PWPW

POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH

PODRĘCZNIK UŻYTKOWNIKA APLIKACJI SIGILLUM SIGN

WERSJA DOKUMENTU: 1.4
WERSJA OPROGRAMOWANIA: 1.4
DATA AKTUALIZACJI: 2019-11-29

Informacje prawne

Prawa autorskie do aplikacji „Sigillum Sign" oraz do dokumentu „Podręcznik użytkownika" należą do Polskiej Wytwórni Papierów Wartościowych S.A. zwanej zamiennie PWPW S.A. z siedzibą w Warszawie, przy ulicy Sanguszki 1.

Polska Wytwórnia Papierów Wartościowych S.A. oświadcza, że wszelkie prawa autorskie dotyczące niniejszej dokumentacji są zastrzeżone, łącznie z tłumaczeniem na języki obce. Zabronione jest publikowanie, wykorzystywanie i rozpowszechniane niniejszej dokumentacji w jakiejkolwiek formie bez zgody PWPW S.A .

Powyższe prawa są chronione ustawą o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24, poz. 83 z dnia 4 lutego 1994 roku z późniejszymi zmianami).

Dokumentacja jest dystrybuowana na podstawie udzielonej licencji.

1 Spis treści

Informacje prawne 2
1 Spis treści 3
2 Wstęp 6
3 Przeznaczenie aplikacji 7
3.1 Wymagania sprzętowe 8
4 Słownik 9
5 Instalacja aplikacji 15
5.1 Instalacja na systemach operacyjnych Ms Windows 15
6 Obsługa aplikacji 20
6.1 Strona główna – widok prosty 20
6.2 Strona główna – widok rozszerzony 21
6.3 Wysoki kontrast 21
6.4 Ustawienia 22
6.4.1 Znacznik PDF 23
6.4.2 Aktualizacje 24
6.4.3 Czas 25
6.4.4 Proxy 25
6.4.5 PKI 26
6.4.6 Usługi sieciowe 34
6.4.7 Tryby podpisu 35
6.4.8 Inne 35
6.5 Pomoc 36
6.6 Certyfikaty 37
7 Operacje PKI 39
7.1 Składanie podpisu 39
7.1.1 Ekran startowy procesu podpisu 39
7.1.2 Ekran składania podpisu i ustawień podpisu 40
7.1.3 Dodanie pliku do obszaru roboczego 41
7.1.4 Ekran wyboru certyfikatów i złożenie podpisu 45
7.1.5 Podpisanie wielu plików 48
7.1.6 Podpisanie pliku PAdES ze znacznikiem 49

7.2 Dodaj kolejny podpis ... 52
7.2.1 Ekran początkowy procesu weryfikacji ... 52
7.2.2 Ekran procesu dodawania kolejnego podpisu ... 53
7.2.3 Dodanie pliku do obszaru roboczego ... 54
7.2.4 Ekran wyboru certyfikatów i złożenie podpisu ... 55
7.3 Weryfikacja podpisu ... 57
7.3.1 Ekran początkowy procesu weryfikacji ... 57
7.3.2 Ekran weryfikacji i ustawień ... 58
7.3.3 Dodanie pliku do obszaru roboczego ... 58
7.3.4 Ekran weryfikacji ... 60
7.4 Proces operacji zaawansowanych ... 61
7.4.1 Ekran startowy procesu zaawansowane ... 61
7.4.2 Zastąp istniejący podpis nowym ... 62
7.4.3 Rozszerz podpis elektroniczny ... 65
7.4.4 Dodaj kontrasygnatę ... 68
7.4.5 Dodaj znacznik czasu ... 71
7.5 Szyfrowanie plików ... 73
7.5.1 Ekran startowy procesu szyfrowania ... 73
7.5.2 Ekran ustawień szyfrowania ... 73
7.5.3 Ekran szyfrowania ... 75
7.6 Odszyfrowywanie plików ... 77
7.6.1 Ekran startowy procesu odszyfrowania ... 77
7.6.2 Ekran ustawień odszyfrowania ... 77
7.6.3 Ekran odszyfrowania ... 79
8 Aplikacja linii komend ... 81
8.1 Wprowadzenie ... 81
8.2 Wymagania aplikacji ... 81
8.3 Uruchamianie aplikacji ... 81
8.4 Lista przełączników wywołania aplikacji ... 82
8.5 Przełącznik –help ... 82
8.6 Przełącznik -certlist ... 83
8.7 Przełącznik –ctlist ... 83
8.8 Przełącznik –signinfo ... 84

