejnego podpisu oraz kontrasygnaty.

6.5.8 Inne



Zaznaczenie opcji ***Wysoki kontrast*** i zapis konfiguracji spowodują, że domyślnie aplikacja będzie uruchamiana w wysokim kontraście. Jeśli checkbox ***Wstawiaj rozszerzenie nazw***

plików BES,T,XL,A jest zaznaczony, w nazwach plików podpisanych będzie wstawiany znacznik BES, T, XL, A.

Wybór języka następuje przy użyciu listy rozwijalnej w sekcji ***Język***.

Przełączenie języka nastąpi dopiero po wybraniu opcji i zapisie ustawień.

Wybór folderu polega na wybraniu jednej z trzech opcji:

- Domyślny z systemu operacyjnego – okno wyboru plików będzie otwierane na folderze ustawionym, jako domyślny w systemie operacyjnym,
- Wybrany folder – po kliknięciu w pole Katalog można wybrać dowolny folder,
- Ostatnio wybrany – aplikacja będzie pamiętać ostatnio otwierany folder.

Parametr **Maksymalna liczba stron do analizy graficznej w podpisach PAdES** określa liczbę stron poniżej której, podczas walidacji podpisów w formacie PAdES jest dodatkowo przeprowadzana weryfikacja różnic wizualnych na wersji dokumentu z przed podpisu względem tych z podpisem. Ze względu na fakt, że takie porównanie jest dość czasochłonne wyższe wartości mogą powodować znaczące spowolnienie działania aplikacji w przypadku podpisów PAdES.

6.5.9 Ustawienie braku ograniczeń dla rozmiaru plików

Istnieje możliwość zmiany wartości parametru ***LimitWielkosciPliku*** w pliku konfiguracji aplikacji. Po zmianie wartości parametru na false, aplikacja nie będzie sprawdzała rozmiaru pliku podczas operacji podpisu oraz weryfikacji. Istnieje ryzyko, że przy dużym pliku oraz niewystarczających zasobach komputera, aplikacja może się zawiesić w trakcie operacji podpisu czy weryfikacji.

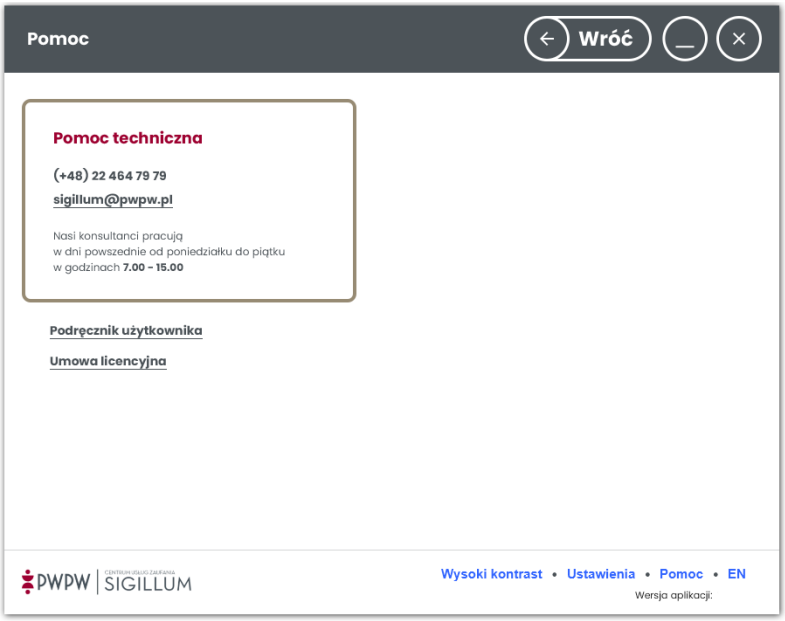
Żeby zmienić wartość parametru ***LimitWielkosciPliku*** należy:

- odszukać plik C:\Users\<nazwa_użytkownika>\sigillumApp**configuration.xml**,
- edytować plik i odszukać tag: <LimitWielkosciPliku>**true**</LimitWielkosciPliku>,
- zmienić wartość na **false**, zapisać zmiany oraz zrestartować aplikację.

Przy wyłączonym parametrze, po dodaniu pliku do podpisu na obszar roboczy status „za duży rozmiar" (wyświetlany przy włączonym parametrze wg tabeli ROZMIAR) nie będzie się już wyświetlał.

6.6 Pomoc

Po kliknięciu w link pomocy na dole w pasku aplikacji, prezentowane jest poniższe okno:



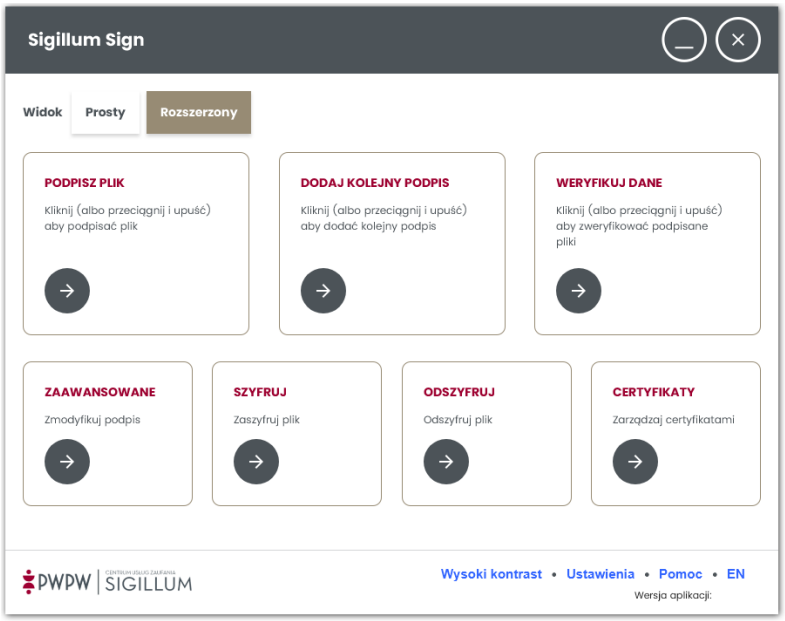
Pomoc techniczna – informacje dotyczące możliwych form kontaktu.

Instrukcja – dostęp do informacji, dostępnych w tym materiale.

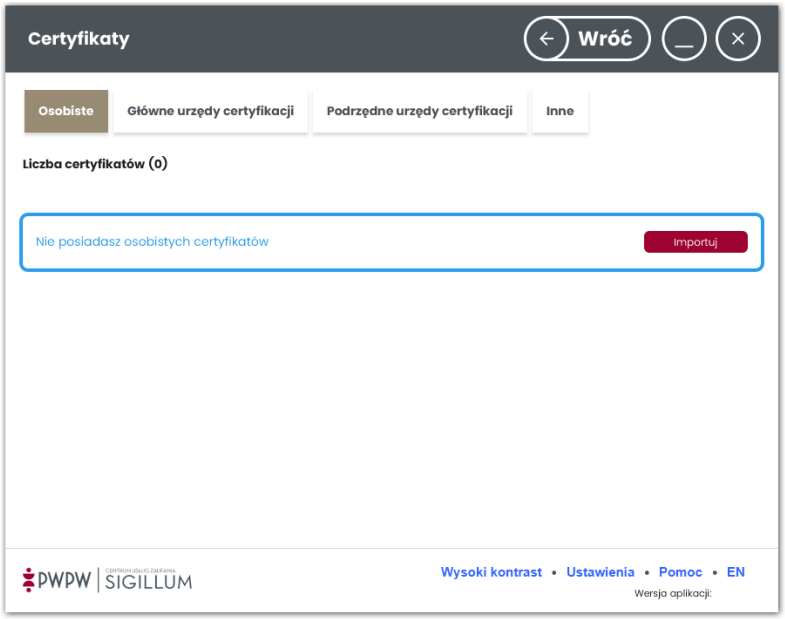
Umowa licencyjna – możliwość zaprezentowania użytkownikowi treści umowy licencyjnej.

6.7 Certyfikaty

Opcja ta umożliwia zarządzanie certyfikatami wykorzystywanymi przez aplikację.



Po kliknięciu na ekranie głównym przycisku ***Rozszerzony*** a następnie kafelka „Certyfikaty", aplikacja prezentuje następujący widok:



Zawiera on listę certyfikatów, które są wykorzystywane przy realizacji funkcji podpisu oraz szyfrowania przez aplikację.

Lista certyfikatów podzielona jest na zakładki:

Osobiste – zawiera listę certyfikatów wraz z kluczami prywatnymi. Wykorzystywane one mogę być przy realizacji funkcji składania podpisu oraz odszyfrowania danych

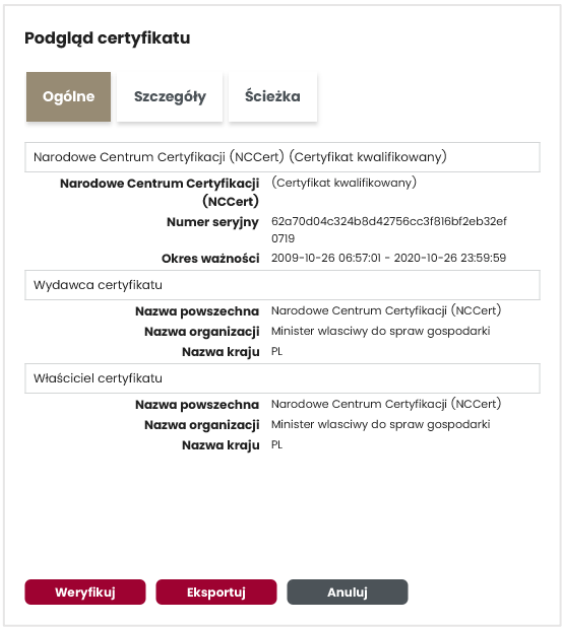
Główne urzędy certyfikacji – zawiera listę głównych urzędów certyfikacji.

Podrzędne urzędy certyfikacji – zawiera listę podrzędnych wobec RootCA urzędów certyfikacji.

Inne – zawiera listę certyfikatów osób, do których możemy szyfrować dane.

Zarządzanie listą certyfikatów jest niezwykle proste. Dostępne są opcje:

1. przycisk **Importuj** – umożliwia dodanie do magazynu certyfikatów aplikacji plik z certyfikatem (postaci pliku crt lub pkcs12),
2. ikona kosza **(Usuń)** – umożliwia usunięcie wybranego certyfikatu z magazynu certyfikatów aplikacji,
3. ikona i **(Podgląd certyfikatu)** – umożliwia podgląd szczegółów certyfikatu.



Na ekranie podglądu certyfikatu dostępne są opcje:

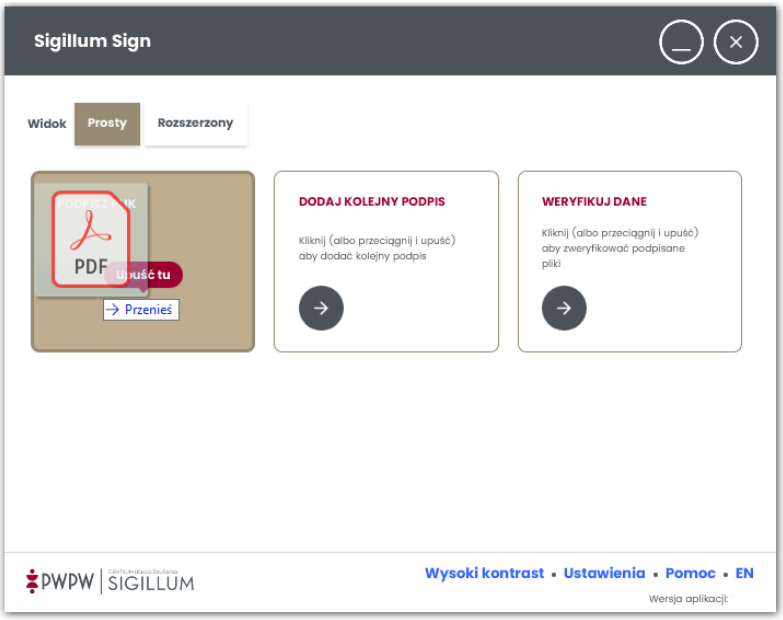
- przycisk **Weryfikuj** – weryfikuje certyfikat,
- przycisk **Eksportuj** – eksportuje certyfikat w postaci pliku *.cer,
- przycisk **Anuluj** – zamyka okno podglądu certyfikatu.

7 Operacje PKI

7.1 Składanie podpisu

7.1.1 Ekran startowy procesu podpisu

Wywołanie operacji **„Podpisz”** ze strony głównej widoku prostego odbywać się może poprzez akcję kliknięcia kafelka, lub akcję *Przeciągnij i upuść* wybrane pliki w obszarze.



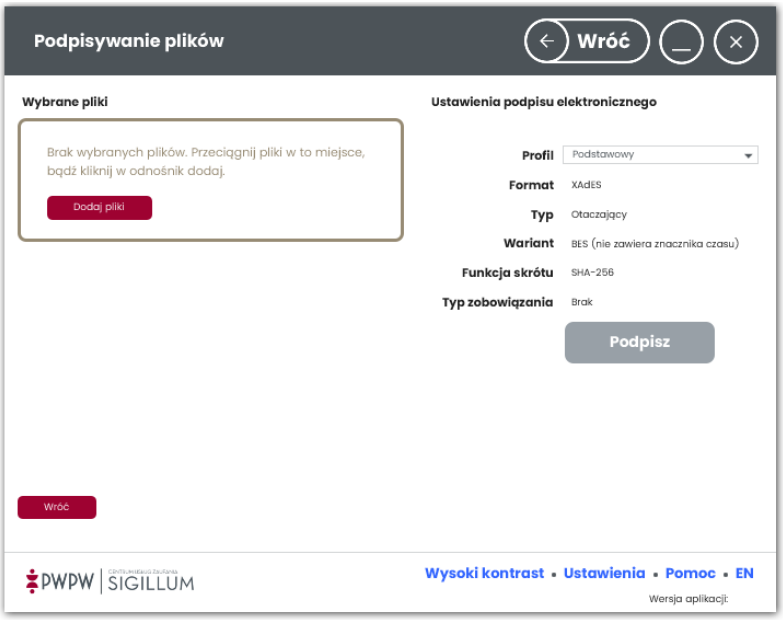
UWAGA!

W zależności od wersji aplikacji, wybranego formatu podpisu oraz od rozszerzenia pliku dozwolony jest określony rozmiar podpisywanego pliku.

Format podpisu	Dozwolony rozmiar pliku	
	wersja 64-bitowa	wersja 32-bitowa
XAdES otaczający, otoczony	100MB	40MB
XAdES zewnętrzny	bez limitu (wariant A - 100MB)	bez limitu (wariant A - 40MB)
PAdES otoczony	320MB	40MB
CAdES otaczający	320MB (pliki XML 150MB)	40MB
CAdES zewnętrzny	bez limitu (wariant A - 320MB)	bez limitu (wariant A - 40MB)
ASiCS otoczony	320MB (pliki XML 150MB)	40MB
ASiCE otoczony	sumaryczny rozmiar plików: 320MB	sumaryczny rozmiar plików: 40MB

7.1.2 Ekran składania podpisu i ustawień podpisu

Po wyborze opcji Podpisz plik lub przeciągnięciu plików na obszar, użytkownikowi prezentowany jest poniższy widok tj. Ekran składania podpisu elektronicznego.



Ekran podzielony jest na dwie części: większą, lewą tzw. obszar roboczy, w którym prezentowane są pliki oraz prawą tzw. obszar ustawień, zawierający ustawienia związane z podpisem oraz przycisk ***„Podpisz”***.

Zarządzanie plikami w obszarze roboczym odbywa się przez użycie ikon w wierszu każdego pliku dodanego w obszarze roboczym.

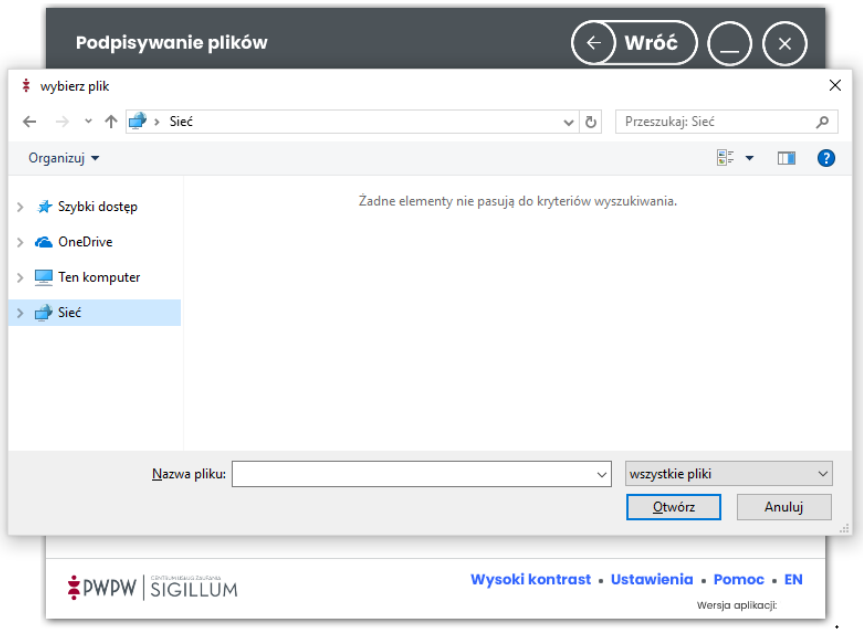
UWAGA!

Istnieje możliwość podpisu wielu plików. W tym celu użytkownik powinien dodać oraz zaznaczyć odpowiednie pliki znajdujące się w obszarze roboczym. Po użyciu przycisku *„Podpisz”*, aplikacja podpisuje wszystkie zaznaczone pliki, jednokrotnie pytając o hasło/pin (z wyjątkiem czytników z pin padem).

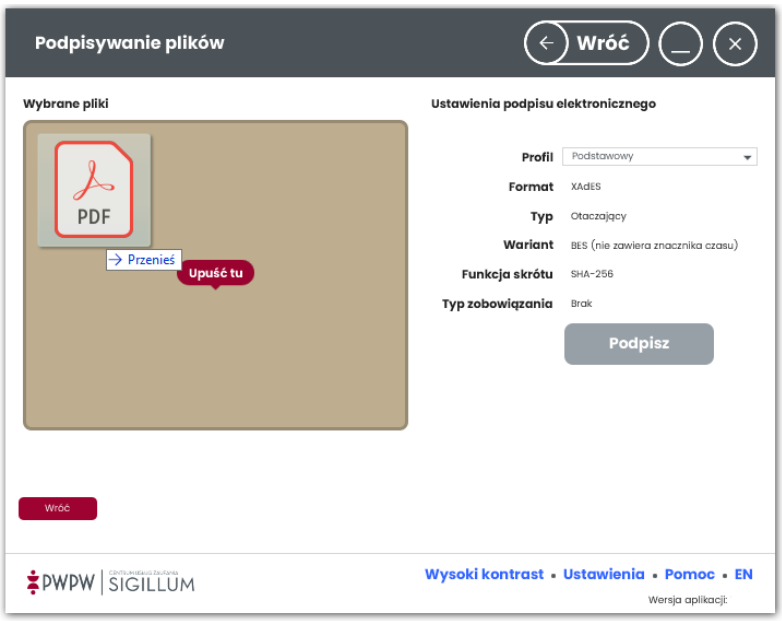
7.1.3 Dodanie plików do obszaru roboczego

Aby podpisać pliki, użytkownik musi dodać pliki do obszaru roboczego. Dodanie pliku/plików może odbyć się na dwa sposoby: przez użycie przycisku **Dodaj pliki** lub funkcję *przeciągnij-upuść*.

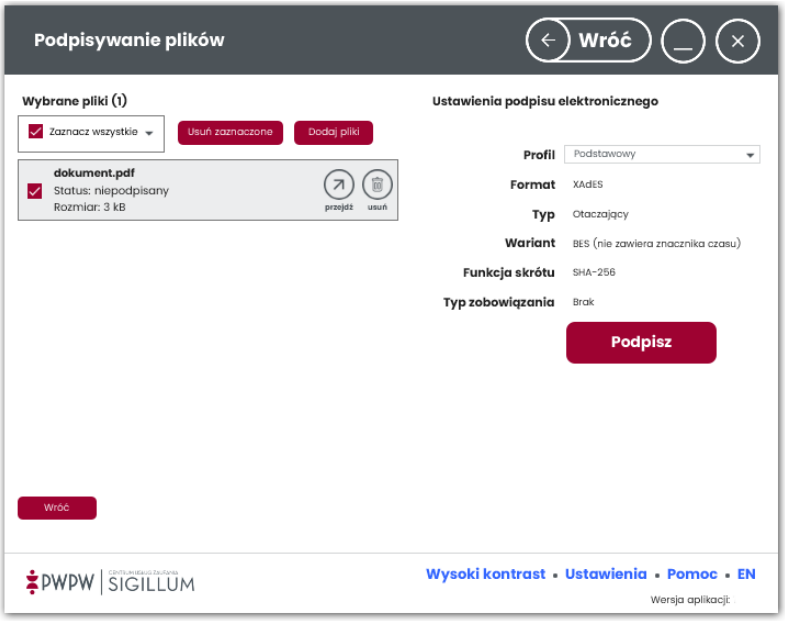
Po kliknięciu opcji ***Dodaj pliki*** pojawi się okno przeglądania zawartości stacji roboczej użytkownika pozwalające wybrać pliki do podpisu.



Dodanie plików do obszaru roboczego może odbywać się również przy użyciu funkcji *przeciągnij i upuść*.



Po wywołaniu opcji dodawania plików do obszaru roboczego, pliki prezentowane są w formie kafelków wraz z danymi je opisującymi.



Kafelki zawierają następujące informacje:

Nazwa dokumentu, Status oraz rozmiar.

Możliwe statusy dodanego pliku to: podpisany, niepodpisany, za duży rozmiar.

Rozszerzenie pliku	Status dodanego pliku „za duży rozmiar" występuje dla plików o rozmiarze:	
	wersja 64-bitowa	wersja 32-bitowa
XML	ponad 150MB	ponad 50MB
Pozostałe	ponad 350MB	ponad 50MB

Po kliknięciu w ikonę ***przejdź*** plik otwierany jest w domyślnej dla rozszerzenia pliku aplikacji.

Kliknięcie w ikonę ***usuń*** umożliwia usunięcie pliku z obszaru roboczego.

Pliki dodane do obszaru roboczego są domyślnie zaznaczone, co prezentowane jest w formie zaznaczonego checkboxa w kafelku pliku. Kliknięcie w checkbox odznacza go.

Konkretne operacje PKI odbywają się tylko na zaznaczonych elementach.

Przy pomocy checkboxa „Zaznacz wszystkie" można zaznaczyć/odznaczyć wszystkie dodane pliki.

Nad listą dodanych plików wyświetlane jest podsumowanie w postaci: **Wybrane pliki (2)**.

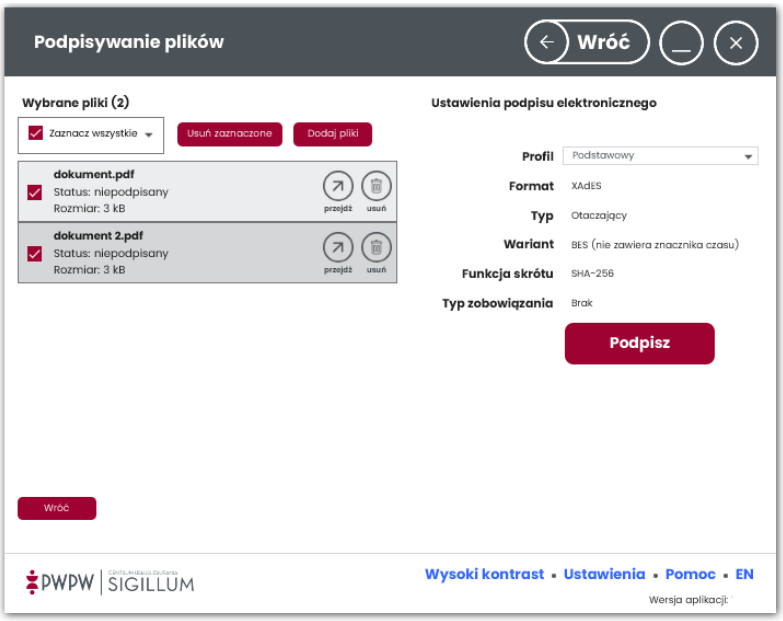
Po prawej stronie ekranu, w obszarze ustawień podpisu użytkownik może wybrać profil podpisu.

Profile podpisu podzielić można na domyślne (nieedytowalne) oraz te, które użytkownik może samodzielnie definiować.

Użytkownik ma również możliwość zdefiniowania domyślnych ustawień profilu w Ustawieniach.

Ustawienia te zostały opisane szerzej w punkcie 6.5.5.2 opisującym definiowanie Ustawień (Ustawienia/Ustawienia PKI/Profil podpisu).

Wybór profilu Użytkownika pozwala ustawić *Format, Typ, Wariant, Funkcję skrótu* oraz *Typ zobowiązania*.



Po zaznaczeniu wybranych dokumentów do podpisu oraz określeniu właściwego profilu podpisu należy kliknąć przycisk **„Podpisz"**.

Jeśli użytkownik wybierze **Profil użytkownika** a następnie jeden z **Formatów** XAdES, CAdES, ASiC-E lub ASiC-S, pliki zostaną podpisane a na końcu wyświetlony zostanie status podpisu. Jeśli zostanie wybrany **Format** PAdES, użytkownik ma możliwość wstawienia elementu graficznego podpisu na dokumencie PDF (np. zawierającego logo firmy) co zostało opisane szerzej w rozdziale 7.1.5

7.1.4 Ekran wyboru certyfikatów i złożenie podpisu

Po wyborze opcji ***„Podpisz"*** użytkownik przeniesiony zostaje do ekranu wyboru karty i certyfikatów, wprowadzenia kodu PIN oraz informacji o złożeniu podpisu.

Ekran widoczny na ekranie poniżej uniemożliwia wprowadzanie zmian w widokach poprzednich. (Ewentualna zmiana w poprzednich widokach możliwa jest przez użycia przycisku *„Wróć"*).

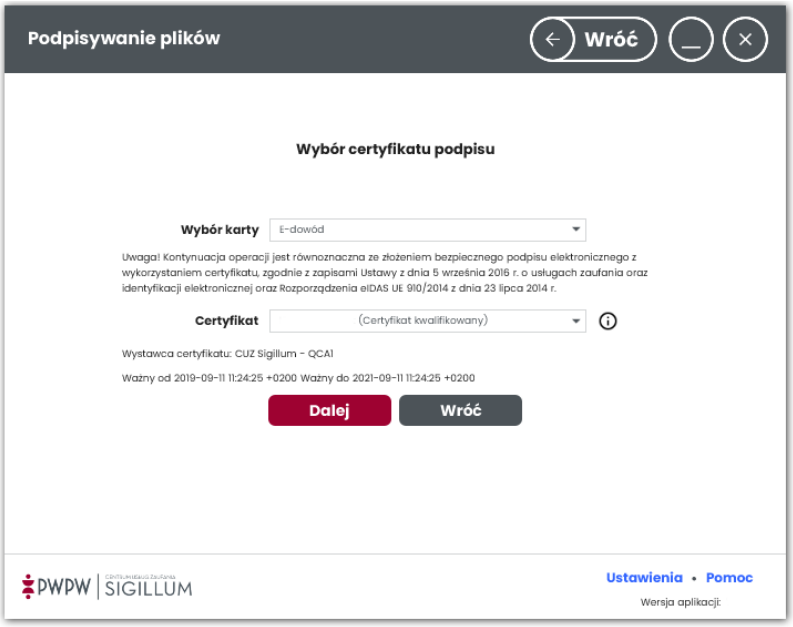
System prezentuje karty i certyfikaty, przy użyciu których będzie można podpisać zaznaczone plik/ki. Użytkownik ma możliwość zmiany ustawień zakresu dostępnych certyfikatów (6.5.5.1).

Wybór karty to wskazanie biblioteki pkcs11 umieszczonej w określonej lokalizacji. Jeśli biblioteki nie ma w określonej lokalizacji, wyświetlone zostaje okno wyboru pliku. Po wskazaniu poprawnego pliku pkcs11 do listy wyboru karty zostaje dodana nowa pozycja.

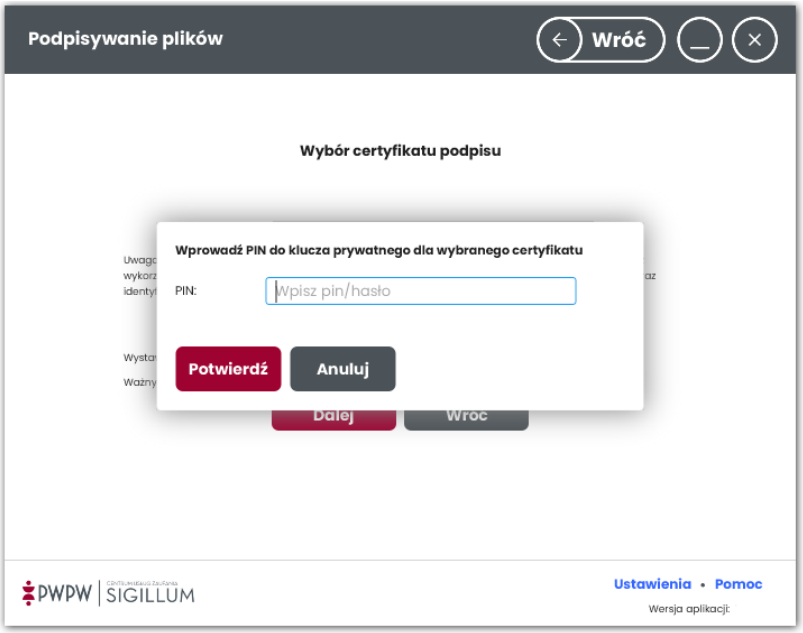
Po wczytaniu, dostępne karty i certyfikaty można wybrać i wskazać z listy rozwijalnej.
Użytkownik powinien wskazać certyfikaty służące do podpisu i/lub ewentualnie do znakowania czasem.

W przypadku, gdy użytkownik wybrał opcję znakowania czasem tj. wariant podpisu -T, wówczas należy też wskazać certyfikat znakowania czasem.

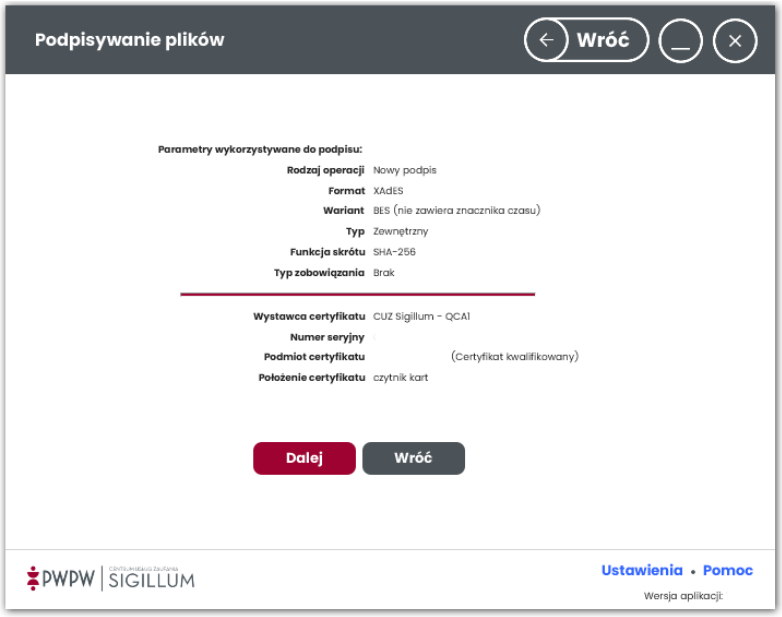
Po wyborze karty i certyfikatu, pojawia się informacja na temat certyfikatu i skutku prawnego wywołanego jego użyciem.



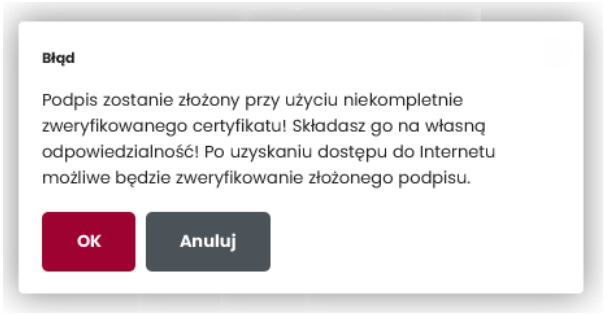
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny. Po kliknięciu „**Dalej**” system otwiera okno wprowadzenia kodu PIN.



Po wpisaniu poprawnego kodu PIN i kliknięciu **Potwierdź**, system prezentuje ekran parametrów wykorzystanych do wykonania podpisu.



W przypadku, gdy aplikacja nie ma dostępu do Internetu wyświetlane jest okno z komunikatem o braku możliwości wykonania kompletnej weryfikacji użytego certyfikatu.



Kliknięcie przycisku OK zamyka okno komunikatu, prezentowany jest ekran końcowy jak poniżej.

W kolumnie „Status" wyświetlany jest status otrzymany po wykonaniu operacji, w wierszu każdego podpisanego pliku znajdują się ikony:

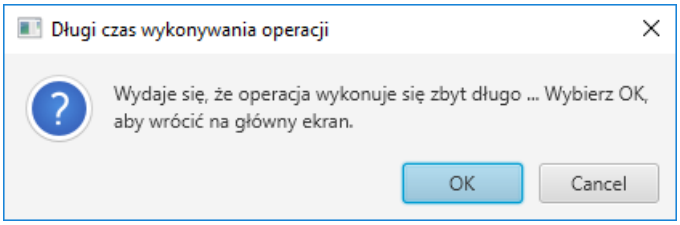
- przejdź – prezentacja (niepodpisanego) pliku źródłowego podpisu,
- pobierz – zapisanie (niepodpisanego) pliku źródłowego podpisu,
- info – szczegóły złożonego podpisu.

Po zaznaczeniu checkboxa w wierszu wybranych plików można wysłać podpisane dokumenty poprzez e-mail klikając przycisk ***Wyślij (e-mailem)***.

Po kliknięciu przycisku ***Weryfikuj*** wyświetlany jest ekran weryfikacji podpisanych plików. Przycisk ***Pobierz pliki*** pozwala zapisać wszystkie zaznaczone pliki.

Potwierdzenie (OK) kończy proces podpisywania. Podpisane pliki odnaleźć można w folderach, gdzie znajdują się pliki źródłowe. Podpis można zweryfikować w procesie weryfikacji.

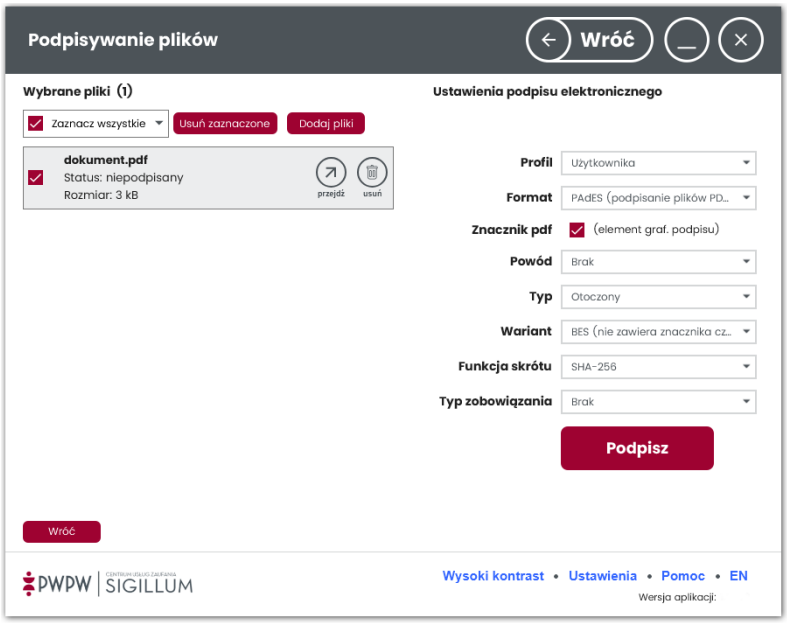
Jeśli jednocześnie podpisywanych jest wiele plików, w trakcie podpisywania może pojawić się okno informujące o długim czasie wykonywania operacji.



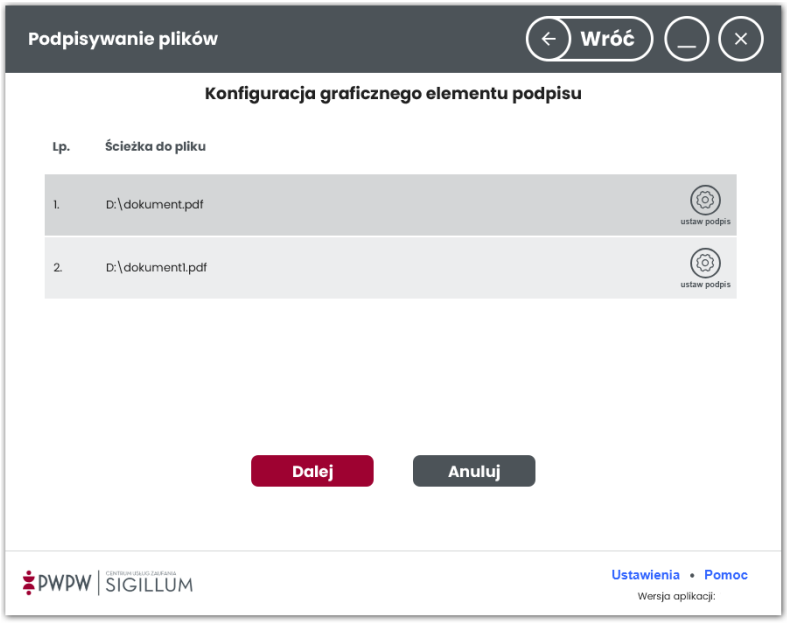
Okno można pozostawić na ekranie lub kliknąć przycisk Cancel – operacja podpisu będzie trwała nadal.

7.1.5 Podpisanie plików PDF podpisem PAdES z elementem graficznym podpisu

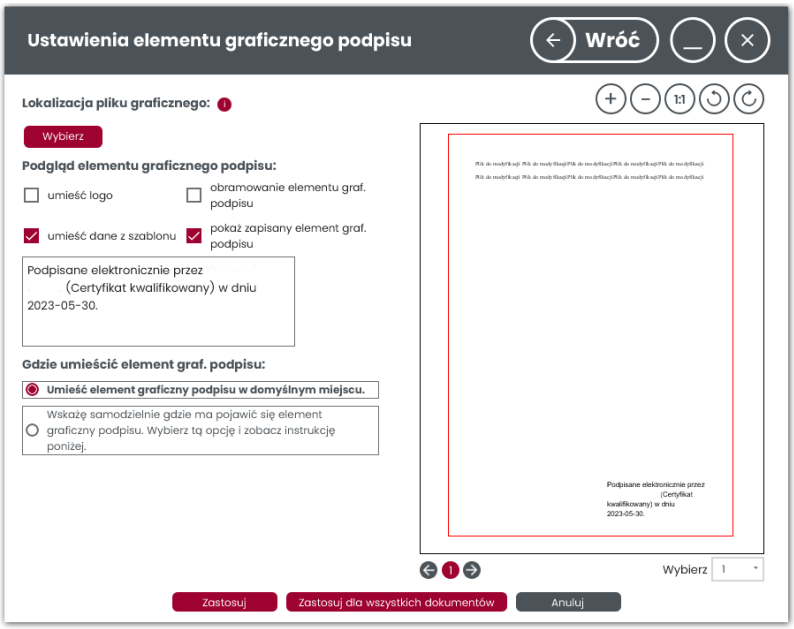
Aby rozpocząć podpisanie plików w formacie PAdES z elementem graficznym podpisu, w pierwszej kolejności należy ustawić w aplikacji element graficzny podpisu (6.5.1). Element graficzny podpisu można też ustawić w trakcie składania podpisu. Po dodaniu plików *.pdf, z menu bocznego wybieramy **Profil: Użytkownika, Format: PAdES** oraz zaznaczamy checkbox **Znacznik pdf (element graf. podpisu).** Można również wybrać powód podpisu – pole dostępne tylko dla plików PDF oraz formatu **PAdES.**



Po kliknięciu przycisku **„Podpisz”**, aplikacja przechodzi do następnego okna konfiguracji. Wybieramy odpowiedni certyfikat oraz potwierdzamy jego wybór a następnie podajemy pin. Dodanie do dokumentu elementu graficznego podpisu (np. zawierającego logo Firmy) a następnie możliwość jego edycji (umieszczenie we wskazanym miejscu oraz określenie rozmiaru) dostępne są dla każdego pliku z osobna po kliknięciu ikony ***ustaw podpis***.