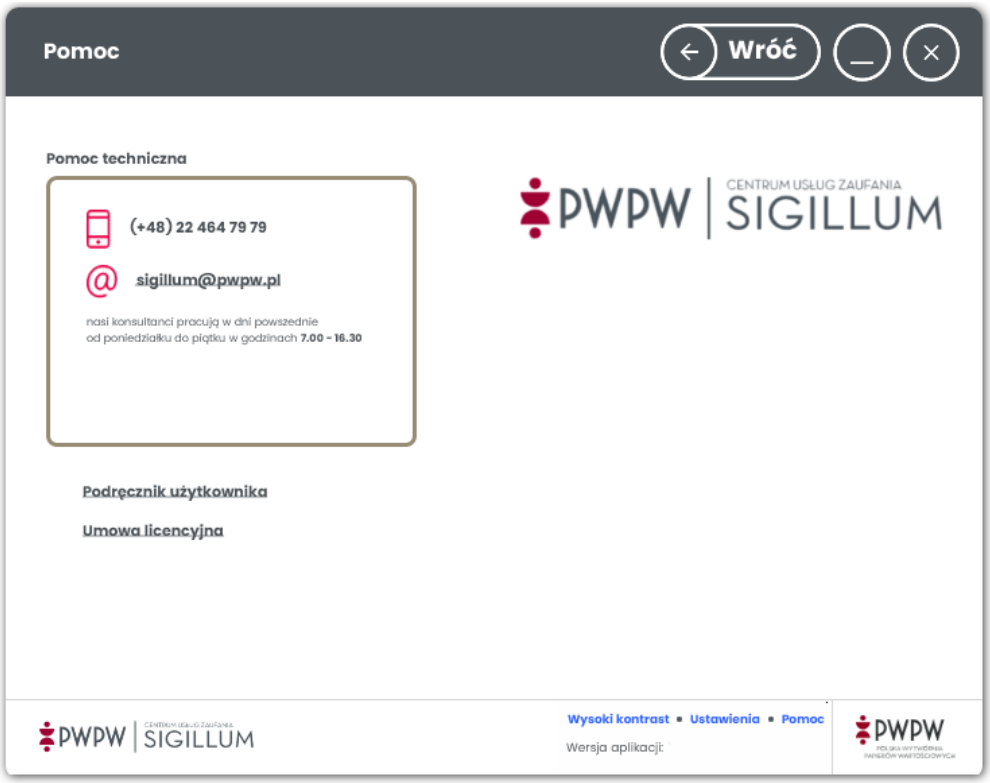
8.9 Przełącznik –sign 84
8.10 Przełącznik –addsign 86
8.11 Przełącznik –addcs 87
8.12 Przełącznik –verify 89
8.13 Przełącznik –enc 89
8.14 Przełącznik –dec 90

2 Wstęp

Niniejszy dokument jest wersją 1.4 Podręcznika użytkownika aplikacji „Sigillum Sign". Podręcznik użytkownika w obecnej postaci dotyczy wersji 1.4.

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

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,
- 800 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 7 (64 bit),
- sterowniki oraz oprogramowanie do obsługi czytnika/karty,
- aplikacja do odczytu dokumentów pdf.

4 Słownik

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

- **ASiC (ang. Application Specific Integrated Circuit)**

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:

- ***ASiC-S (Simple)*** - służy on do przechowywania jednego zestawu danych oraz kilku powiązanych z nim podpisów, przy czym podpisy te muszą zwierać się w jednej strukturze.
- ***ASiC-E (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.

- **Bezpieczny podpis elektroniczny (wg UoPE)**

Jest to podpis elektroniczny:
- przyporządkowany wyłącznie do osoby składającej go,
- sporządzany za pomocą bezpiecznych urządzeń i danych służących do jego złożenia, podlegających wyłącznej kontroli osoby składającej ten podpis,
- powiązany z danymi, do których został dołączony w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest zauważalna.

- **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.

- **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 (wg UoPE)**

Certyfikat spełniający warunki określone w Ustawie o Podpisie Elektronicznym, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w tejże Ustawie.

- **Kwalifikowany podmiot świadczący usługi**

To podmiot świadczący usługi certyfikacyjne i wpisany do rejestru kwalifikowanych podmiotów realizujących ww. usługi. Musi on spełniać szereg warunków technicznych i organizacyjnych określonych przez ROZPORZĄDZENIE RADY MINISTRÓW z dnia 7 sierpnia 2002 r. mających na celu przede wszystkim bezpieczeństwo i pewność wystawianych certyfikatów.

- **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**

Zgodnie z definicją ustawową (Art. 3 Ustawy z dnia 18 września 2001r. o podpisie elektronicznym, Dz. U. Nr 130, Poz. 1450, z dnia 15.11.2001r.) są to informacje w postaci cyfrowej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane służą do identyfikacji osoby składającej podpis elektroniczny.

- **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 (wg UoPE)**

Sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający złożenie podpisu lub poświadczenia elektronicznego przy wykorzystaniu danych służących do składania podpisu lub poświadczenia elektronicznego.

- **Urządzenie służące do weryfikacji podpisu elektronicznego (wg UoPE)**

Sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający identyfikację osoby fizycznej, która złożyła podpis elektroniczny przy wykorzystaniu danych służących do weryfikacji podpisu elektronicznego lub w sposób umożliwiający identyfikację podmiotu świadczącego usługi certyfikacyjne bądź organu wydającego zaświadczenia certyfikacyjne przy wykorzystaniu danych służących do weryfikacji poświadczenia elektronicznego.

- **Usługi certyfikacyjne (wg UoPE)**

Wydawanie certyfikatów, znakowanie czasem lub inne usługi związane z podpisem elektronicznym.

- **UoPE (Ustawa o Podpisie Elektronicznym)**

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dziennik Ustaw z dnia 15 listopada 2001 r.), określająca warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych oraz zasady nadzoru nad podmiotami świadczącymi te usługi.

- **Uwierzytelnienie (ang. authentication)**

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

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

Urząd realizujący usługę certyfikacyjną oznaczania czasem przedstawionego skrótu dokumentu elektronicznego.

- **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.

- **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.

- **Znakowanie czasem (wg UoPE)**

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.

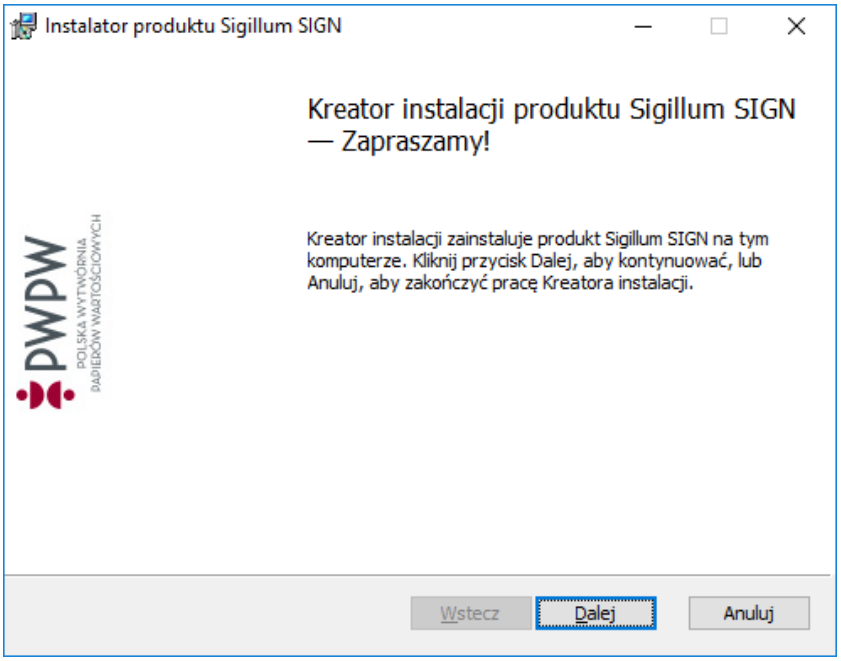
- **Zaświadczenie certyfikacyjne**

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.