Po kliknięciu w wyżej wymienioną ikonę, aplikacja otwiera okno: **„Ustawienia elementu graficznego”.**



7.1.5.1 Ustawienia elementu graficznego podpisu – lewa kolumna okna

W lewej kolumnie okna dostępne są pozycje:

- ***Lokalizacja pliku graficznego*** – przycisk ***Wybierz*** pozwala wybrać obraz, który zostanie umieszczony w elemencie graficznym podpisu, lokalizację pliku graficznego można skonfigurować również w Ustawieniach (patrz 6.5.1),
- ***Podgląd elementu graficznego podpisu*** – zawiera podgląd elementu graficznego umieszczanego na dokumencie oraz ustawienia (które można skonfigurować również w Ustawieniach (patrz 6.5.1)) elementu graficznego podpisu takie jak:
  - ***umieść logo*** – jeśli wybrano plik graficzny, po zaznaczeniu zostanie on wstawiony do elementu graficznego podpisu,
  - ***obramowanie elementu graf. podpisu*** – po zaznaczeniu element graficzny podpisu będzie zawierał obramowanie,
  - ***umieść dane z szablonu*** – domyślnie zaznaczone, element graficzny podpisu będzie zawierał dane z certyfikatu użytego do podpisu, w formie którą można skonfigurować w Ustawieniach
  - ***pokaż zapisany elementu graf. podpisu*** - steruje widocznością elementu graf. podpisu na dokumencie, w zapisanej pozycji podczas ustawiania elementu graficznego
- ***Gdzie umieścić element graf. podpisu*** – pozwala wybrać sposób wstawiania elementu graficznego podpisu na dokumencie, zawiera dwa pola wyboru:
  - ***Umieść element graficzny podpisu w domyślnym miejscu*** – pozycja zaznaczona domyślnie, element graficzny wstawiany jest:
    - w prawym dolnym rogu ostatniej strony dokumentu jeśli nie zapisano wcześniej pozycji elementu graficznego,
    - w zapisanej wcześniej pozycji elementu graficznego podpisu,
    - jeśli w przypadku dodawania kolejnych podpisów pozycja wstawianego elementu graficznego jest już zajęta przez wcześniej wstawione elementy graficzne, przeprowadzane jest poszukiwanie wolnego miejsca na stronie (przesuwanie od prawej do lewej krawędzi strony o szerokość elementu graficznego a następnie przejście o wysokość elementu

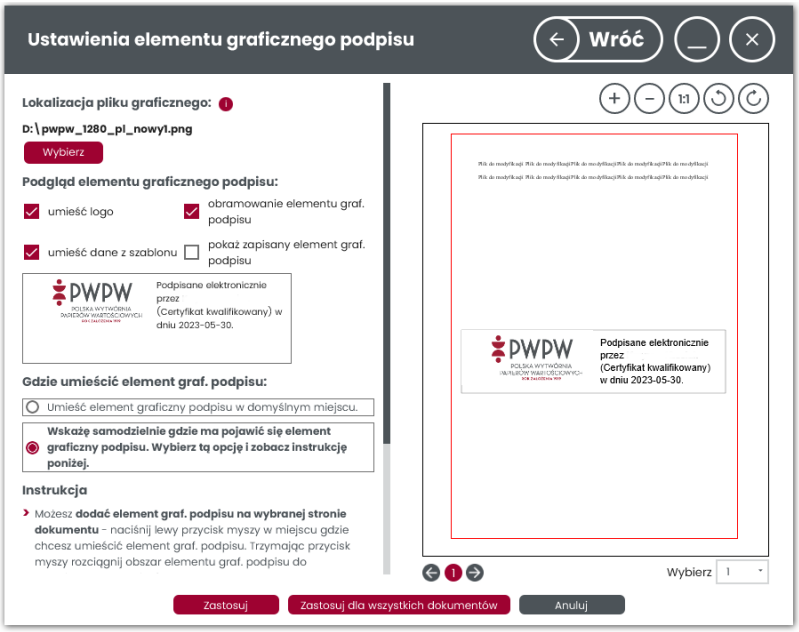
graficznego w górę i znów przesuwanie od prawej do lewej krawędzi strony o szerokość elementu graficznego, po znalezieniu wolnego miejsca element graficzny zostaje wstawiony,

- jeśli w przypadku dodawania kolejnych podpisów pozycja wstawianego elementu graficznego jest już zajęta i nie uda się znaleźć wolnego miejsca na stronie, wyświetlony zostaje komunikat:
  - jeśli dokument jest jednostronicowy komunikat zawiera przycisk ***OK*** pozwalający kontynuować podpisywanie bez wstawiania elementu graficznego podpisu,
  - jeśli dokument jest wielostronicowy komunikat zawiera przycisk ***OK*** pozwalający kontynuować podpisywanie bez wstawiania elementu graficznego podpisu oraz przycisk ***Anuluj*** kierujący do poniższej opcji wyboru,

- ***Wskażę samodzielnie gdzie ma pojawić się element graficzny podpisu. Wybierz tą opcję i zobacz instrukcję poniżej*** – po zaznaczeniu dostępna jest instrukcja wraz z przyciskiem **Zapisz pozycję elementu graf. podpisu**, aplikacja umożliwia naniesienie elementu graficznego, poprzez naciśnięcie lewego przycisku myszy i rozciągnięcie obszaru elementu graficznego do oczekiwanych rozmiarów.

7.1.5.2 Ustawienia elementu graficznego podpisu – prawa kolumna okna

W prawej kolumnie okna znajduje się obszar podglądu dokumentu a nad nim ikony pozwalające powiększyć, pomniejszyć, ustawić rozmiar 1:1, obrócić w lewo o 90 stopni oraz obrócić w prawo o 90 stopni. Po powiększeniu dodatkowo pojawia się możliwość włączenia Trybu przesuwania, pozwalająca „złapać" stronę i dowolnie przesuwać.

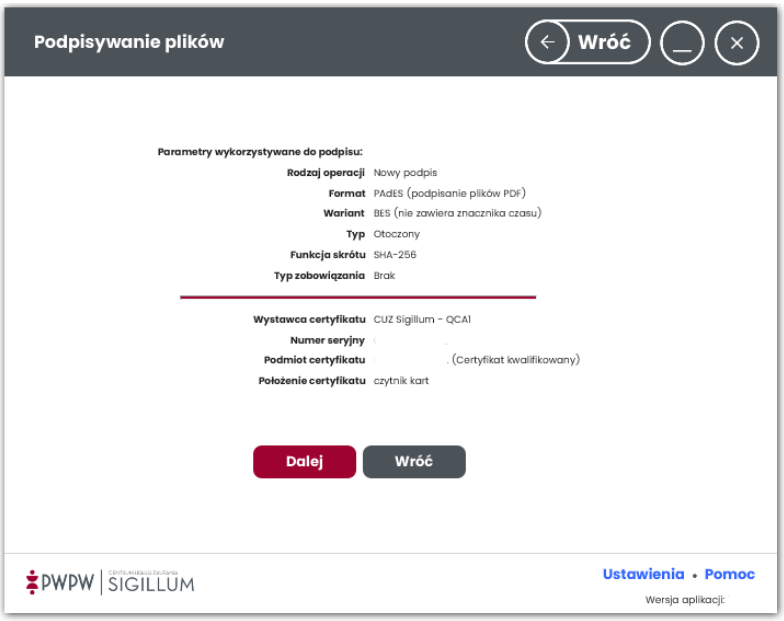


Przy zaznaczonej pozycji ***Wskażę samodzielnie gdzie ma pojawić się element graficzny podpisu. Wybierz tą opcję i zobacz instrukcję poniżej.***, po wstawieniu elementu graficznego na dokumencie, możliwe jest zapisanie pozycji i rozmiaru elementu graficznego poprzez przycisk **Zapisz pozycję elementu graf. podpisu** (przycisk dostępny po przewinięciu

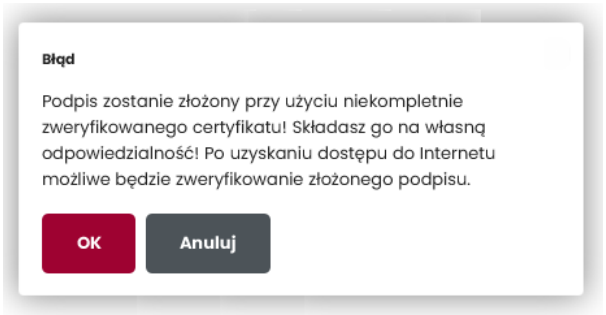
zawartości lewej kolumny w dół). Jeśli pozycja elementu graficznego zostanie zapisana, przy kolejnym ustawianiu elementu graficznego pojawi się ramka w zapisanej pozycji. Pole **pokaż zapisany element graf. podpisu** steruje widocznością elementu graficznego na dokumencie, w zapisanej pozycji podczas ustawiania elementu graficznego.

7.1.5.3 Finalizowanie wstawiania elementu graficznego podpisu

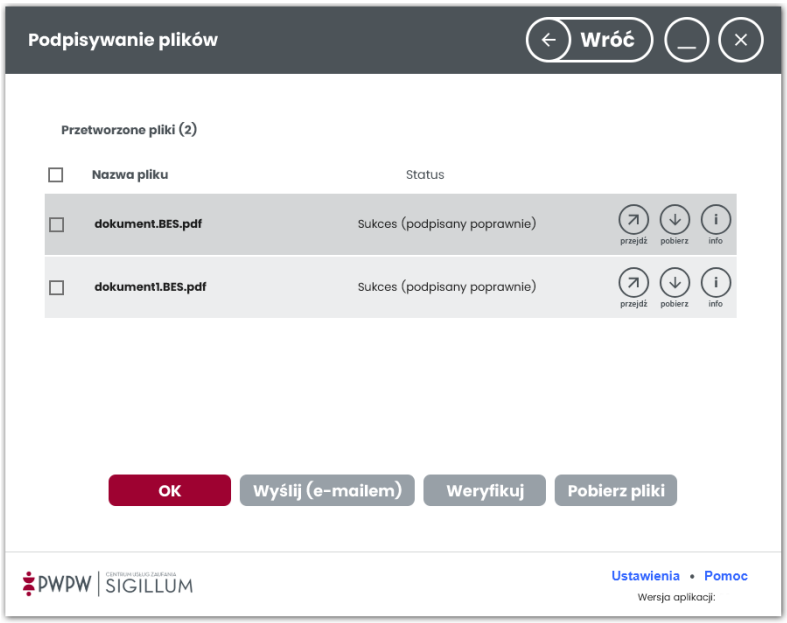
Na ekranie ***Ustawienia elementu graficznego podpisu***, pod lewą i prawą kolumną znajduje się sekcja przycisków. Przycisk **Zastosuj** zapisuje element graficzny podpisu na wybranym dokumencie, przycisk **Zastosuj do wszystkich dokumentów** zapisuje element graficzny podpisu dla wszystkich podpisywanych dokumentów PDF.
Po zastosowaniu elementu graficznego do wybranego dokumentu i kliknięciu ***Dalej***, system prezentuje ekran parametrów wykorzystanych do wykonania podpisu.



W przypadku, gdy aplikacja nie ma dostępu do Internetu wyświetlane jest okno z komunikatem o braku możliwości wykonania kompletnej weryfikacji użytego certyfikatu.



Kliknięcie przycisku OK zamyka okno komunikatu, prezentowany jest ekran końcowy jak poniżej zawierający listę podpisanych plików wraz ze statusem podpisu. Jeżeli w trakcie procesu podpisu wybrano element graficzny, został on umieszczony na dokumencie lub dokumentach w zależności od wyboru użytkownika.



7.1.5.4 Wstawianie elementu graficznego podpisu – wskazówki dla osób niewidomych

Aplikacja pozwala osobom niewidomym wstawić element graficzny podpisu na dokumencie PDF. Po tym jak otwarte zostanie okno ***Ustawienia elementu graficznego podpisu***, domyślnie zaznaczony zostaje sposób wstawiania elementu graficznego: ***Umieść element graficzny podpisu w domyślnym miejscu***. Domyślnym miejscem jest prawy dolny róg ostatniej strony dokumentu PDF. Jeśli istnieje potrzeba zmiany domyślnego miejsca, z pomocą osoby widzącej należy zmienić sposób wstawiania elementu graficznego na ***Wskażę samodzielnie gdzie ma pojawić się element graficzny podpisu. Wybierz tą opcję i zobacz instrukcję poniżej.*** a następnie rozciągnąć element graficzny na obszarze podglądu dokumentu w oczekiwanym miejscu oraz rozmiarze. Przycisk **Zapisz pozycję elementu graf. podpisu** (przycisk dostępny po przewinięciu zawartości lewej kolumny w dół) zapisuje wybrane: pozycję oraz rozmiar jako nową domyślną pozycję elementu graficznego.

W przypadku dodawania kolejnych podpisów, jeśli domyślna pozycja elementu graficznego jest zajęta przez elementy graficzne poprzednich podpisów, aplikacja próbuje znaleźć wolne miejsce. Jeśli nie uda się znaleźć wolnego miejsca, użytkownik może kontynuować podpisywanie bez wstawiania elementu graficznego podpisu lub z pomocą osoby widzącej wskazać gdzie ma się pojawić element graficzny podpisu.

7.2 Dodaj kolejny podpis

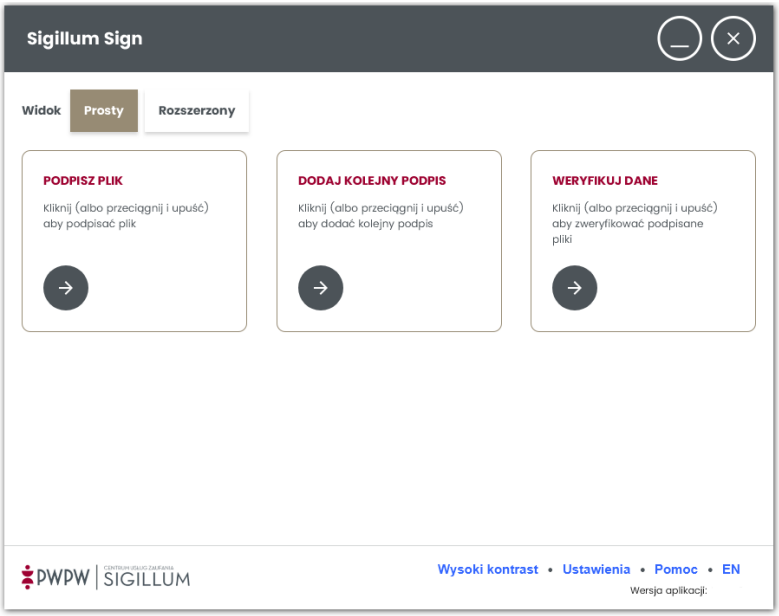
7.2.1 Ekran początkowy procesu weryfikacji

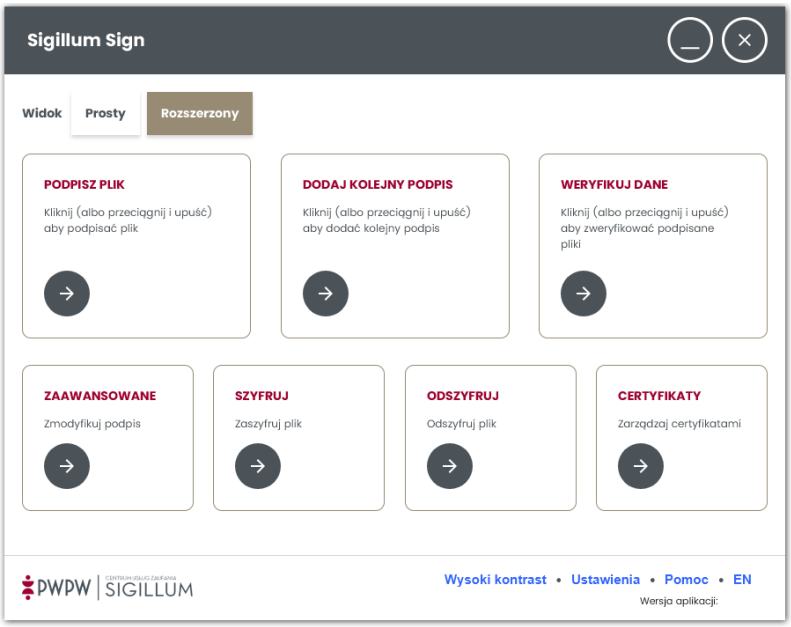
Wybranie opcji Dodaj kolejny podpis oznacza, że do podpisanego certyfikatem dokumentu dodany zostanie kolejny podpis wskazany przez użytkownika (podpis równoległy).

Podpis równoległy oznacza, że składany podpis jest niezależny wobec istniejących innych podpisów w dokumencie.

Funkcjonalność dodania kolejnego podpisu dostępna jest zarówno z panelu w widoku prostym, jak i rozszerzonym. Wykonywane operacje są natomiast takie same, niezależnie od tego, w którym oknie rozpoczynamy pracę.

Kliknięcie, lub przeciągnięcie plików na obszar ***„Dodaj kolejny podpis”*** na stronie głównej rozpoczynają proces weryfikacji. Opcja dostępna jest w widoku prostym oraz rozszerzonym.

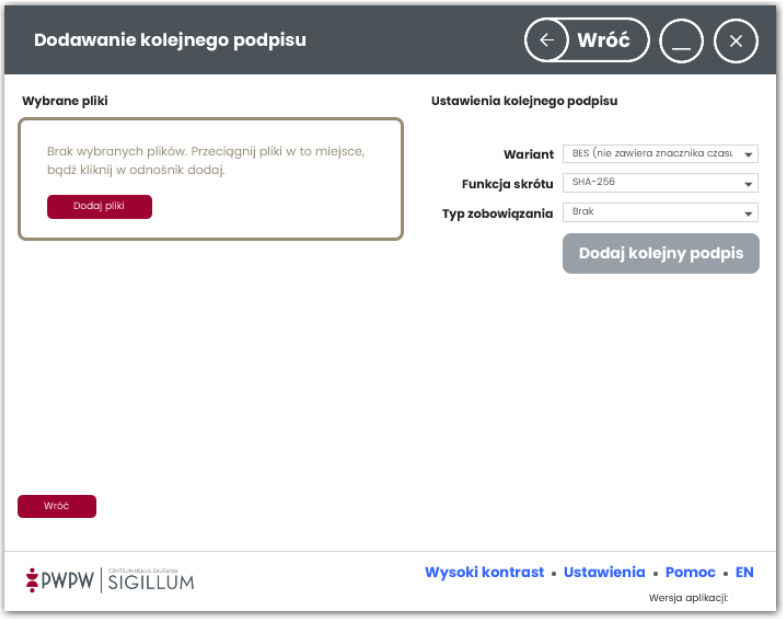




Po kliknięciu kafelka ***„Dodaj kolejny podpis”*** Użytkownik określa szczegóły składanego podpisu takie jak wariant (bez lub ze znacznikiem czasu), funkcję skrótu oraz typ zobowiązania.

7.2.2 Ekran procesu dodawania kolejnego podpisu

Po wyborze opcji ***„Dodaj kolejny podpis"*** lub przeciągnięciu plików na obszar Dodaj kolejny podpis, użytkownikowi prezentowany jest poniższy widok tj. Dodawanie kolejnego podpisu do pliku.

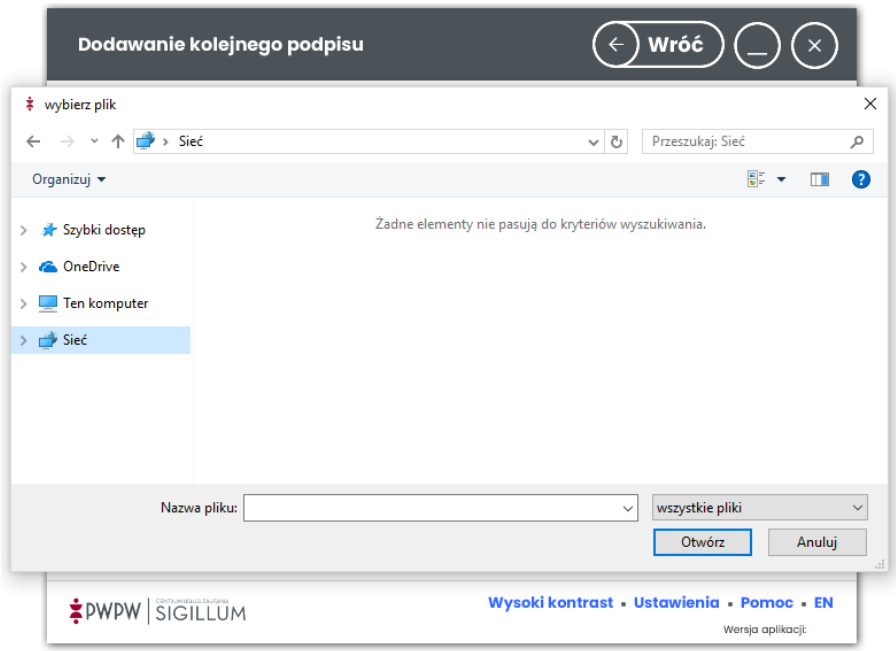


Ekran podzielony jest na dwie części: większą, centralną tzw. obszar roboczy, w którym prezentowane są pliki oraz mniejszą, z prawej strony tzw. obszar ustawień, zawierający ustawienia związane z podpisem oraz przycisk ***„Dodaj kolejny podpis"***. Oprócz pól ustawień widocznych na ekranie powyżej, jeśli do obszaru roboczego zostaną dodane pliki z podpisami PAdES dostępne będzie dodatkowe pole specyficzne dla tego formatu: **Powód**.

7.2.3 Dodanie plików do obszaru roboczego

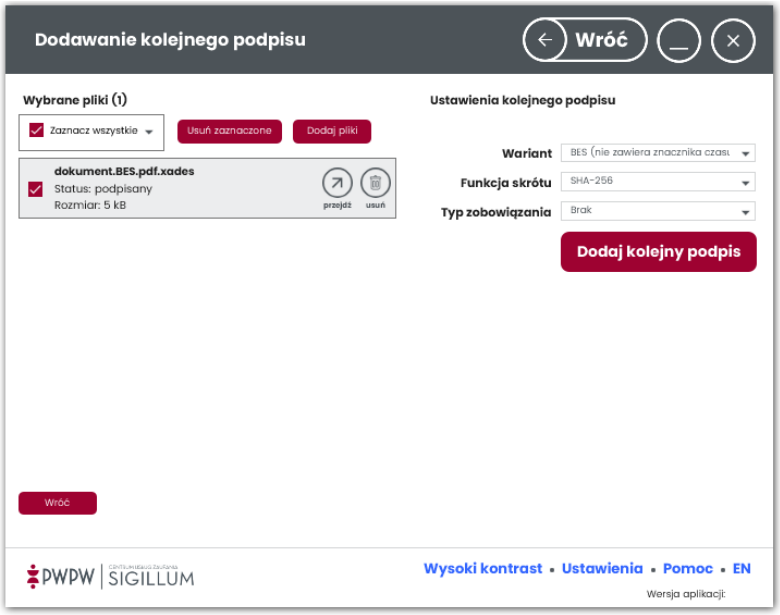
Dodanie pliku/plików może odbyć się na dwa sposoby: przez użycie przycisku **Dodaj pliki** lub funkcję *przeciągnij-upuść*.

Po kliknięciu opcji ***Dodaj pliki*** pojawi się okno przeglądania zawartości stacji roboczej użytkownika pozwalające wybrać pliki do podpisu.



Dodanie pliku do obszaru roboczego może odbywać się przy użyciu funkcji *przeciągnij i upuść*.

Po wywołaniu opcji dodawania plików do obszaru roboczego, pliki prezentowane są w formie kafelków wraz z danymi je opisującymi.