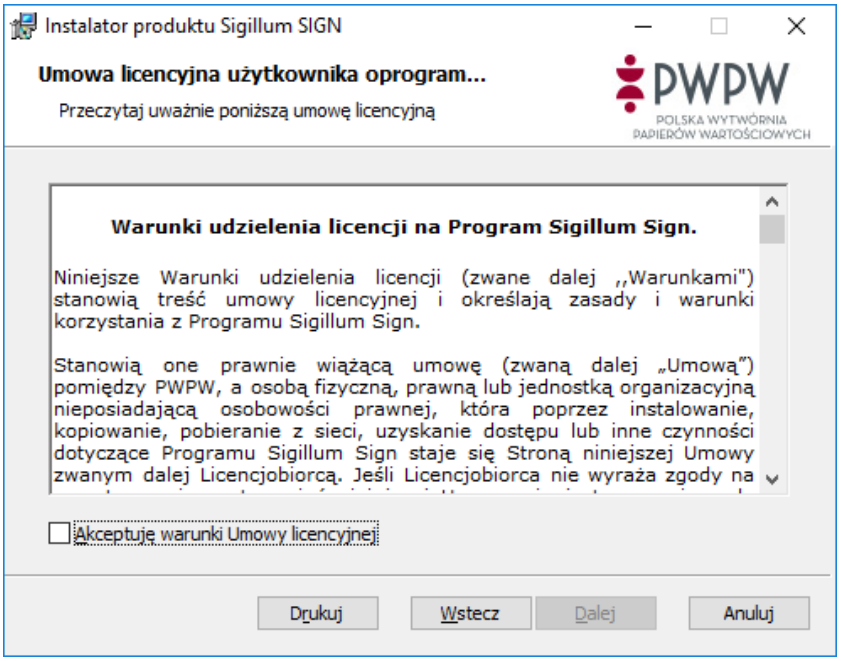
5 Instalacja aplikacji

5.1 Instalacja na systemach operacyjnych Ms Windows

Po uruchomieniu instalatora pojawia się okno informacyjne z przyciskami nawigacyjnymi:



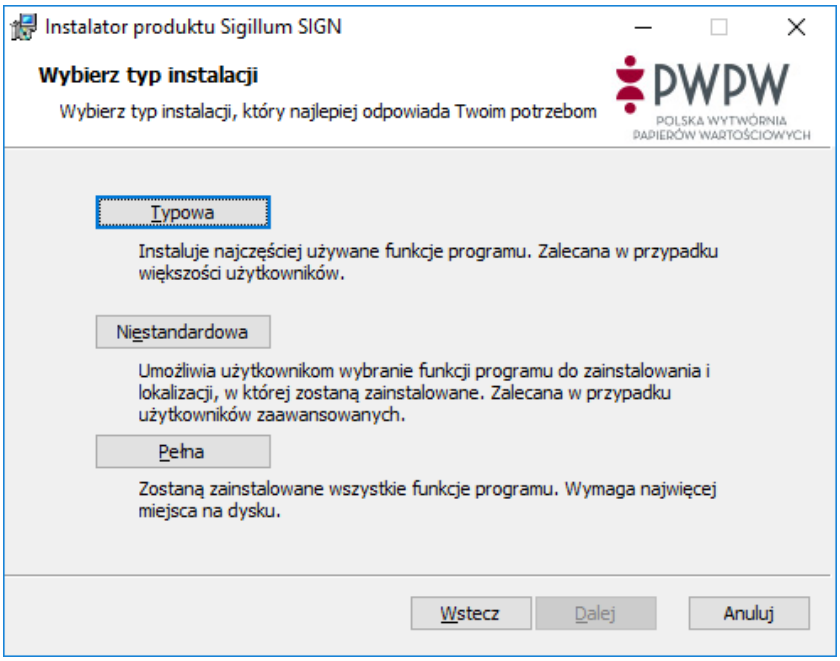
Kliknięcie przycisku *Dalej* powoduje wyświetlenie ekranu z Umową licencyjną:



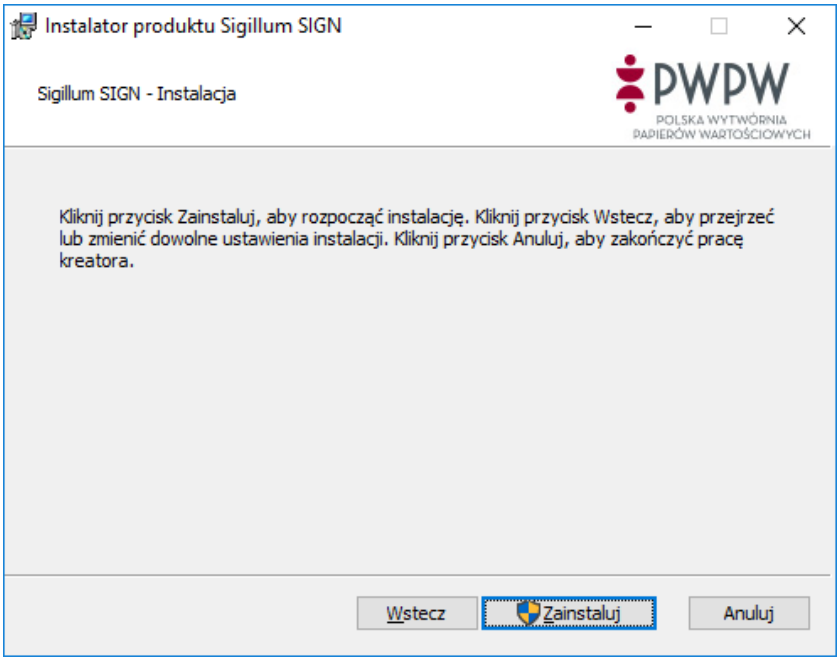
Po przeczytaniu umowy i zaznaczeniu akceptacji jej warunków przycisk *Dalej* umożliwia przejście do kolejnego kroku.

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

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

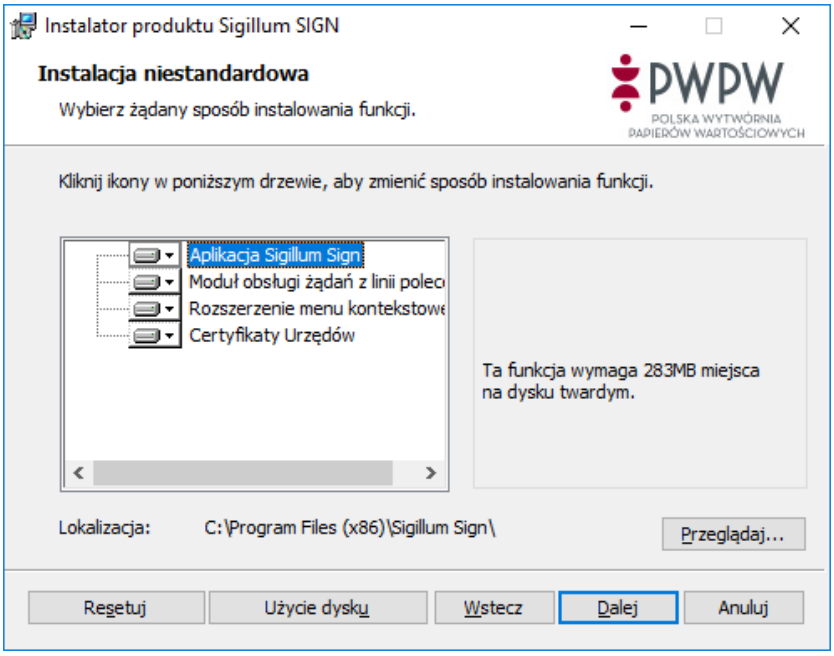


Po wybraniu opcji Typowa lub Pełna, instalator wyświetla okno potwierdzenia instalacji.

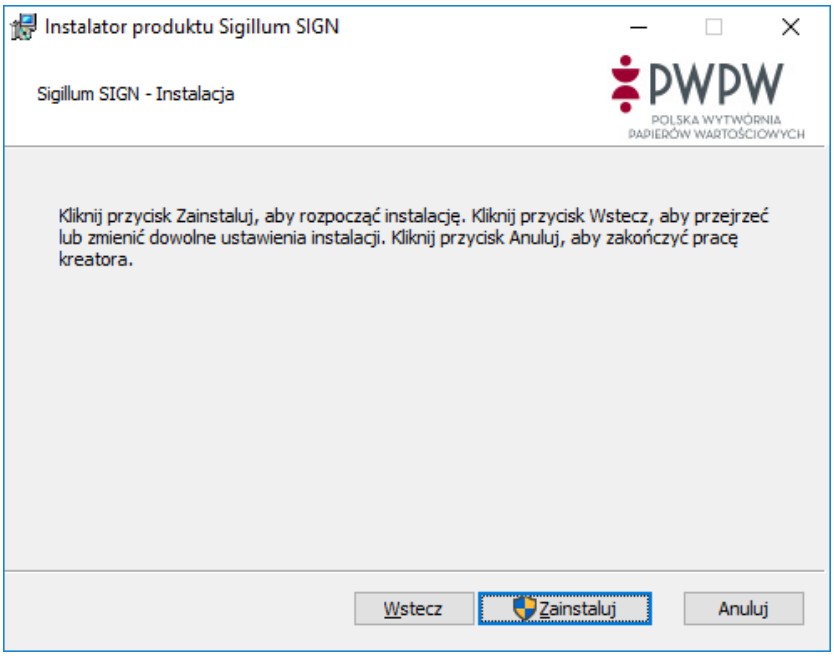


W przypadku, gdy zostanie wybrana opcja *Niestandardowa*, instalator wyświetli okno, w którym należy wybrać, które ze składników aplikacji zostaną zainstalowane.