Kafelki zawierają następujące informacje:

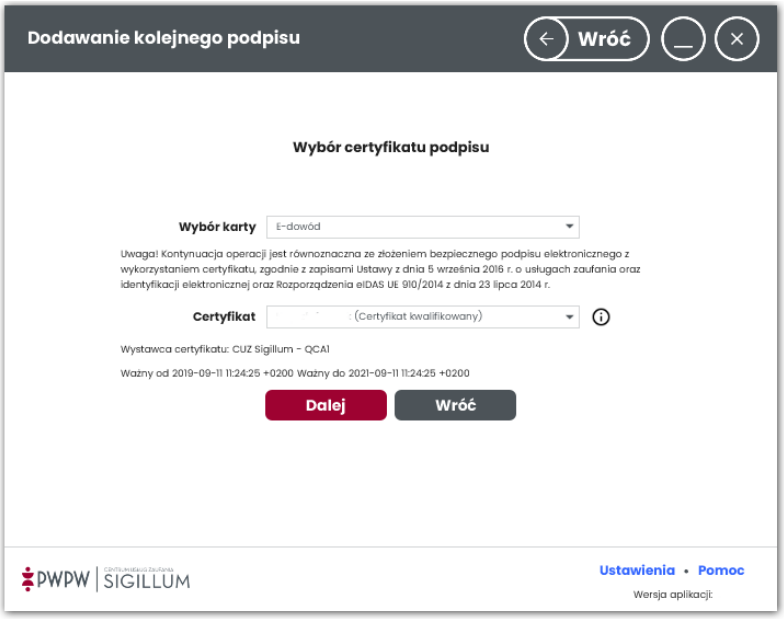
Nazwa dokumentu, Status oraz rozmiar.

Możliwe statusy dodanego pliku to: podpisany, niepodpisany, za duży rozmiar (patrz ROZMIAR). Kliknięcie w ikonę ***przejdź*** na kafelku umożliwia otwarcie (niepodpisanego) pliku źródłowego podpisu. Kliknięcie w ikonę ***usuń*** na kafelku umożliwia usunięcie pliku z obszaru roboczego.

7.2.4 Ekran wyboru certyfikatów i złożenie podpisu

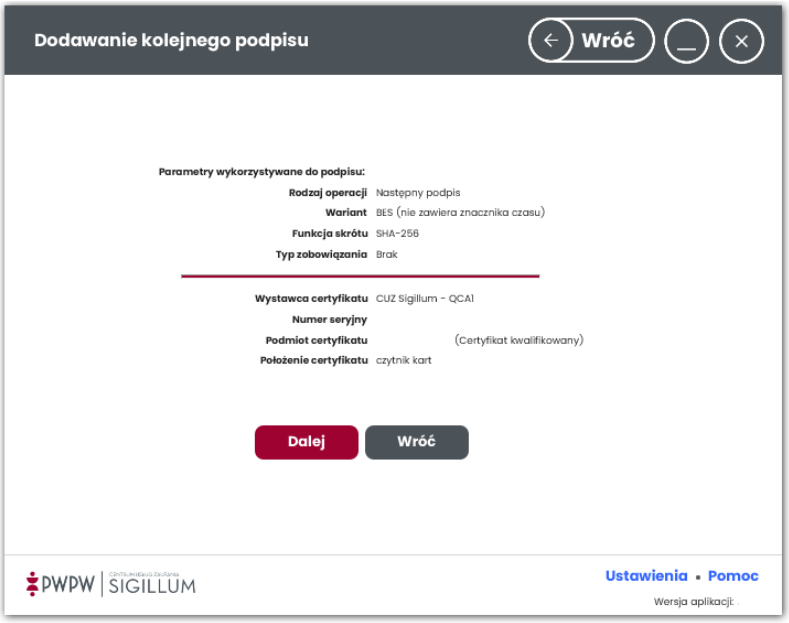
Po wyborze opcji ***„Dodaj kolejny podpis”*** użytkownik przeniesiony zostaje do ekranu wyboru karty i certyfikatów.

Wybór karty to wskazanie biblioteki pkcs11 umieszczonej w określonej lokalizacji. Jeśli biblioteki nie ma w określonej lokalizacji, wyświetlone zostaje okno wyboru pliku. Po wskazaniu poprawnego pliku pkcs11 do listy wyboru karty zostaje dodana nowa pozycja.



Po wyborze karty i certyfikatu, pojawia się informacja na temat certyfikatu i skutku prawnego wywołanego jego użyciem.
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny.
Po kliknięciu ***„Dalej”*** system otwiera okno wprowadzenia kodu PIN.

Po wpisaniu poprawnego kodu PIN i kliknięciu ***„Potwierdź”***, system prezentuje ekran parametrów wykorzystanych do wykonania kolejnego podpisu.



Po kliknięciu ***„Dalej”*** prezentowany jest ekran końcowy, potwierdzający przebieg operacji.

W kolumnie „Status" wyświetlany jest status otrzymany po wykonaniu operacji, w wierszu każdego podpisanego pliku znajdują się ikony:

- przejdź – prezentacja (niepodpisanego) pliku źródłowego podpisu,
- pobierz – zapisanie (niepodpisanego) pliku źródłowego podpisu,
- info – szczegóły złożonego podpisu.

Po zaznaczeniu checkboxa w wierszu wybranych plików można wysłać podpisane dokumenty poprzez e-mail klikając przycisk Wyślij (e-mailem).

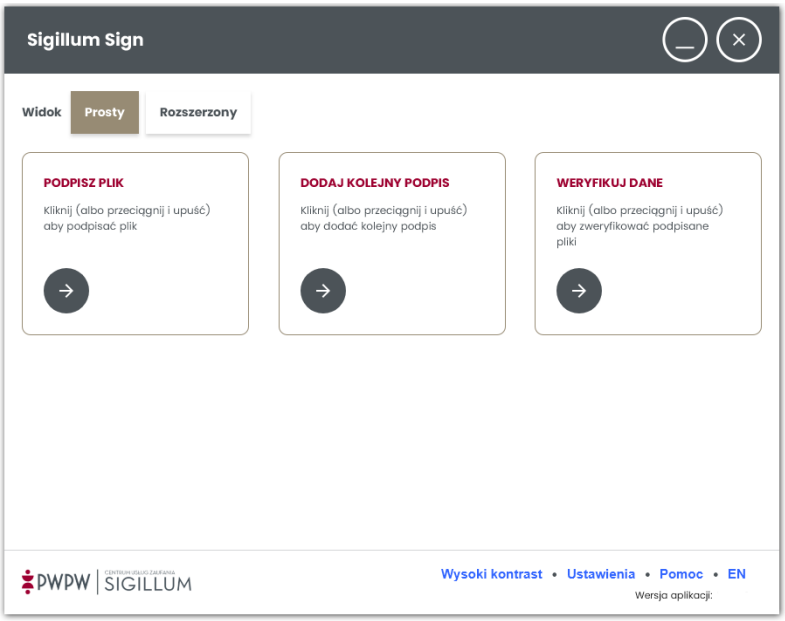
Po kliknięciu przycisku Weryfikuj wyświetlany jest ekran weryfikacji podpisanych plików.

Potwierdzenie (OK) kończy proces podpisywania. Podpisane pliki odnaleźć można w folderach, gdzie znajdują się pliki źródłowe. Podpis można zweryfikować w procesie weryfikacji.

7.3 Weryfikacja podpisu

7.3.1 Ekran początkowy procesu weryfikacji

Kliknięcie, lub przeciągnięcie plików na obszar ***„Weryfikuj dane"*** na stronie głównej rozpoczynają proces weryfikacji. Opcja dostępna jest w widoku prostym oraz rozszerzonym.



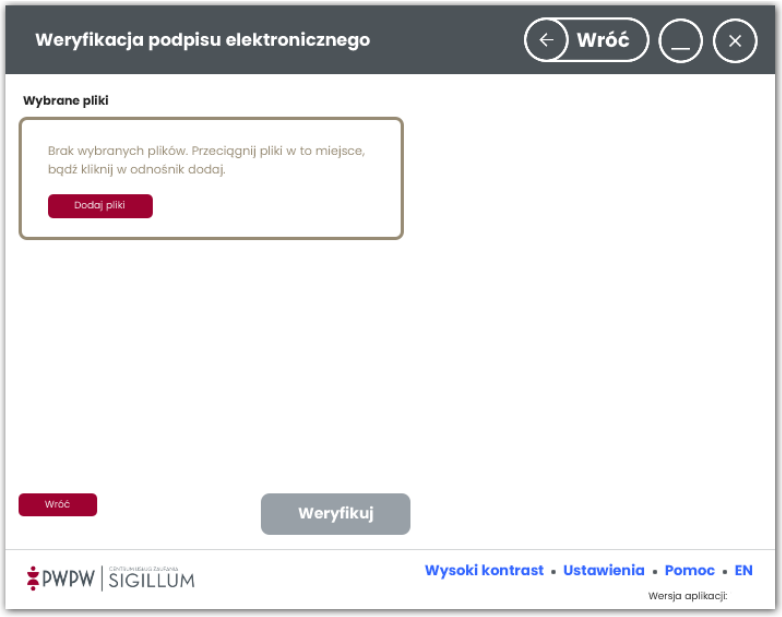
UWAGA!
W zależności od wersji aplikacji, formatu oraz od rozszerzenia pliku weryfikowanego podpisu dozwolony jest określony rozmiar weryfikowanego pliku.

Format podpisu	Dozwolony rozmiar pliku	
	wersja 64-bitowa	wersja 32-bitowa
XAdES otaczający, otoczony	150MB	50MB
XAdES zewnętrzny	bez limitu	bez limitu
PAdES otoczony	350MB	50MB
CAdES otaczający	350MB	50MB
CAdES zewnętrzny	bez limitu	bez limitu
ASiCS otoczony	350MB	50MB
ASiCE otoczony	350MB	50MB

Jeśli podpisany plik jest plikiem xml to jego maksymalny rozmiar wynosi 150MB / 40MB.

7.3.2 Ekran weryfikacji i ustawień

Po wyborze opcji ***„Weryfikuj dane”*** użytkownikowi prezentowany jest poniższy widok tj. Weryfikacji podpisu elektronicznego.

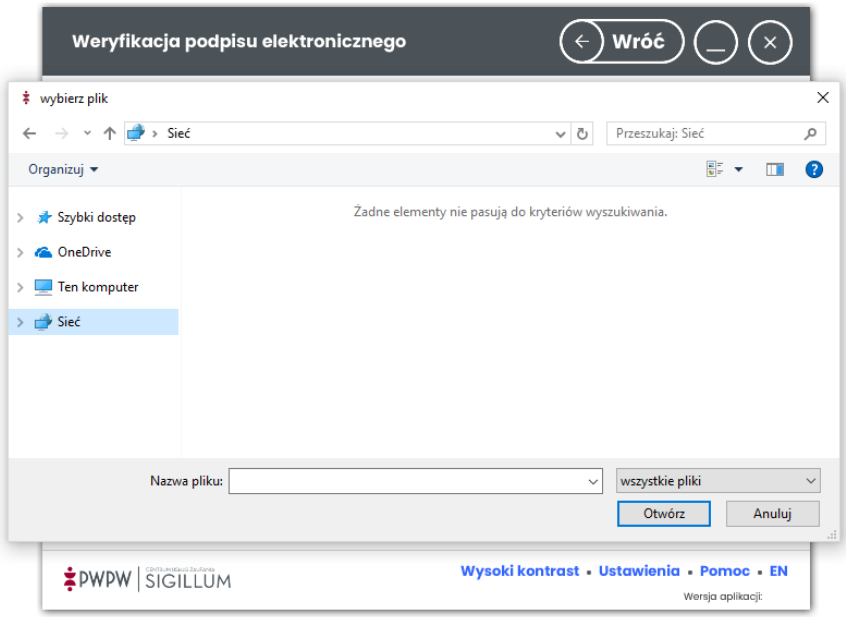


Ekran podzielony jest na dwie części: większą, centralną tzw. obszar roboczy, w którym prezentowane są pliki oraz mniejszą, z prawej strony wyświetlający wynik weryfikacji.

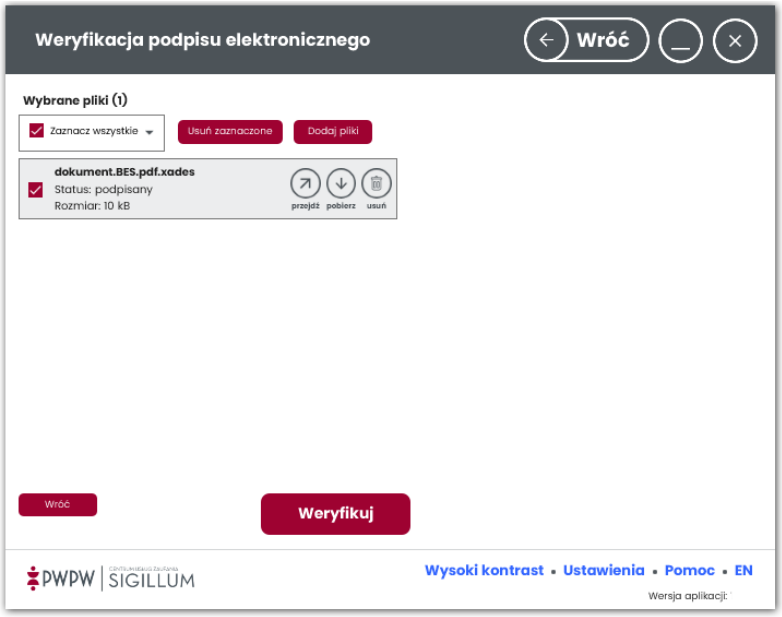
7.3.3 Dodanie plików do obszaru roboczego

Po kliknięciu opcji *„**Dodaj pliki**”* pojawi się okno przeglądania zawartości stacji roboczej użytkownika pozwalające wybrać pliki do podpisu.

Użytkownik powinien dodać do obszaru roboczego pliki (podpisane), które mają zostać zweryfikowane. System umożliwia dodanie plików z odpowiednimi rozszerzeniami.



Po wybraniu i dodaniu plików do obszaru roboczego prezentowane są one w formie kafelków.



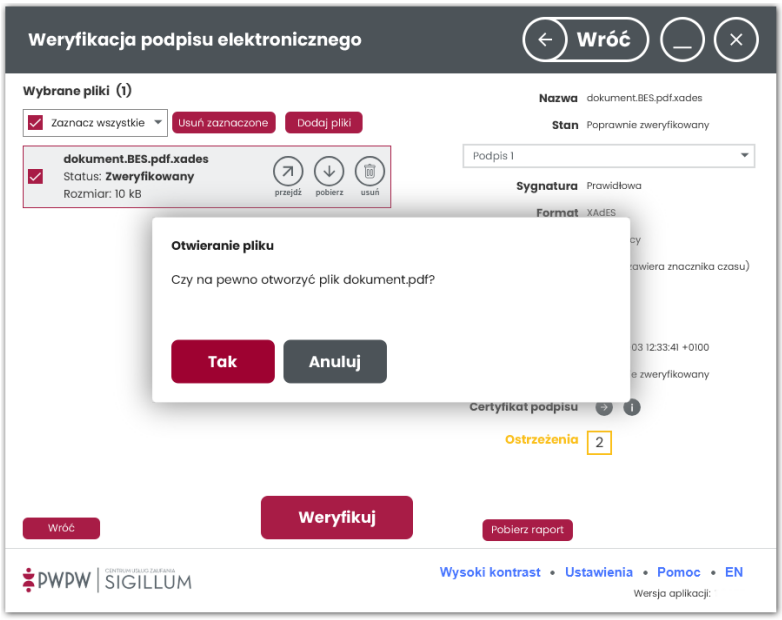
Zaznaczenie/odznaczenie kafelka odbywa się przez kliknięcie w checkbox. Operacja weryfikacji może odbyć się na zaznaczonym pliku.

Możliwe statusy dodanego pliku to: podpisany, niepodpisany, za duży rozmiar (patrz ROZMIAR).

Kliknięcie w ikonę ***usuń*** umożliwia usunięcie pliku z obszaru roboczego.

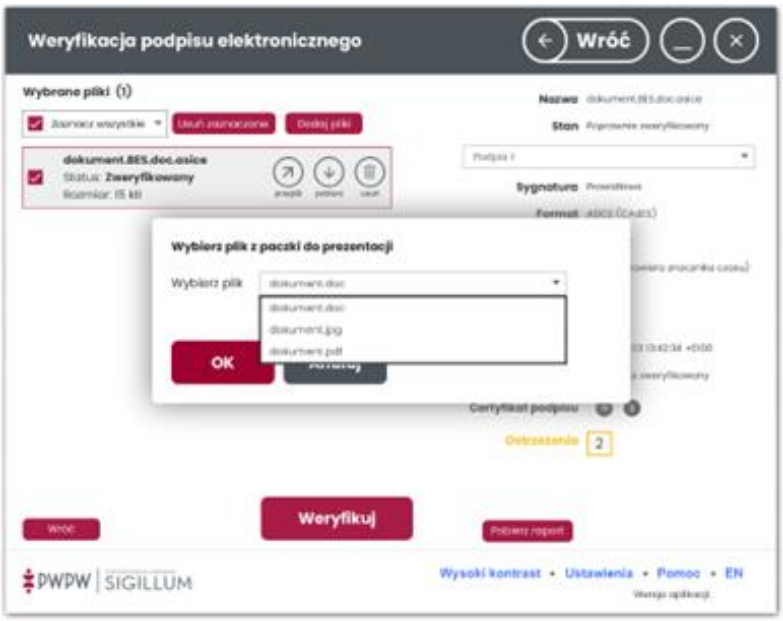
7.3.3.1 Wyświetlenie pliku oryginału

Aby wyświetlić plik oryginału, który został podpisany należy dla określonego pliku na liście kliknąć ikonę ***przejdź***. Wskazana akcja dla plików podpisanych popisem otaczającym ekstrahuje plik oryginału z pliku podpisanego i wyświetla go w skojarzonej w systemie operacyjnym aplikacji. Po kliknięciu w ikonę ***przejdź*** wyświetlony zostaje komunikat wymagający potwierdzenia zamiaru otwarcia pliku.



Po potwierdzeniu przyciskiem ***Tak***, plik otwierany jest w domyślnej dla rozszerzenia pliku aplikacji. Kliknięcie przycisku ***Anuluj*** oznacza rezygnację z zamiaru otwarcia pliku.

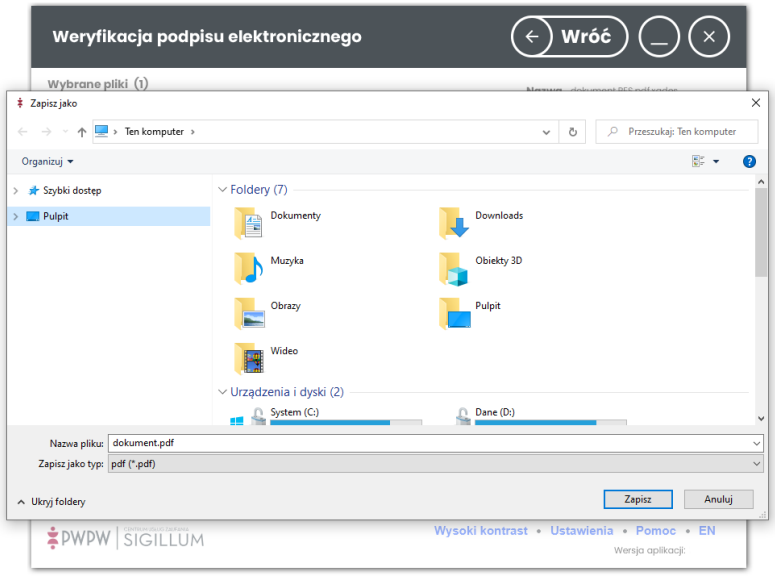
W przypadku formatu ASIC-E, po kliknięciu w ikonę ***przejdź*** należy wybrać plik zawarty w podpisanej paczce, który ma zostać otwarty.



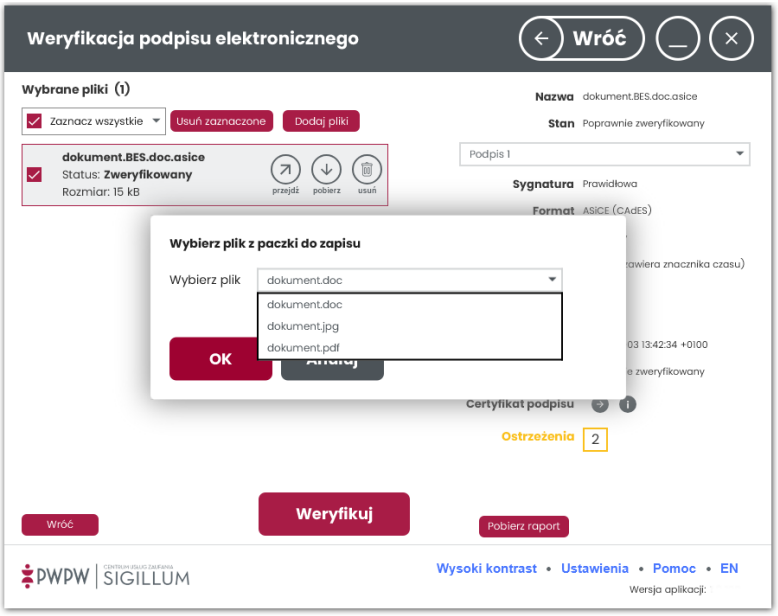
Po potwierdzeniu przyciskiem ***OK***, plik otwierany jest w domyślnej dla rozszerzenia pliku aplikacji. Kliknięcie przycisku ***Anuluj*** oznacza rezygnację z zamiaru otwarcia pliku.

7.3.3.2 Pobranie pliku oryginału

Aby pobrać plik oryginału, który został podpisany należy dla określonego pliku na liście kliknąć ikonę ***pobierz***. Wskazana akcja dla plików popisanych podpisem otaczającym ekstrahuje plik oryginału z pliku podpisanego i zapisuje go we wskazanym przez użytkownika katalogu. Kliknięcie w ikonę ***pobierz*** otwiera okno ***Zapisz jako*** umożliwiające zapis pliku w wybranej lokalizacji.



W przypadku formatu ASIC-E, po kliknięciu w ikonę ***pobierz*** należy wybrać plik zawarty w podpisanej paczce, który ma zostać zapisany.

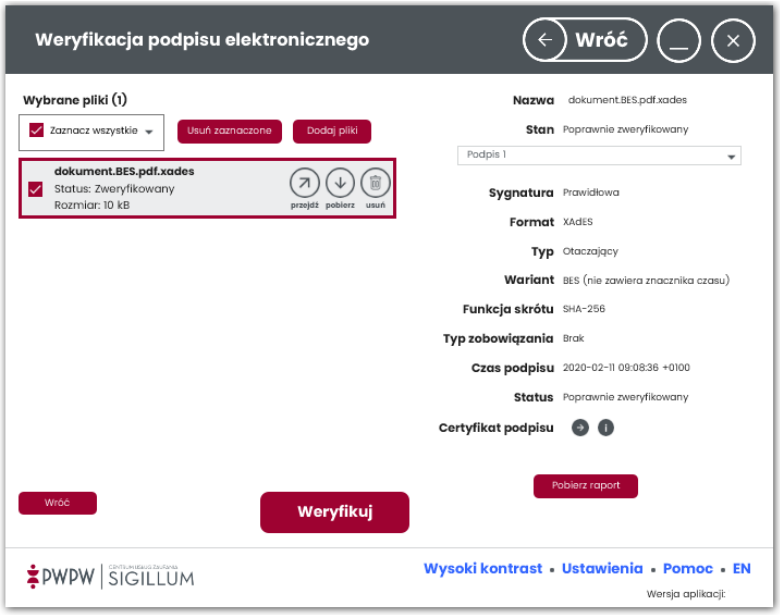


W przypadku formatów XAdES/CAdES otaczający oraz formatów ASiC-S / ASiC-E otoczonych, plik oryginału znajduje się wewnątrz pliku podpisanego.

7.3.4 Ekran weryfikacji

Przycisk ***„Weryfikuj dane”*** rozpoczyna operację automatycznej weryfikacji podpisu.

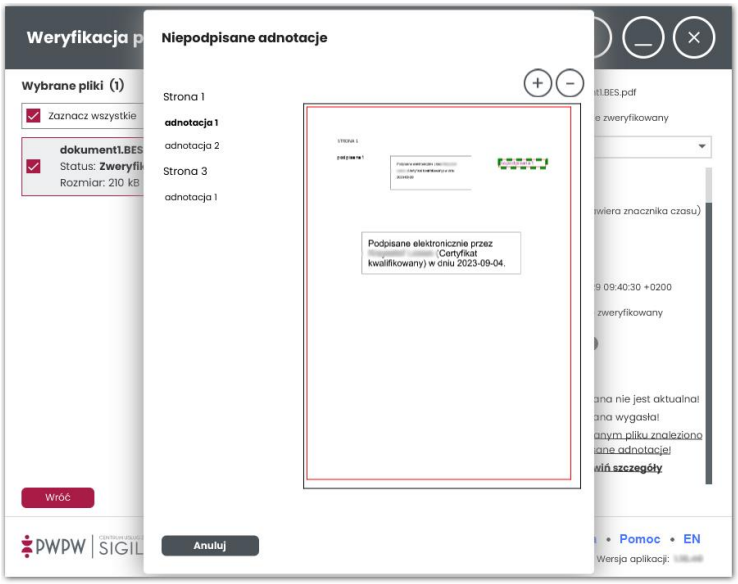
Po chwili użytkownik otrzymuje informację na temat statusu weryfikacji.



W obszarze po prawej stronie zwracany jest status weryfikacji:

- Poprawnie zweryfikowany — gdy bezpieczny podpis elektroniczny jest poprawny w rozumieniu specyfikacji zastosowanego algorytmu szyfrowego, a kwalifikowany certyfikat lub zaświadczenie certyfikacyjne zawierające dane służące do jego weryfikacji oraz użyta ścieżka certyfikacji są ważne;
- Negatywnie zweryfikowany — gdy bezpieczny podpis elektroniczny jest niepoprawny w rozumieniu specyfikacji zastosowanego algorytmu szyfrowego lub kwalifikowany certyfikat albo zaświadczenie certyfikacyjne zawierające dane służące do jego weryfikacji są nieważne;
- Niekompletnie zweryfikowany — gdy bezpieczny podpis elektroniczny jest poprawny w rozumieniu specyfikacji zastosowanego algorytmu szyfrowego, ale podczas weryfikacji nie udało się potwierdzić, że kwalifikowany certyfikat lub zaświadczenie certyfikacyjne służące do jego weryfikacji oraz użyta ścieżka certyfikacji zawiera ważne w określonym czasie poświadczenia elektroniczne, w szczególności gdy kwalifikowany certyfikat służący do weryfikacji tego podpisu jest zawieszony.
- Ostrzeżenia — stanowią informację dotyczącą podpisu, w przypadku podpisów niespełniających wymogów eIDAS są to ostrzeżenia:
    - *Certyfikat nie zawiera adresów list CRL/OCSP*
    - *Certyfikat nie zawiera hiperłączy do danych wystawcy (Authority information access locations)*

Wśród ostrzeżeń może pojawić się ostrzeżenie o treści „W podpisanym pliku znaleziono niepodpisane adnotacje!", po kliknięciu w nie, wyświetlone zostaje okno z listą niepodpisanych adnotacji, pozwalające wyświetlić zaznaczoną adnotację na stronie dokumentu PDF. Ikona ze znakiem „+" powiększa dwukrotnie widok dokumentu PDF, ikona ze znakiem „–„ przywraca oryginalny rozmiar.

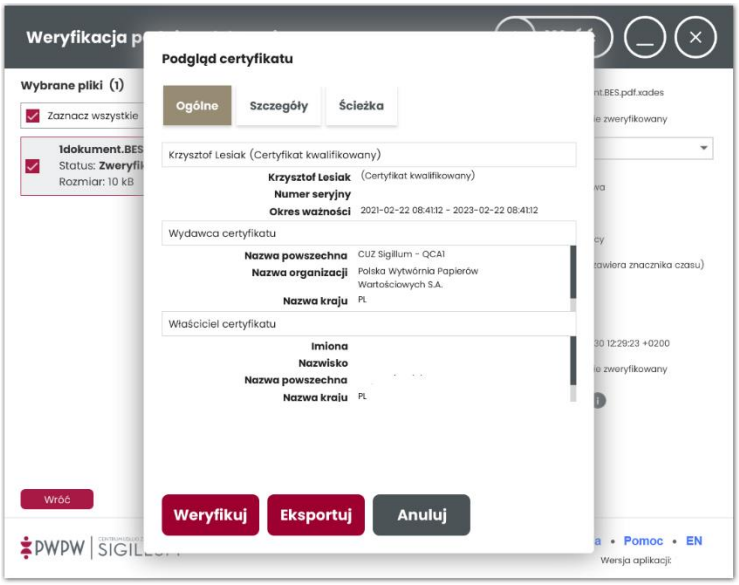


Użytkownik ma możliwość podglądu informacji o podpisie po kliknięciu ikony strzałki skierowanej w prawo lub ikony z literką i w oknie z wynikiem weryfikacji.

Jeśli dane PZ są osadzone w podpisie to wyświetlony zostaje klucz "Dane PZ" z ikonką "I", po kliknięciu której można zobaczyć szczegóły użytego profilu zaufanego.1

Można również pobrać raport z weryfikacji klikając przycisk Pobierz raport.

Kliknięcie ikony z literką i powoduje wyświetlenie okna Podgląd certyfikatu.



W powyższym oknie można m.in. zweryfikować certyfikat użyty do podpisu (przycisk **Weryfikuj**) oraz wyeksportować certyfikat do pliku (przycisk **Eksportuj**).

Poniższa tabela przedstawia wszystkie możliwe błędy oraz ostrzeżenia.

Identyfikator ostrzeżenia lub błędu	Znaczenie (EN)	Znaczenie (PL)
BBB_FC_IEFF_ANS	The expected format is not found!	Oczekiwany format nie został znaleziony!
BBB_FC_IECTF_ANS	The expected container type is not found!	Oczekiwany typ kontenera nie został odnaleziony!
BBB_FC_ITZCP_ANS	The zip comment is absent!	Brak komentarza zip!
BBB_FC_ITEZCF_ANS	The expected zip comment is not found!	Nie odnaleziono oczekiwanego komentarza zip!
BBB_FC_ITMFP_ANS	The mimetype file is absent!	Brak pliku typu MIME!
BBB_FC_IEMCF_ANS	The expected mimetype content is not found!	Nie znaleziono oczekiwanej zawartości typu MIME!
BBB_FC_IMFP_ASICE_ANS	The manifest file (ASiC-E) is absent!	Brak pliku manifestu (ASiC-E)!
BBB_FC_IMFP_ASICS_ANS	The manifest file (ASiC-S) is present!	Plik manifestu (ASiC-E) jest obecny!
BBB_CV_IRDOF_ANS	The reference data object(s) not found!	Nie znaleziono danych dla referencji zawartych w sygnaturze!
BBB_CV_IRDOI_ANS	The reference data object(s) is not intact!	Obiekty referencji są niespójne!
BBB_CV_ISI_ANS	The signature is not intact!	Sygnatura nie jest spójna!
BBB_CV_IAFS_ANS	Structure contains unsigned content!	Struktura zawiera niepodpisaną zawartość!
BBB_ICS_SCISV_ANS	The signing certificate is inconsistent!	Certyfikat podpisujący jest niespójny!
BBB_ICS_ISCI_ANS	There is no candidate for the signing certificate!	Nie znaleziono certyfikatu podpisującego!
BBB_ICS_ISCS_ANS	The signing certificate is not signed!	Certyfikat podpisujący nie jest podpisany!
BBB_ICS_ISASCP_ANS	The signed attribute: 'signing-certificate' is absent!	Brak atrybutu podpisu ‘signing-certificate’!
BBB_ICS_ISACDP_ANS	The signed attribute: 'cert-digest' is absent!	Brak atrybutu podpisu ‘cert-digest’!
BBB_ICS_ICDVV_ANS	The signing certificate digest value does not match!	Wartość skrótu certyfikatu podpisywania nie jest zgodna!
BBB_ICS_AIDNASNE_ANS	The 'issuer-serial' attribute is absent or does not match!	Brak atrybutu ‘issuer-serial’ lub nie pasuje!
BBB_RFC_NUP_ANS	There is no Next Update defined for the revocation data!	Następna aktualizacja dla unieważnień nie została określona!
BBB_RFC_IRIF_ANS	The revocation status information is not considered as 'fresh'.	Status informacji o unieważnieniach nie jest aktualny.
BBB_SAV_TSP_IMIDF_ANS	The timestamp message imprint data is not found!	Nie znaleziono skrótu znacznika czasu!
BBB_SAV_TSP_IMIVC_ANS	The timestamp message imprint verification has failed!	Błąd podczas weryfikacji skrótu znacznika czasu!

ADEST_ITVPC_ANS_1	The timestamp is rejected, its generation time is before the best-signature-time!	Znacznik czasu został odrzucony, czas jego generacji jest z przed czasu generacji sygnatury!
ADEST_ITVPC_INFO_1	The best-signature-time was set to the generation time of the timestamp.	Czas sygnatury został ustawiony na czas generacji znacznika czasu.
ADEST_ITVPC_ANS_2	Timestamp validation is not conclusive!	Weryfikacja znacznika czasu nie jest rozstrzygająca.
ADEST_ROBVPIIC_ANS	The result of the Basic validation process is not conclusive!	Wynik podstawowej weryfikacji nie jest rozstrzygający!
ADEST_ROTVPIIC_ANS	The result of the timestamps validation process is not conclusive!	Wynik weryfikacji znacznika czasu nie jest rozstrzygający!
ADEST_RORPIIC_ANS	The result of the revocation data validation process is not acceptable!	Rezultat procesu weryfikacji unieważnień nie jest akceptowalny!
LTV_ABSV_ANS	The result of the Basic validation process is not acceptable to continue the process!	Rezultat procesu podstawowej weryfikacji nie jest akceptowany, aby kontynuować proces weryfikacji!
ARCH_LTVV_ANS	The result of the LTV validation process is not acceptable to continue the process!	Rezultat procesu weryfikacji LTV nie jest akceptowany, aby kontynuować proces weryfikacji!
ASCCM_ANS_1	The encryption algorithm not authorised!	Algorytm szyfrowania nie jest autoryzowany!
ASCCM_ANS_2	The digest algorithm not authorised!	Algorytm podsumowania nie jest autoryzowany!
ASCCM_ANS_3	The public key size is too small!	Długość klucza publicznego jest za mała!
ASCCM_ANS_4	The algorithm expiration date not found!	Nie znaleziono daty wygaśnięcia algorytmu!
ASCCM_ANS_5	The algorithm is expired!	Algorytm wygasł!
BBB_SAV_ISSV_ANS	The structure of the signature is not valid!	Struktura sygnatury jest nieprawidłowa!
BBB_SAV_ICERRM_ANS	The requested certified role is not present!	Wymagane upoważnienie certyfikatu nie istnieje!
BBB_SAV_ICRM_ANS	The requested claimed role is not present!	Wymagane upoważnienie certyfikatu nie istnieje!
BBB_SAV_ISQPCTP_ANS	The signed qualifying property: 'content-type' is not present!	Podpisany atrybut ‘content-type’ nie istnieje!
BBB_SAV_ISQPCHP_ANS	The signed qualifying property: 'content-hints' is not present!	Podpisany atrybut 'content-hints' nie istnieje!
BBB_SAV_ISQPCIP_ANS	The signed qualifying property: 'content-identifier' is not present!	Podpisany atrybut 'content-identifier' nie istnieje!
BBB_SAV_ISQPCTSIP_ANS	The signed qualifying property: 'content-timestamp' is not present!	Podpisany atrybut 'content-timestamp' nie istnieje!
BBB_SAV_ISQPSLP_ANS	The signed qualifying property: 'signer-location' is not present!	Podpisany atrybut 'signer-location' nie istnieje!

BBB_SAV_ISQPSTP_ANS	The signed qualifying property: 'signing-time' is not present!	Podpisany atrybut 'signing-time' nie istnieje!
BBB_SAV_ISQPXTIP_ANS	The signed qualifying property: 'commitment-type-indication' is not present!	Podpisany atrybut 'commitment-type-indication' nie istnieje!
BBB_SAV_IUQPCSP_ANS	The unsigned qualifying property: 'countersignature' is not present!	Niepodpisany atrybut 'countersignature' nie istnieje!
BBB_VCI_ISPK_ANS_1	The signature policy is mandatory!	Polityka podpisu jest wymagana!
BBB_VCI_ISPA_ANS	The signature policy is not available!	Polityka podpisu nie jest dostępna!
BBB_VCI_ISPM_ANS	The signature policy's hash doesn't match the computed one!	Skrót polityki podpisu nie jest zgodny z wyznaczonym podczas weryfikacji!
BBB_XCV_SUB_ANS	The certificate validation is not concluant!	Weryfikacja podpisu nie jest rozstrzygająca!
BBB_XCV_RFC_ANS	The revocation freshness check is not concluant!	Sprawdzenie aktualności unieważnień nie jest rozstrzygające!
BBB_XCV_CCCBB_ANS	The certificate chain is not trusted, there is no trusted anchor!	Ścieżka certyfikatu nie jest zaufana, ponieważ żaden z certyfikatów znajdujących się w ścieżce nie jest zaufany!
BBB_XCV_CCCBB_SIG_ANS	The certificate chain for signature is not trusted, there is no trusted anchor!	Ścieżka certyfikatu dla podpisu nie jest zaufana, ponieważ żaden z certyfikatów znajdujących się w ścieżce nie jest zaufany!
BBB_XCV_CCCBB_TSP_ANS	The certificate chain for timestamp is not trusted, there is no trusted anchor!	Ścieżka certyfikatu dla znacznika czasu nie jest zaufana, ponieważ żaden z certyfikatów znajdujących się w ścieżce nie jest zaufany!
BBB_XCV_CCCBB_REV_ANS	The certificate chain for revocation data is not trusted, there is no trusted anchor!	Ścieżka certyfikatu dla unieważnień nie jest zaufana, ponieważ żaden z certyfikatów znajdujących się w ścieżce nie jest zaufany!
BBB_XCV_CMDCIPI_ANS	The certificate has not required policy ids.	Certyfikat nie zawiera oczekiwanych identyfikatorów polityki.
BBB_XCV_CMDCIQCS_ANS	The certificate has not required QC Statement ids.	Certyfikat nie zawiera oczekiwanych identyfikatorów Deklaracji wydawcy certyfikatu (QC Statement).
BBB_XCV_CMDCIITLP_ANS	The certificate is not issued to a legal person.	Certyfikat nie jest wystawiony dla osoby prawnej.
BBB_XCV_CMDCIITNP_ANS	The certificate is not issued to a natural person.	Certyfikat nie jest wystawiony dla osoby fizycznej.
BBB_XCV_CMDCIQC_ANS	The certificate is not qualified!	Certyfikat nie jest certyfikatem kwalifikowanym (w kontekście eIDAS)!
BBB_XCV_CMDCIQSCD_ANS	The certificate is not supported by QSCD!	Certyfikat nie jest wspierany przez QSCD!
BBB_XCV_ICTIVRSC_ANS	The current time is not in the validity range of the signer's certificate.	Obecny czas jest poza zakresem ważności certyfikatu podpisującego.
BBB_XCV_IRDPFC_ANS	No revocation data for the certificate.	Nie znaleziono ważnej listy CRL dla danego certyfikatu.

BBB_VTS_IRDPFC_ANS	No satisfying revocation status information found for the certificate.	Nie znaleziono wystarczających informacji o statusie unieważnień dla certyfikatu.
BBB_XCV_IRDTFC_ANS	The revocation data for the certificate is not trusted!	Dane odwołania dla certyfikatu nie są zaufane!
BBB_XCV_IRIF_ANS	The revocation status information is not considered as 'fresh'.	Dane odwołania dla certyfikatu nie są uważane za aktualne.
BBB_XCV_ISCOH_ANS	The certificate is on hold!	Certyfikat jest wstrzymany!
BBB_XCV_ISCR_ANS	The certificate is revoked!	Certyfikat jest odwołany!
BBB_XCV_ISCGKU_ANS	The signer's certificate has not expected key-usage!	Certyfikat podpisujący nie posiada oczekiwanego atrybutu użycia klucza!
BBB_XCV_ICSI_ANS	The signature of the certificate is spoiled or it is not possible to validate it!	Podpis certyfikatu jest sfałszowany lub nie można go zweryfikować!
BBB_XCV_OCSP_NO_CHECK	The certificate has the id-pkix-ocsp-nocheck extension (RFC is skipped).	Certyfikat posiada rozszerzenie id-pkix-ocsp-nocheck (RFC jest pomijane).
BBB_XCV_PSEUDO_USE_ANS	A pseudonym is used.	Używany jest pseudonim.
BBB_XCV_AIA_PRES_ANS	Certificate does not contain a hyperlink to issuer data (Authority information access locations).	Certyfikat nie zawiera hiperłączy do danych wystawcy (Authority information access locations).
BBB_XCV_REVOC_PRES_ANS	Certificate does not contain addresses of CRL/OCSP list.	Certyfikat nie zawiera adresów list CRL/OCSP.
BBB_XCV_ISCGCOUN_ANS	The certificate has not expected country-name!	Certyfikat nie posiada atrybutu: nazwa kraju (country-name)!
BBB_XCV_ISCGORGAN_ANS	The certificate has not expected organization name!	Certyfikat nie posiada atrybutu: nazwa organizacji (organization name)!
BBB_XCV_ISCGORGAU_ANS	The certificate has not expected organization unit!	Certyfikat nie posiada atrybutu: jednostka organizacyjna (organization unit)!
BBB_XCV_ISCGSURN_ANS	The certificate has not expected surname!	Certyfikat nie posiada atrybutu: nazwisko (surname)!
BBB_XCV_ISCGGIVEN_ANS	The certificate has not expected given name!	Certyfikat nie posiada atrybutu: imię (name)!
BBB_XCV_ISCGPSEUDO_ANS	The certificate has not expected pseudonym!	Certyfikat nie posiada atrybutu: pseudonim (pseudonym)!
BBB_XCV_ISCGCOMMONN_ANS	The certificate has not expected common name!	Certyfikat nie posiada atrybutu: nazwa powszechna (common name)!
XCV_IFCCIIPC_ANS	The interval for the certificate is inconsistent in the prospective chain.	Interwał dla certyfikatu jest niespójny w przyszłym łańcuchu.
XCV_TSL_ESP_ANS	The trust service has not expected status!	Zaufana usługa ma nieodpowiedni status!
XCV_TSL_ESP_SIG_ANS	The trust service of the signing certificate has not expected status!	Zaufana usługa podpisywania certyfikatem ma nieodpowiedni status!
XCV_TSL_ESP_TSP_ANS	The trust service of the timestamp has not expected status!	Zaufana usługa wystawiania znaczników czasu ma nieodpowiedni status!

XCV_TSL_ESP_REV_ANS	The trust service of the revocation has not expected status!	Zaufana usługa unieważniania ma nieodpowiedni status!
XCV_TSL_ETIP_ANS	The trust service has not expected type identifier!	Zaufana usługa nie posiada odpowiedniego identyfikatora typu!
XCV_TSL_ETIP_SIG_ANS	The trust service of the signing certificate has not expected type identifier!	Zaufana usługa podpisywania certyfikatem ma nieodpowiedni identyfikator typu!
XCV_TSL_ETIP_TSP_ANS	The trust service of the timestamp has not expected type identifier!	Zaufana usługa wystawiania znaczników czasu ma nieodpowiedni identyfikator typu!
XCV_TSL_ETIP_REV_ANS	The trust service of the revocation has not expected type identifier!	Zaufana usługa unieważniania ma nieodpowiedni identyfikator typu!
PCV_IVTSC_ANS	The indications returned by validation time sliding sub-process.	Wskazania zostały zwrócone przed podproces kontroli przesunięcia czasu.
PSV_IPCVA_ANS	The past certificate validation is not acceptable!	Weryfikacja przeszłego certyfikatu nie jest rozstrzygająca!
PSV_IPCVC_ANS	The current time validation is not conclusive!	Weryfikacja przy użyciu bieżącego czasu nie jest rozstrzygająca!
PSV_IPSVC_ANS	The past signature validation is not conclusive!	Weryfikacja przeszłego podpisu nie jest rozstrzygająca!
PSV_ITPOOBCT_ANS	No Proof Of Existence found at (or before) control-time!	Brak potwierdzenia na istnienie w momencie weryfikacji lub na chwilę przed!
TSV_ASTPTCT_ANS	The timestamps were not generated in the right order!	Kolejność znaczników czasu nie jest prawidłowa!
TSV_IBSTAIDOSC_ANS	The best-signature-time is before the issuance date of the signing certificate!	Czas produkcji sygnatury nie znajduje się w okresie ważności certyfikatu!
TSV_ISCNVABST_ANS	The past signing certificate validation must be performed!	Musi zostać wykonana walidacja poprzedniego certyfikatu podpisującego!
ADEST_IRTPTBST_ANS	The revocation time is not posterior to best-signature-time!	Czas odwołania jest przed 'best-signature-time'!
ADEST_VFDTAOCST_ANS	The validation failed due to the absence of claimed signing time!	Weryfikacja nie powiodła się z powodu braku czasu podpisu!
ADEST_ISTPTDABST_ANS	The validation failed due to the timestamp delay constraint!	Weryfikacja nie powiodła się z powodu wymagań na czas uzyskanie znacznika czasu!
TSV_WACRABST_ANS	The algorithm(s) was not considered reliable at best-signature-time!	Algorytm nie był uważany za zaufany dla 'best-signature-time'!
LABEL_TINTWS	Additional assurance on the signing time may be needed to prove the validity of the signature.	Potrzeba dodatkowego zabezpieczenia dotyczącego czasu podpisania w celu potwierdzenia ważności podpisu.
LABEL_TINVTWS	There is no valid timestamp within the signature.	Brak znacznika czasu w podpisie.
VTS_IRC_ANS	The revocation data is not consistant!	Dane unieważnień nie są spójne!

VTS_ICTBRD_ANS	The issuance date of revocation data is not before control-time!	Data wystawienia unieważnień nie jest wcześniejsza niż data weryfikacji!
QUAL_TL_EXP_ANS	The trusted list is expired!	Lista zaufana wygasła!
QUAL_TL_FRESH_ANS	The trusted list is not fresh!	Lista zaufana nie jest nowa!
QUAL_TL_VERSION_ANS	The trusted list has not the expected version!	Lista zaufana nie ma oczekiwanej wersji!
QUAL_TL_WS_ANS	The trusted list is not well signed!	Lista zaufana nie jest prawidłowo podpisana!
QUAL_TL_SERV_CONS_ANS0	No CA/QC Trust service found.	Nie odnaleziono usługi zaufania CA/QC.
QUAL_TL_SERV_CONS_ANS1	Trust service not consistent! (QCStatement and NotQualified).	Usługa zaufania jest niespójna! (QCStatement and NotQualified).
QUAL_TL_SERV_CONS_ANS2	Trust service not consistent! (QCForLegalPerson and QCForeSig).	Usługa zaufania jest niespójna! (QCForLegalPerson and QCForeSig).
QUAL_TL_SERV_CONS_ANS3	Trust service not consistent! (X_QSCD and NotQSCD).	Usługa zaufania jest niespójna! (QSCDStatusAsInCert and X_QSCD).
QUAL_TL_SERV_CONS_ANS4	Trust service not consistent! (incompatible usages of QCForeSig, QCForeSeal, QCForWSA).	Usługa zaufania jest niespójna (niezgodne zastosowania QCForeSig, QCForeSeal, QCForWSA).
QUAL_TL_SERV_CONS_ANS5	Trust service not consistent! (invalid additional service info / qualifier in service before 1/7/16).	Usługa zaufania jest niespójna (nieprawidłowe dodatkowe informacje o usłudze / kwalifikator w serwisie przed 1/7/16).
QUAL_TL_SERV_CONS_ANS6	Trust service not consistent! (conflict between additional service info and qualifier).	Usługa zaufania jest niespójna (konflikt między dodatkowymi informacjami o usłudze i kwalifikatorem).
QUAL_TRUSTED_CERT_PATH_ANS	A trusted path can not be built based TSL list!	Nie można zbudować zaufanej ścieżki w oparciu o listę TSL!
QUAL_TRUSTED_LIST_ACCEPT_ANS	The trusted list is not acceptable!	Lista zaufana jest nie do przyjęcia!
QUAL_QC_AT_ST_ANS	Certificate is not marked as qualified at the moment of sigining (eIDAS context).	Certyfikat nie jest oznaczony jako kwalifikowany w momencie podpisywania (w kontekście eIDAS).
QUAL_FOR_SIGN_AT_ST_ANS	Certificate is not marked as intended for electronic signature or eSeal, at the moment of signing (eIDAS context).	Certyfikat, w momencie podpisywania, nie jest oznaczony jako przeznaczony do ePodpisu ani pieczęci (w kontekście eIDAS).
QUAL_QC_AT_CC_ANS	Certificate is not qualified at the moment of issue (eIDAS context).	Certyfikat nie jest kwalifikowany w momencie wystawienia (w kontekście eIDAS).
QUAL_UNIQUE_CERT_ANS	The certificate cannot be defined as unique!	Certyfikat nie może być zdefiniowany jako unikalny!
QUAL_QSCD_AT_ST_ANS	The signature/seal is not created by a QSCD!	Certyfikat nie został utworzony przez urządzenie QSCD!
QUAL_IS_ADES_IND	Signature can not be determined as ETSI EN 319 102-1 compliant!	Podpis nie może zostać określony jako zgodny z ETSI EN 319 102-1!

QUAL_IS_ADES_INV	Signature structure is incorrect!	Podpis ma niepoprawną strukturę!
QUAL_TL_CERT_CONS_ANS1	Certificate is presented as QC for the stamp, while the Q status is not provided for the electronic stamp.	Certyfikat przedstawia się jako QC dla pieczęci, podczas gdy status Q nie jest zapewniony dla pieczęci elektronicznej.
QUAL_TL_CERT_CONS_ANS2	Inconsistency in TL - Cert claimed as QC for WSA while Q status not granted for WSA, digital signature generated with cert. for WSA considered as special case of AdESeal.	Niespójność w TL - Cert zgłoszona jako QC dla WSA, podczas gdy status Q nie został przyznany dla WSA, podpis cyfrowy generowany za pomocą cert. dla WSA uznany za szczególny przypadek AdESeal.
QUAL_TL_CERT_CONS_ANS3	Inconsistency in TL - Cert claimed as QC for eSig while Q status not granted for electronic Sig.	Niespójność w TL - Cert zgłoszona jako QC dla eSig, podczas gdy status Q nie jest przyznany dla elektronicznego Sig.
TSL_NOT_INITIALIZED	The TSL structure has not been initialized by the server yet.	Struktura TSL nie została jeszcze zainicjalizowana przez serwer.
TSP_INVALID_SIGNATURE	Invalid signature for timestamp.	Niepoprawny znacznik czasu.
UNABLE_TO_REFRESH_TSL	There was a problem occurred during refreshing TSL.	Wystąpił problem podczas odświeżania TSL.
pades.unsigned.addons	The document was changed after signing. Some unsigned addons were added to signed document.	Po podpisaniu wprowadzono zmiany nieobjęte podpisem.

7.3.5 Raport z wynikiem weryfikacji

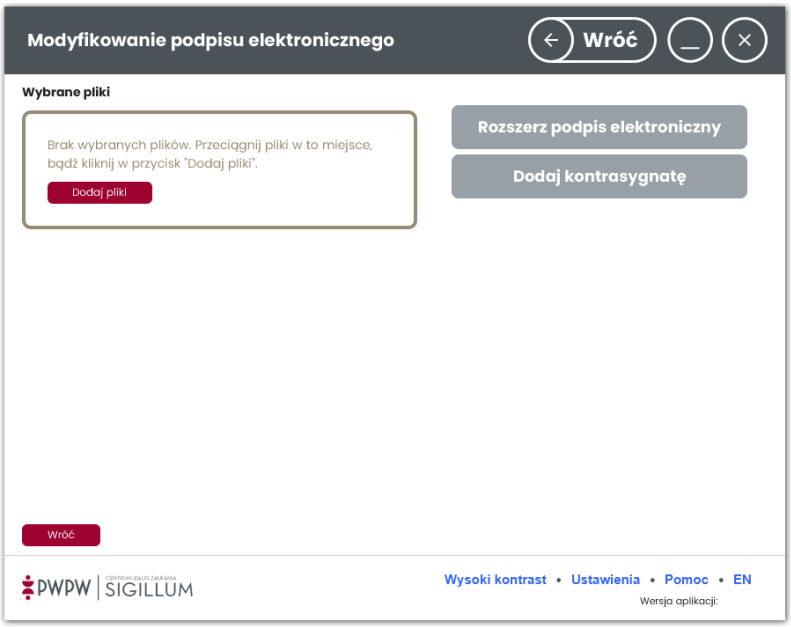
Po kliknięciu **Pobierz raport** na ekranie wyniku weryfikacji, użytkownik może wybrać jeden z dwóch dostępnych formatów raportu: PDF lub XML.

W raporcie znajdują się wszystkie informacje dotyczące wyniku weryfikacji oraz weryfikowanego pliku m.in. **Suma kontrolna pliku podpisu (SHA-256)**. Jest to wynik konwersji HEX -> ASCII a następnie zakodowania BASE64 sumy kontrolnej podpisanego pliku.

7.4 Proces operacji zaawansowanych

7.4.1 Ekran startowy procesu zaawansowane

Wywołanie operacji modyfikacji podpisu (już istniejącego) odbywa się przez kliknięcie przycisku ***„Rozszerzony”*** na stronie głównej a następnie kliknięcie kafelka **„Zaawansowane”**. Wywołanie funkcjonalności może odbyć się również przez akcję *Przeciągnij i upuść* wybrane pliki na obszar **„Zaawansowane”**.



Po dodaniu plików do obszaru roboczego, pliki prezentowane są w formie kafelków wraz z danymi je opisującymi. Kafelki zawierają następujące informacje: *Nazwa dokumentu, Status oraz rozmiar*.

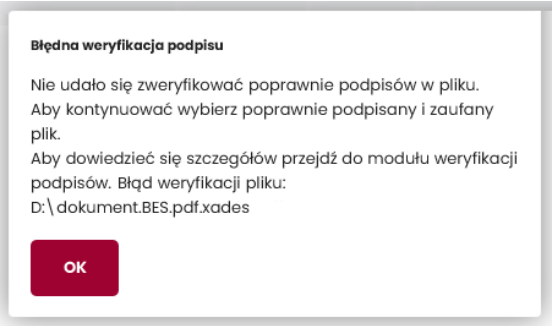
Możliwe statusy dodanego pliku to: podpisany, niepodpisany, za duży rozmiar (patrz ROZMIAR).

W zależności od formatu/typu/wariantu dodanych plików, odpowiednie przyciski akcji staną się aktywne lub nieaktywne, aplikacja pozwoli na wykonanie wybranych podpisów, co przedstawia poniższa tabela.

Format/typ/wariant modyfikowanego podpisu	**Rozszerz podpis elektroniczny**			**Dodaj kontrasygnatę**			
	T	**XL**	**A**	**BES**	**T**	**XL**	**A**
XAdES Zewnętrzny BES	TAK	TAK	TAK	TAK	TAK		TAK
XAdES Zewnętrzny T		TAK	TAK	TAK	TAK		TAK
XAdES Zewnętrzny XL		TAK	TAK	TAK	TAK		TAK
XAdES Zewnętrzny A			TAK	TAK	TAK		TAK
XAdES Otaczający BES	TAK	TAK	TAK	TAK	TAK		TAK
XAdES Otaczający T		TAK	TAK	TAK	TAK		TAK
XAdES Otaczający XL		TAK	TAK	TAK	TAK		TAK
XAdES Otaczający A			TAK	TAK	TAK		TAK

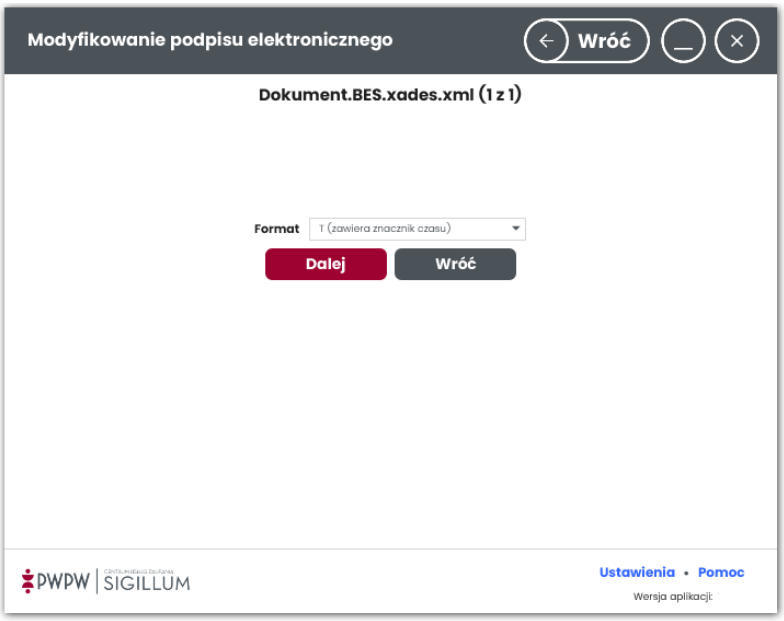
XAdES Otoczony BES	TAK	TAK	TAK	TAK	TAK		TAK
XAdES Otoczony T		TAK	TAK	TAK	TAK		TAK
XAdES Otoczony XL		TAK	TAK	TAK	TAK		TAK
XAdES Otoczony A			TAK	TAK	TAK		TAK
PAdES Otoczony BES	TAK	TAK	TAK				
PAdES Otoczony T		TAK	TAK				
PAdES Otoczony XL		TAK	TAK				
PAdES Otoczony A			TAK				
CAdES Zewnętrzny BES	TAK	TAK	TAK	TAK			
CAdES Zewnętrzny T		TAK	TAK	TAK			
CAdES Zewnętrzny XL		TAK	TAK	TAK			
CAdES Zewnętrzny A			TAK	TAK			
CAdES Otaczający BES	TAK	TAK	TAK	TAK			
CAdES Otaczający T		TAK	TAK	TAK			
CAdES Otaczający XL		TAK	TAK	TAK			
CAdES Otaczający A			TAK	TAK			
ASiCS Otoczony BES	TAK	TAK	TAK	TAK			
ASiCS Otoczony T		TAK	TAK	TAK			
ASiCS Otoczony XL		TAK	TAK	TAK			
ASiCS Otoczony A			TAK	TAK			
ASiCE Otoczony BES	TAK	TAK	TAK	TAK			
ASiCE Otoczony T		TAK	TAK	TAK			
ASiCE Otoczony XL		TAK	TAK	TAK			
ASiCE Otoczony A			TAK				

W przypadku, gdy po dodaniu plików i wybraniu opcji zaawansowanej nie ma dostępu do Internetu, wyświetlony zostaje następujący komunikat. Skorzystanie z opcji zaawansowanych nie jest wtedy możliwe.



7.4.2 Rozszerz podpis elektroniczny

Po dodaniu pliku w odpowiednim formacie/typie/wariancie i wyborze opcji ***„Rozszerz podpis elektroniczny”*** użytkownikowi prezentowany jest ekran rozszerzania podpisu elektronicznego.



Na ekranie znajduje się informacja dot. liczby plików wybranych do rozszerzenia (1 z 1), gdzie pierwsza liczba mówi, który plik jest obecnie rozszerzany, druga liczba prezentuje liczbę wszystkich rozszerzanych plików z podpisem.

Użytkownik może wybrać jeden z 3 formatów rozszerzenia: T, XL, A, w zależności od formatu/typu/wariantu rozszerzanego podpisu, co przedstawia TABELA.

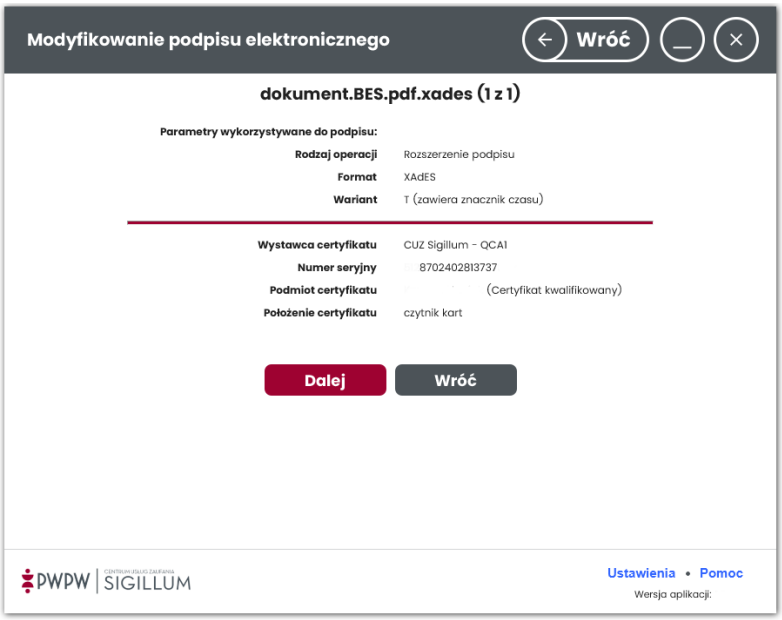
Po wyborze formatu rozszerzenia i kliknięciu przycisku Dalej prezentowany jest ekran wyboru karty i certyfikatu.

Wybór karty to wskazanie biblioteki pkcs11 umieszczonej w określonej lokalizacji. Jeśli biblioteki nie ma w określonej lokalizacji, wyświetlone zostaje okno wyboru pliku. Po wskazaniu poprawnego pliku pkcs11 do listy wyboru karty zostaje dodana nowa pozycja.

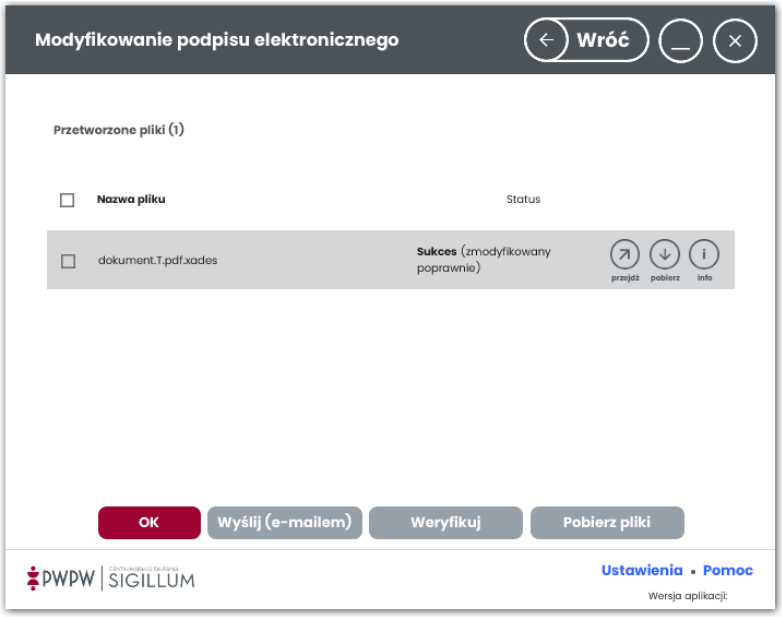
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny. Po wyborze certyfikatu, pojawia się informacja na temat certyfikatu i skutku prawnego wywołanego jego użyciem.

Po kliknięciu ***„Dalej”*** system otwiera okno wprowadzenia kodu PIN.

Po wpisaniu poprawnego kodu PIN i kliknięciu ***„Potwierdź”***, system prezentuje ekran parametrów wykorzystanych do wykonania podpisu.



Po kliknięciu ***„Dalej”*** prezentowany jest ekran końcowy, potwierdzający przebieg operacji.



W kolumnie „Status" wyświetlany jest status otrzymany po wykonaniu operacji, w wierszu każdego podpisanego pliku znajdują się ikony:

- przejdź – prezentacja (niepodpisanego) pliku źródłowego podpisu,
- pobierz – zapisanie (niepodpisanego) pliku źródłowego podpisu,
- info – szczegóły złożonego podpisu.

Po zaznaczeniu checkboxa w wierszu wybranych plików można wysłać podpisane dokumenty poprzez e-mail klikając przycisk Wyślij (e-mailem).

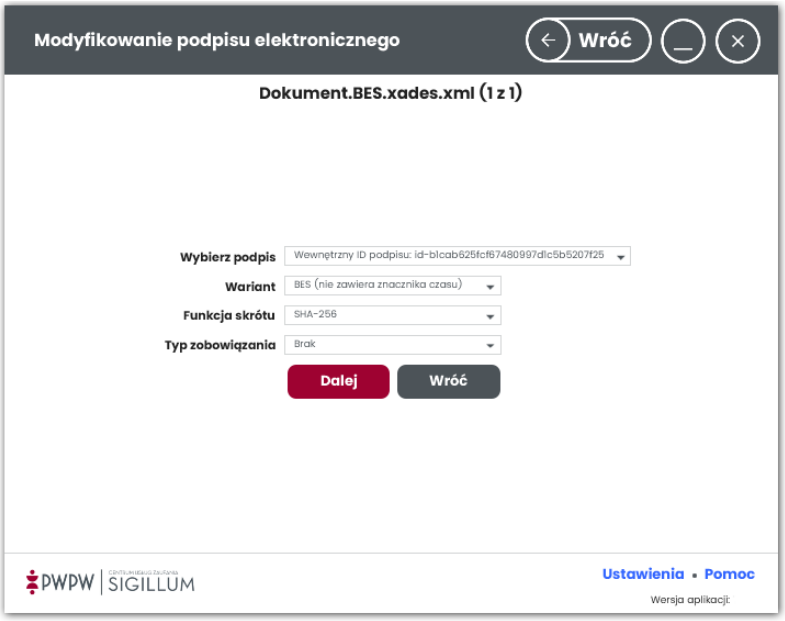
Po kliknięciu przycisku Weryfikuj wyświetlany jest ekran weryfikacji podpisanych plików.

Potwierdzenie (OK) kończy proces podpisywania. Podpisane pliki odnaleźć można w folderach, gdzie znajdują się pliki źródłowe. Podpis można zweryfikować w procesie weryfikacji.

7.4.3 Dodaj kontrasygnatę

Wybranie opcji *Dodaj kontrasygnatę* oznacza, że do podpisu, przyporządkowanego do pliku dodany zostanie kolejny potwierdzający integralność treści (podpis kontrasygnujący).

Użytkownik wybiera podpis do zastąpienia oraz określa *Wariant*, *Funkcję skrótu* i *Typ zobowiązania*.

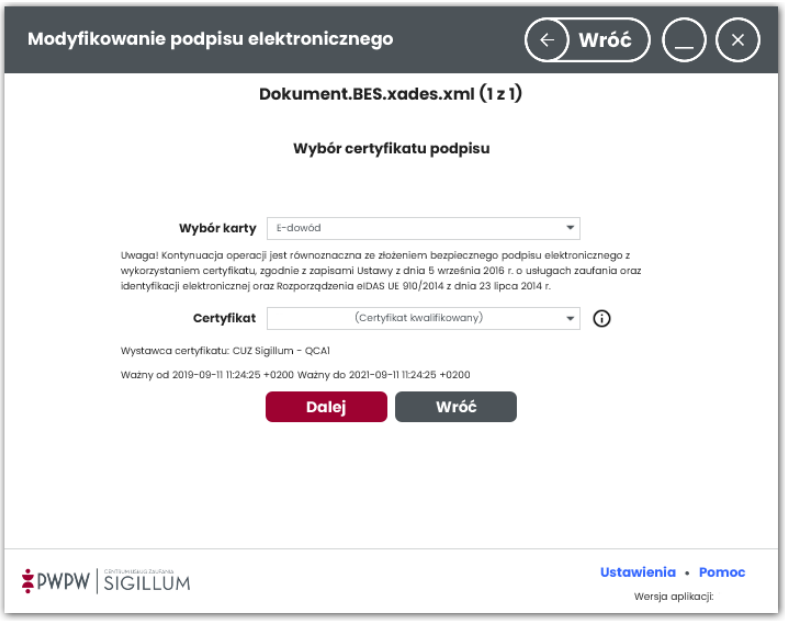


Użytkownik może wybrać jeden z 3 wariantów: BES, T, A, w zależności od formatu/typu/wariantu kontrasygnowanego podpisu, co przedstawia TABELA.

Po kliknięciu przycisku Dalej, prezentowany jest ekran wyboru karty i certyfikatu.

Wybór karty to wskazanie biblioteki pkcs11 umieszczonej w określonej lokalizacji. Jeśli biblioteki nie ma w określonej lokalizacji, wyświetlone zostaje okno wyboru pliku. Po wskazaniu poprawnego pliku pkcs11 do listy wyboru karty zostaje dodana nowa pozycja.

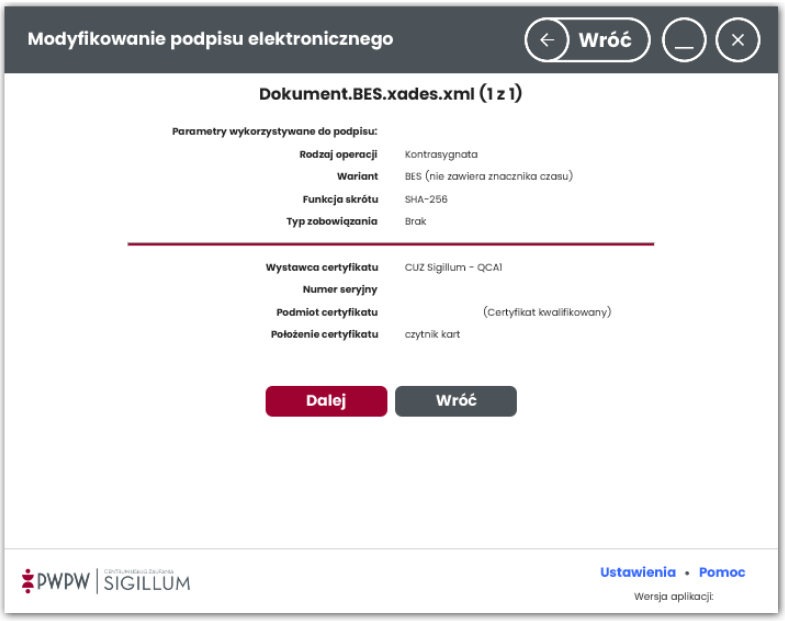
Po wyborze karty i certyfikatu, pojawia się informacja na temat certyfikatu i skutku prawnego wywołanego jego użyciem.



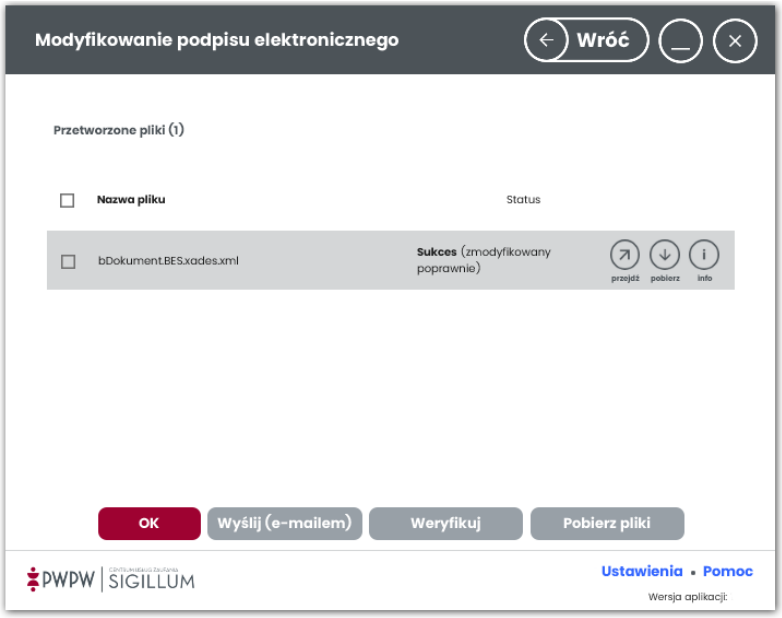
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny.

Po kliknięciu ***„Dalej”*** system otwiera okno wprowadzenia kodu PIN.

Po wpisaniu poprawnego kodu PIN i kliknięciu ***„Potwierdź”***, system prezentuje ekran parametrów wykorzystanych do wykonania podpisu.



Po kliknięciu ***„Dalej”*** prezentowany jest ekran końcowy, potwierdzający przebieg operacji.



W kolumnie „Status” wyświetlany jest status otrzymany po wykonaniu operacji, w wierszu każdego podpisanego pliku znajdują się ikony:

- przejdź – prezentacja (niepodpisanego) pliku źródłowego podpisu,
- pobierz – zapisanie (niepodpisanego) pliku źródłowego podpisu,
- info – szczegóły złożonego podpisu.

Po zaznaczeniu checkboxa w wierszu wybranych plików można wysłać podpisane dokumenty poprzez e-mail klikając przycisk Wyślij (e-mailem).

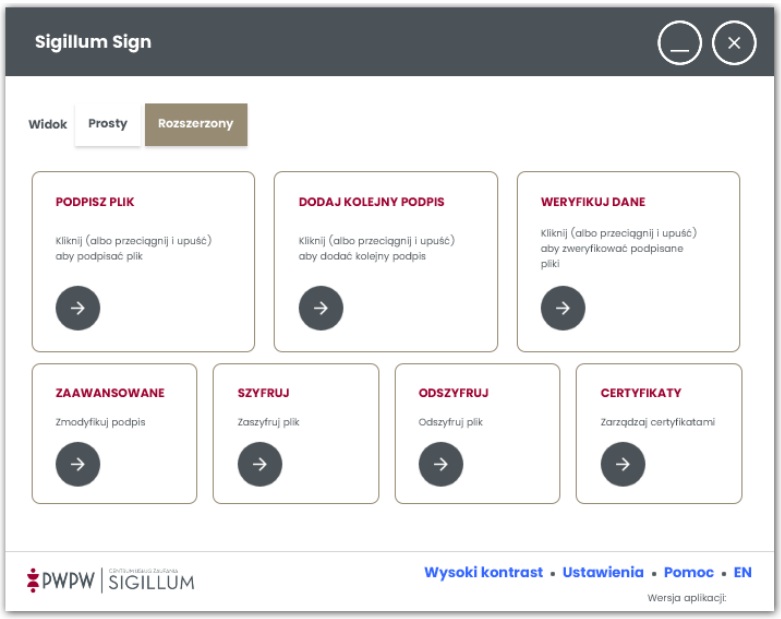
Po kliknięciu przycisku Weryfikuj wyświetlany jest ekran weryfikacji podpisanych plików.

Potwierdzenie (OK) kończy proces podpisywania. Podpisane pliki odnaleźć można w folderach, gdzie znajdują się pliki źródłowe. Podpis można zweryfikować w procesie weryfikacji.

7.5 Szyfrowanie plików

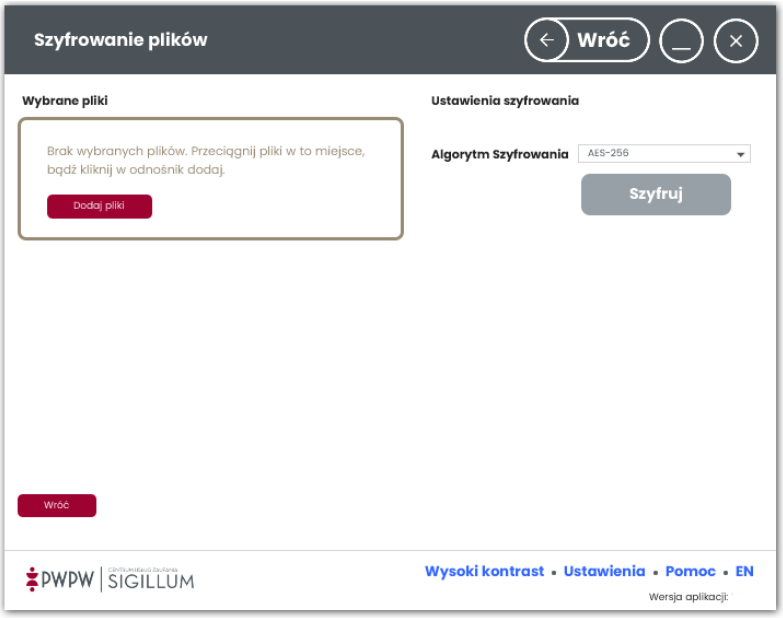
7.5.1 Ekran startowy procesu szyfrowania

Wywołanie operacji szyfrowania odbywa się przez kliknięcie kafelka ***„Szyfruj”*** w widoku rozszerzonym strony głównej. Zmiana widoku strony głównej odbywa się przy użyciu przycisku „Rozszerzony”. Funkcjonalność uruchomić można również przez akcję *Przeciągnij i upuść* wybrany plik na obszar.



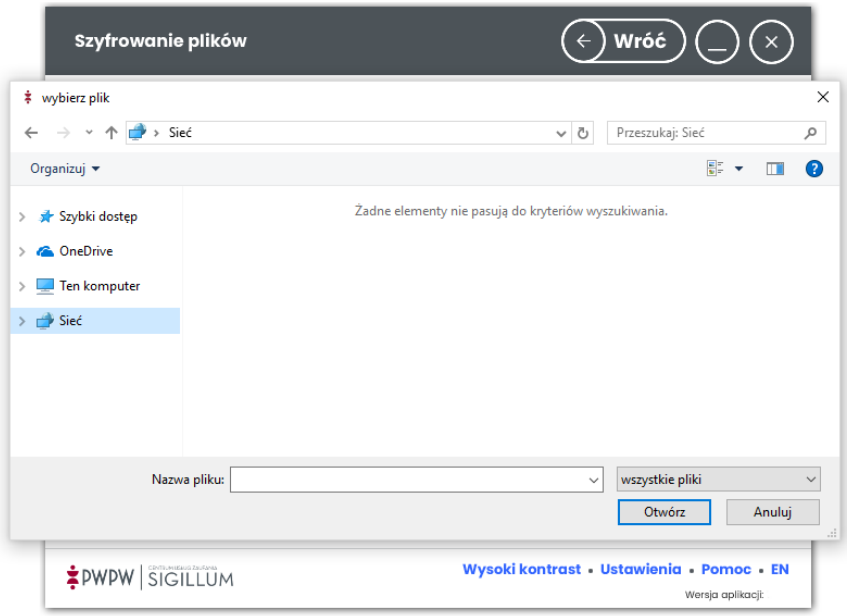
7.5.2 Ekran ustawień szyfrowania

Po wyborze opcji ***„Szyfruj”*** użytkownikowi prezentowany jest ekran szyfrowania.

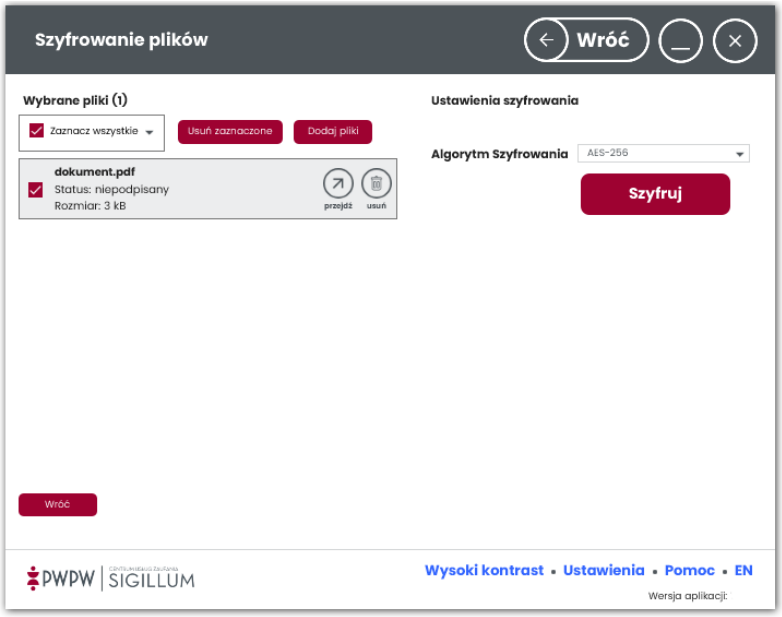


Ekran podzielony jest na dwie części: lewą tzw. obszar roboczy, w którym prezentowane są pliki oraz prawą tzw. obszar ustawień, zawierający ustawienia związane z szyfrowaniem oraz przycisk ***„Szyfruj”***.

Aby zaszyfrować plik użytkownik musi dodać plik/ki do obszaru roboczego. Dodanie pliku/plików może odbyć się na dwa sposoby: przez użycie przycisku Dodaj pliki lub funkcję przeciągnij-upuść. Po kliknięciu opcji ***Dodaj pliki*** pojawi się okno przeglądania zawartości stacji roboczej użytkownika.



Po dodaniu plików do obszaru roboczego, pliki prezentowane są w formie kafelków wraz z danymi je opisującymi.



Kafelki zawierają następujące informacje: *Nazwa dokumentu, Status oraz rozmiar.*

Możliwe statusy dodanego pliku to: podpisany, niepodpisany, za duży rozmiar (patrz ROZMIAR).

Po kliknięciu w ikonę ***przejdź*** można otworzyć plik.

Kliknięcie w ikonę ***usuń*** pozwala usunąć plik z obszaru roboczego.

Aby rozpocząć proces szyfrowania, należy wybrać algorytm szyfrowania, po zaznaczeniu właściwego pliku użytkownik klika przycisk ***„Szyfruj"***.

Po wykonaniu tej czynności prezentowany jest kolejny widok Ekran szyfrowania.

7.5.3 Ekran szyfrowania

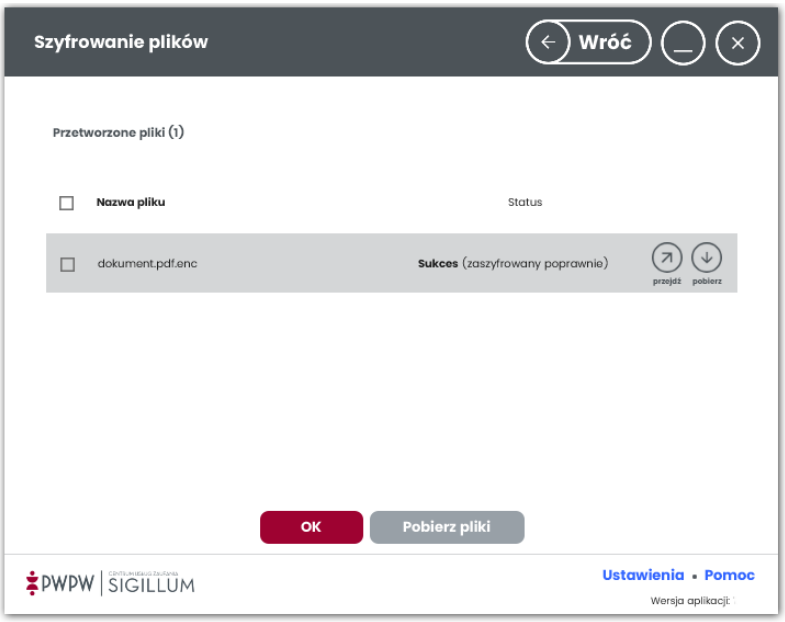
Okno szyfrowania prezentuje użytkownikowi dostępne certyfikaty służące do szyfrowania plików.

Odpowiedni komunikat przypomina użytkownikowi o tym by wskazał swój certyfikat, aby w przyszłości móc odczytać konkretny plik.

UWAGA!

Istnieje również możliwość zaszyfrowania pliku kluczem publicznym odbiorcy (wyszukujemy i dodajemy certyfikat zgodnie z punktem 6.7), do którego chcemy przekazać zaszyfrowany plik. Wówczas odbiorca odszyfrowuje plik swoim certyfikatem (kluczem prywatnym).

Po wybraniu przycisku OK, prezentowany jest ekran końcowy z wynikiem szyfrowania.



W kolumnie „Status" wyświetlany jest status otrzymany po wykonaniu operacji. Dostępne są następujące ikony:

- przejdź – prezentacja (niezaszyfrowanego) pliku źródłowego,

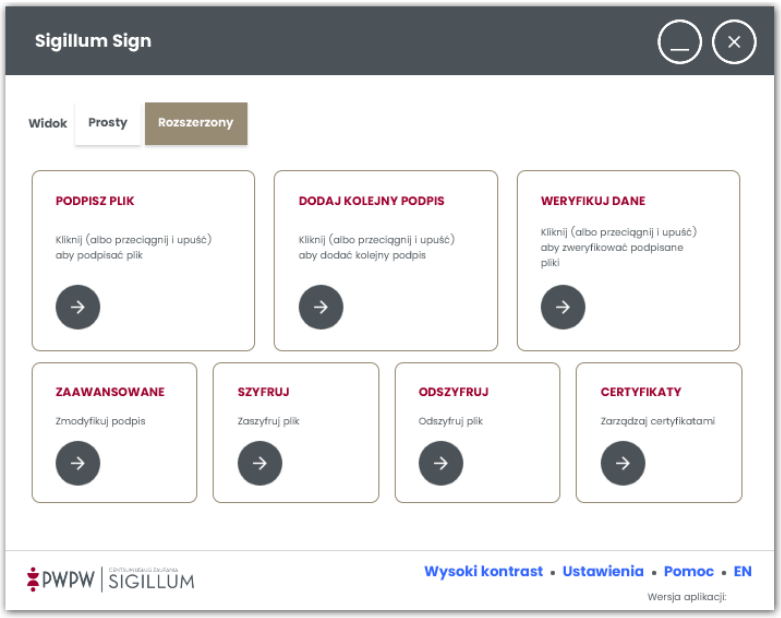
- pobierz – zapisanie (niezaszyfrowanego) pliku źródłowego.

Potwierdzenie (OK) kończy proces szyfrowania. Zaszyfrowane pliki odnaleźć można w folderach, gdzie znajdują się pliki źródłowe.

7.6 Odszyfrowywanie plików

7.6.1 Ekran startowy procesu odszyfrowania

Wywołanie operacji odszyfrowania odbywa się przez kliknięcie kafelka ***„Odszyfruj”*** w widoku rozszerzonym strony głównej lub akcję *Przeciągnij i upuść* wybrany plik na obszarze.



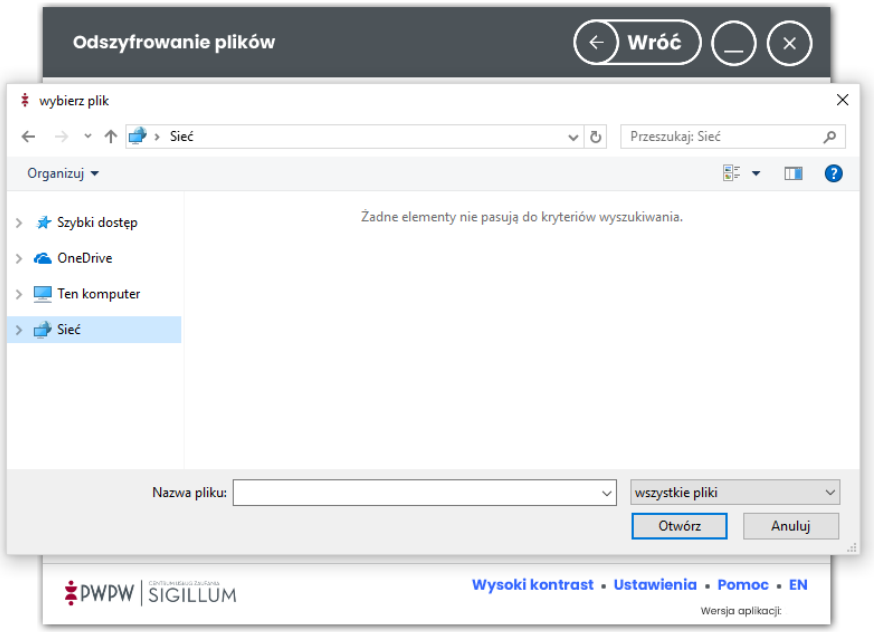
7.6.2 Ekran ustawień odszyfrowania

Po wyborze opcji ***„Odszyfruj”*** użytkownikowi prezentowany jest ekran odszyfrowania plików.

Okno podzielone jest na dwie części: lewą tzw. obszar roboczy, w którym prezentowane są pliki oraz prawą zawierającą przycisk ***„Odszyfruj”***.

Aby dodać podpis użytkownik musi dodać plik/ki do obszaru roboczego. Dodanie pliku/plików może odbyć się na dwa sposoby: przez użycie przycisku Dodaj pliki lub funkcję przeciągnij-upuść.

Po kliknięciu opcji ***Dodaj pliki*** pojawi się okno przeglądania zawartości stacji roboczej użytkownika.



Po dodaniu plików do obszaru roboczego, pliki prezentowane są w formie kafelków wraz z danymi je opisującymi.

Kafelki zawierają następujące informacje: *Nazwa dokumentu, Status oraz rozmiar.*

Możliwe statusy dodanego pliku to: podpisany, niepodpisany, szyfrowany, za duży rozmiar (patrz ROZMIAR).

Po kliknięciu w ikonę przejdź można otworzyć zaszyfrowany plik.

Kliknięcie w ikonę kosza pozwala usunąć plik z obszaru roboczego.

Aby rozpocząć proces deszyfrowania, należy zaznaczyć plik i kliknąć przycisk ***„Odszyfruj”***.

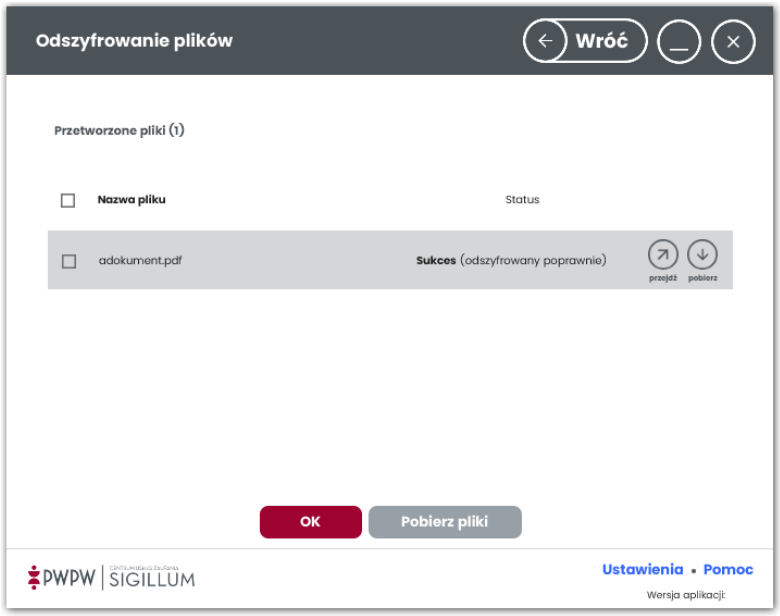
Po wykonaniu tej czynności prezentowany jest kolejny widok Ekran szyfrowania.

7.6.3 Ekran odszyfrowania

Po wyborze opcji ***„Odszyfruj”*** użytkownik przeniesiony zostaje do ekranu wyboru karty i certyfikatu.

Po wyborze karty prezentowane są certyfikaty, przy użyciu których będzie można odszyfrować zaznaczone plik/ki.

Po wyborze certyfikatu i kliknięciu Dalej należy podać PIN, system odszyfrowuje plik i wyświetla ekran podsumowania.



W kolumnie „Status" wyświetlany jest status otrzymany po wykonaniu operacji. Dostępne są następujące ikony:

- przejdź – prezentacja (niezaszyfrowanego) pliku źródłowego,
- pobierz – zapisanie (niezaszyfrowanego) pliku źródłowego.

Potwierdzenie (OK) kończy proces szyfrowania. Zaszyfrowane pliki odnaleźć można w folderach, gdzie znajdują się pliki źródłowe.

8 Aplikacja linii komend

8.1 Wprowadzenie

Aplikacja linii komend stanowi rozszerzenie aplikacji interfejsu graficznego. Jej zadaniem jest dostarczenie funkcji PKI dla środowiska, w którym wykorzystanie interfejsu graficznego nie jest możliwe.

8.2 Wymagania aplikacji

Minimalne wymagania sprzętowe dla systemu operacyjnego użytkownika aplikacji:

- procesor o taktowaniu 2 gigaherc (GHz) lub szybszy,
- przynajmniej 4 gigabajt (GB) pamięci RAM,
- 970 megabajtów (MB) przestrzeni na dysku twardym,
- minimalna rozdzielczość: 1024x768px, 16bit,
- skonfigurowane połączenie internetowe,
- jeden port USB 2.0,
- czytnik kart elektronicznych USB.

Wymagania programowe dla stacji roboczej użytkownika aplikacji:

- Microsoft Windows 7, 8, 10 (64bit),
- Sterowniki dla czytnika,
- Oprogramowanie do obsługi karty:
    - Sigillum Manager
    - Active Client w wersji 5.4 i wyższej
    - Sigillum Card
    - Gemalto Classic Client w wersji 6 i wyższej
- Aplikacja do odczytu dokumentów pdf.

8.3 Uruchamianie aplikacji

Po instalacji należy uruchomić aplikację sigillum.exe i ustawić w Ustawieniach domyślną kartę do podpisu (patrz 6.5.5.1) a następnie wyłączyć aplikację sigillum.exe.

Aplikacja linii komend dystrybuowana jest w pełnej wersji instalacji w postaci pliku sigillumCli.exe

Aplikacja uruchamiana jest następująco:

sigillumCli.exe <przełącznik_aplikacji>

Np.
sigillumCli.exe –help

8.4 Lista przełączników wywołania aplikacji

Polecenia wydawane są aplikacji za pośrednictwem listy przełączników. Lista dostępnych poleceń znajduje się w poniższej tabeli.

Nazwa polecenia	Skrót polecenia	Przeznaczenie
-help	--h	Wyświetla pomoc aplikacji.
-certlist	--cl	Prezentuje listę certyfikatów w magazynie certyfikatów.
-ctlist	--ctl	Prezentuje listę dostępnych wartości dla atrybutu Commitment Type Indication określającego charakter składanego podpisu elektronicznego.
-signinfo	--si	Prezentuje informacje o podpisie elektronicznym zapisanym we wskazanym pliku.
-sign	--s	Podpisuje wskazany plik.
-addsign	--as	Dodanie podpisu równoległego.
-addcs	--acs	Dodanie kontrasygnaty do podpisu elektronicznego.
-verify	--v	Weryfikuje podpis elektroniczny zawarty we wskazanym pliku.
-enc	--e	Szyfruje dane zawarte we wskazanym pliku.
-dec	--d	Odszyfrowuje dane zawarte we wskazanym pliku.
-prlist	--prl	Prezentuję listę dostępnych wartości dla atrybutu Pades Reason.

8.5 Przełącznik –help

Użycie tego polecenia powoduje wyświetlenie pomocy aplikacji w postaci listy przełączników i opcji, które użytkownik może wykorzystać.

Przykład wywołania:
sigillumCli.exe –help

8.6 Przełącznik -certlist

Użycie tego polecenia powoduje wyświetlenie listy certyfikatów wraz z kluczami prywatnymi, które są dostępne dla danej operacji. Polecenie zwraca listę certyfikatów wraz z numerem certyfikatu na liście certyfikatów. Numerem tym należy się posługiwać przy wywoływaniu innych przełączników aplikacji (opisano to w kolejnych rozdziałach podręcznika).

Parametrem polecenia jest typ operacji, jaka może zostać wykonana danym certyfikatem.

Parametr	Skrót parametru	Dopuszczalne wartości	Opis
-operation	--o	sign encrypt decrypt	Rodzaj operacji

Przykładowa lista certyfikatów:

```
[0] Jan Kowalski | kwalifikowany | 061cd6 | czytnik kart | 2013-12-13
12:52:05 - 2015-12-13 12:52:05
[1] Jan kowalski | komercyjny | 052aa3 | czytnik kart | 2013-12-13
12:45:55 - 2015-12-13 12:45:55
```

Numer certyfikatu znajduje się pomiędzy znakami „[ ]" np. „[0]".

Przykład wywołania:

sigillumCli.exe –certlist –operation decrypt

8.7 Przełącznik –ctlist

Użycie tego polecenia prezentuje listę dostępnych wartości dla atrybutu Commitment Type Indication określającego charakter składanego podpisu elektronicznego. Polecenie zwraca listę wartości wraz z numerem na liście. Numerem tym należy się posługiwać przy wywoływaniu innych przełączników aplikacji (opisano to w kolejnych rozdziałach podręcznika).

Przykładowa lista wartości:

```
[0] Brak
[1] Dowód pochodzenia (proof of origin)
[2] Potwierdzenie odbioru (proof of receipt)
[3] Dowód dostawy (proof of delivery)
[4] Dowód nadawcy (proof of sender)
[5] Formalne potwierdzenie (proof of approval)
[6] Potwierdzenie utworzenia (proof of creation)
```

Numer wartości znajduje się *pomiędzy znakami „[ ]" np. „[0]".*

Przykład wywołania:

sigillumCli.exe –ctlist

8.8 Przełącznik -prlist

Użycie tego polecenia prezentuje listę dostępnych wartości dla atrybutu Pades Reason określającego Powód składanego podpisu elektronicznego wyłącznie w formacie PAdES. Polecenie zwraca listę wartości wraz z numerem na liście. Numerem tym należy się posługiwać przy wywoływaniu przełączników sign, addsign (opisano to w kolejnych rozdziałach podręcznika).

Przykładowa lista wartości:

```
[0] Brak
[1] Jestem autorem tego dokumentu
[2] Przejrzałem ten dokument
[3] Zatwierdzam ten dokument
[4] Potwierdzam dokładność i integralność tego dokumentu
[5] Zgadzam się ze zdefiniowanymi warunkami przez umieszczenie podpisu w
tym dokumencie
[6] Zgadzam się na określenie podziału dokumentu
```

Numer wartości znajduje się *pomiędzy znakami „[ ]" np. „[0]".*

Przykład wywołania:
sigillumCli.exe -prlist

8.9 Przełącznik –signinfo

Użycie tego polecenia prezentuje informacje o podpisie elektronicznym zapisanym we wskazanym pliku. Parametrem polecenia jest ścieżka do podpisanego pliku.

Wywołanie:
sigillumCli.exe –signinfo –f <ścieżka do pliku>

Parametry:

Parametr	Skrót parametru	Dopuszczalne wartości	Opis
-f	-	Nie dotyczy	Ścieżka do pliku z podpisem elektronicznym

Przykład wywołania:
sigillumCli.exe –signinfo –f "c:\podpis.txt.xades"

8.10 Przełącznik –sign

Użycie tego polecenia umożliwia podpisanie wskazanego pliku

Wywołanie:
sigillumCli.exe -sign -format [XAdES, CAdES, PAdES] -variant [BES, T, A, XL] –type [ENVELOPED, ENVELOPING, DETACHED] -hash [SHA1, SHA256, SHA384, SHA512] -cert <numer certyfikatu z listy dla operacji sign> -pin <kod pin do karty> -ct <typ potwierdzenia, numer z listy ctlist> -pr <pades reason, numer z listy prlist> -f <ścieżka do pliku>

Argumenty:

Argument	Dopuszczalne wartości	Opis
-format	XAdES CAdES PAdES	Format podpisu elektronicznego.
-variant	BES T A XL	Wariant podpisu.
-type	ENVELOPED ENVELOPING DETACHED	Określa sposób powiązania podpisywanych danych z podpisem elektronicznym.
-hash	SHA1 SHA256 SHA384 SHA512	Określa rodzaj funkcji skrótu, która my być wykorzystana przy składaniu podpisu elektronicznego.
-cert	Wartości liczbowe większe lub równe 0	Numer certyfikatu na liście certyfikatów, która może być wykorzystana do składania podpisu elektronicznego. Patrz przełącznik –certlist.
-pin	Kod pin do karty	Wartość kodu pin do karty kryptograficznej.

-ct	Wartości liczbowe większe lub równe 0	Numer wartości Commitment Type Indication, która może być wykorzystana do składania podpisu elektronicznego. Patrz przełącznik –ctlist.
-pr	Wartości liczbowe większe lub równe 0	Numer wartości Pades Reason, która może być wykorzystana do składania podpisu elektronicznego. Patrz przełącznik -prlist.
-f	Nie dotyczy	Ścieżka do pliku, który ma zostać podpisany.

Przykład wywołania:
sigillumCli.exe -sign -format XAdES -variant BES -type ENVELOPING -hash SHA256 -cert 7 -pin 1111 -ct 1 -pr 0 -f "D:\podpis.txt"
sigillumCli.exe -sign -format XAdES -variant T -type ENVELOPING -hash SHA256 -cert 7 -pin 1111 -cert 7 -pin 1111 -ct 1 -pr 0 -f "D:\podpis.txt"

8.11 Przełącznik –addsign

Użycie tego polecenia umożliwia dodanie kolejnego podpisu elektronicznego do wskazanego pliku z podpisem.

Wywołanie:
sigillumCli.exe -addsign -format [XAdES, CAdES, PAdES] -variant [BES, T, A, XL] –type [ENVELOPED, ENVELOPING, DETACHED] -hash [SHA1, SHA256, SHA384, SHA512] -cert <numer certyfikatu z listy dla operacji sign> -pin <kod pin do karty> -ct <typ potwierdzenia, numer z listy ctlist> -pr <pades reason, numer z listy prlist> -f <ścieżka do pliku> -of <ścieżka do pliku źródłowego>

Argumenty:

Argument	Dopuszczalne wartości	Opis
-format	XAdES CAdES PAdES	Format podpisu elektronicznego.
-variant	BES T	Wariant podpisu.
-type	ENVELOPED ENVELOPING	Określa sposób powiązania podpisywanych danych z podpisem elektronicznym.

	DETACHED	
-hash	SHA1 SHA256 SHA384 SHA512	Określa rodzaj funkcji skrótu, która my być wykorzystana przy składaniu podpisu elektronicznego.
-cert	Wartości liczbowe większe lub równe 0	Numer certyfikatu na liście certyfikatów, która może być wykorzystana do składania podpisu elektronicznego. Patrz przełącznik –certlist.
-pin	Kod pin do karty	Wartość kodu pin do karty kryptograficznej.
-ct	Wartości liczbowe większe lub równe 0	Numer wartości Commitment Type Indication, która może być wykorzystana do składania podpisu elektronicznego. Patrz przełącznik –ctlist.
-pr	Wartości liczbowe większe lub równe 0	Numer wartości Pades Reason, która może być wykorzystana do składania podpisu elektronicznego. Patrz przełącznik -prlist.
-f	Nie dotyczy	Ścieżka do pliku z podpisem elektronicznym lub folderu.
-of	Ścieżka do pliku źródłowego (podpisywanego)	Wymagany podczas dodawania kolejnego podpisu do pliku z podpisem zewnętrznym (DETACHED)

Przykłady wywołania:
sigillumCli.exe -addsign -format XAdES -variant BES -type ENVELOPING -hash SHA256 -cert 1 -pin 1111 -ct 1 -pr 0 -f "D:\podpis.BES.txt.xades"

sigillumCli.exe -addsign -format XAdES -variant BES -type DETACHED -hash SHA256 -cert 1 -pin 1111 -ct 1 -pr 0 -f "D:\podpis.BES.txt.xades" -of "D:\podpis.txt"

8.12 Przełącznik –addcs

Użycie tego polecenia umożliwia dodanie kontrasygnaty do podpisu elektronicznego zawartego we wskazanym pliku.

Wywołanie:
sigillumCli.exe -addcs -sigid [identyfikator_podpisu] -variant [BES, T, A, XL] -type [ENVELOPED, ENVELOPING, DETACHED] -hash [SHA1, SHA256, SHA384, SHA512] -cert <numer certyfikatu z listy> -pin <kod pin do karty> -pr <pades reason, numer z listy prlist> -f <ścieżka lub ścieżki do pliku lub katalogów> -of <ścieżka do pliku źródłowego>

Argumenty:

Argument	Dopuszczalne wartości	Opis
- sigid	Wartości liczbowe większe lub równe 0	Numer podpisu elektronicznego zawartego w pliku z podpisem, który będzie kontrasygnowany. W celu uzyskania tego numeru należy uprzednio wywołać aplikację z przełącznikiem -signinfo.
-variant	BES T A XL	Wariant podpisu.
-type	ENVELOPED ENVELOPING DETACHED	Określa sposób powiązania podpisywanych danych z podpisem elektronicznym. Należy wybrać zgodny z kontrasygnowanym podpisem.
-hash	SHA1 SHA256 SHA384 SHA512	Określa rodzaj funkcji skrótu, która my być wykorzystana przy składaniu podpisu elektronicznego.
-cert	Wartości liczbowe większe lub równe 0	Numer certyfikatu na liście certyfikatów, która może być wykorzystana do składania podpisu elektronicznego. Patrz przełącznik –certlist.
-pin	Kod pin do karty	Wartość kodu pin do karty kryptograficznej.
-ct	Wartości liczbowe większe lub równe 0	Numer wartości Commitment Type Indication, która może być wykorzystana do

		składania podpisu elektronicznego. Patrz przełącznik –ctlist.
-f	Nie dotyczy	Ścieżka do pliku z podpisem elektronicznym lub folderu.
-of	Ścieżka do pliku źródłowego (podpisywanego)	Wymagany podczas dodawania kontrasygnaty do pliku z podpisem zewnętrznym (DETACHED).

Przykłady wywołania:
sigillumCli.exe -addcs -sigid 0 -variant BES -type ENVELOPING -hash SHA256 -cert 1 -pin 1111 -ct 1 -pr 0 -f "D:\podpis.BES.txt.xades"

sigillumCli.exe -addcs -sigid 0 -variant BES -type DETACHED -hash SHA256 -cert 1 -pin 1111 -ct 1 -pr 0 -f "D:\podpis.BES.txt.xades" -of "D:\podpis.txt"

8.13 Przełącznik –verify

Użycie tego polecenia wykonuje proces weryfikacji podpisów elektronicznych zawartych we wskazanym pliku z podpisem elektronicznym.

Wywołanie:
sigillumCli.exe -verify -f <ścieżka lub ścieżki do pliku lub katalogów> -of <ścieżka do pliku źródłowego> -raport

Argumenty:

Argument	Dopuszczalne wartości	Opis
-f	Nie dotyczy	Ścieżka do pliku z podpisem elektronicznym lub katalogów
-of	Ścieżka do pliku źródłowego (podpisywanego)	Wymagany podczas weryfikacji podpisów zewnętrznych (DETACHED)
-raport	Nie dotyczy	Tworzy szczegółowy raport w pliku pdf, w tej samej lokalizacji co weryfikowany plik

Przykłady wywołania:
sigillumCli.exe -verify -f "c:\podpis.txt.xades" -raport
sigillumCli.exe -verify -f "D:\dokument1.BES.pdf.xades" -of "D:\dokument1.pdf" -raport

8.14 Przełącznik –enc

Użycie tego polecenia wykonuje proces szyfrowania danych zawartych we wskazanym pliku.

Wywołanie:
sigillumCli.exe -enc -alg <nazwa_algorytmu> -f <ścieżka do pliku> -cert <certyfikaty odbiorców szyfrowanej informacji w formie numerów z listy certyfikatów dla operacji encrypt>

Argumenty:

Argument	Dopuszczalne wartości	Opis
-f	Nie dotyczy	Ścieżka do pliku, które ma być zaszyfrowany.
-alg	DES 3DES AES-128	Nazwa algorytmu który zostanie wykorzystany do zaszyfrowania informacji.
-cert	Wartości liczbowe większe lub równe 0	Certyfikaty odbiorców szyfrowanej informacji w formie numerów z listy certyfikatów dla operacji encrypt. Patrz przełącznik –certlist.

Przykład wywołania:
sigillumCli.exe -enc -alg AES-128 -cert 0 -f "D:\podpis.txt"

8.15 Przełącznik –dec

Użycie tego polecenia wykonuje proces odszyfrowania danych zawartych we wskazanym pliku.

Wywołanie:
sigillumCli.exe -dec -cert <numer certyfikatu z listy> -pin < Wartość kodu pin do karty kryptograficznej> -f <ścieżka do pliku> -r <ścieżka pliku wynikowego>

Argumenty:

Argument	Dopuszczalne wartości	Opis
-f	Nie dotyczy	Ścieżka do pliku, które ma być odszyfrowany.
-cert	Wartości liczbowe większe lub równe 0	Numer certyfikatu na liście certyfikatów dla operacji decrypt. Patrz przełącznik –certlist.

-pin	Kod pin do karty	Wartość kodu pin do karty kryptograficznej.
-r	Nie dotyczy	Ścieżka do pliku, w którym ma być zapisana odszyfrowana informacja.

Przykład wywołania:

sigillumCli.exe -dec –cert 0 -pin 111111 -f "C:\plik.png.enc" –r "C:\plik-odszyfrowany.txt"