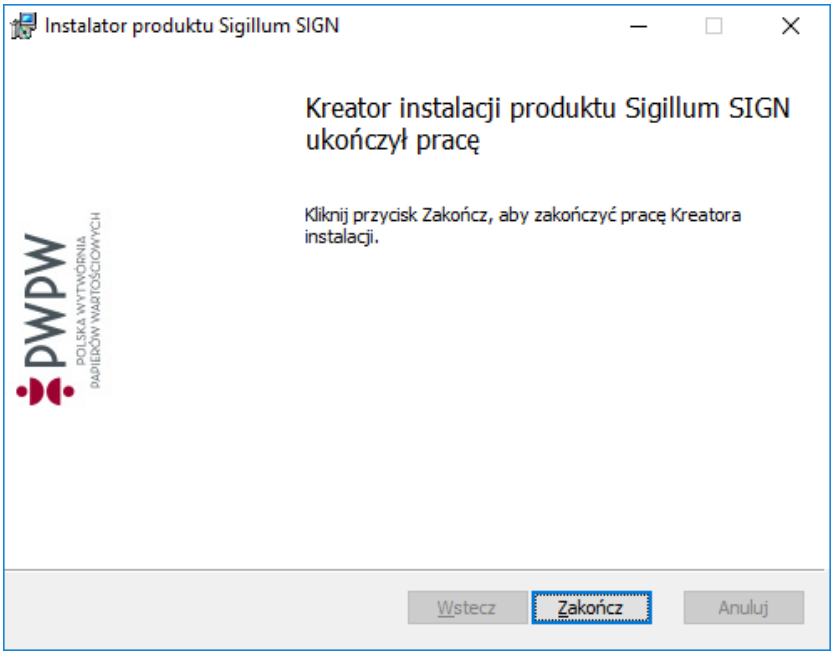
Można też wskazać miejsce na dysku, w którym aplikacja zostanie zainstalowana.



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

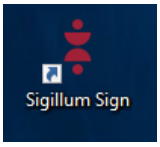


Po zakończeniu procesu instalacji, pojawia się okno potwierdzające pomyślną instalację aplikacji:



Kliknięcie przycisku *Zakończ* kończy proces instalacji.

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



UWAGA!

Mając zainstalowaną starszą wersję aplikacji, instalator wykrywa ją oraz dodatkowo wyświetla informację dla użytkownika z komunikatem o możliwości odinstalowania i zastąpienia wcześniejszej wersji.

6 Obsługa aplikacji

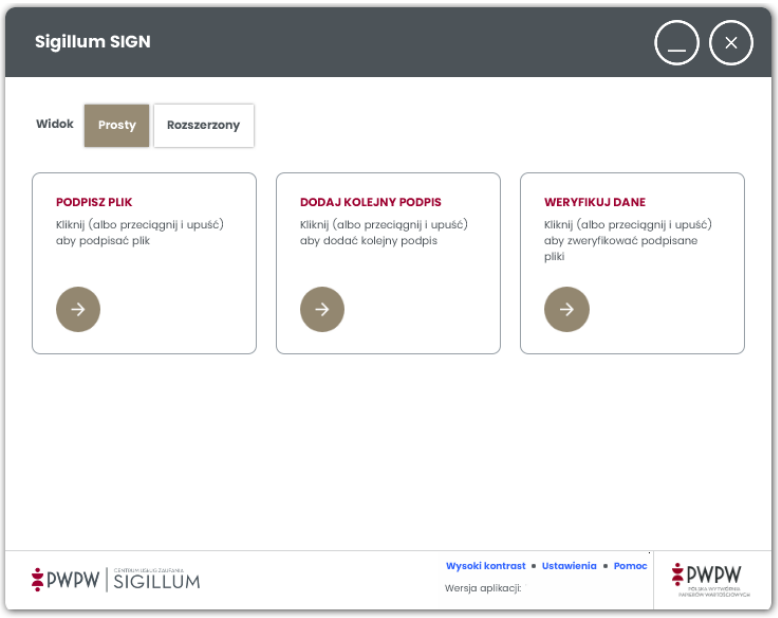
6.1 Strona główna – widok prosty

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.

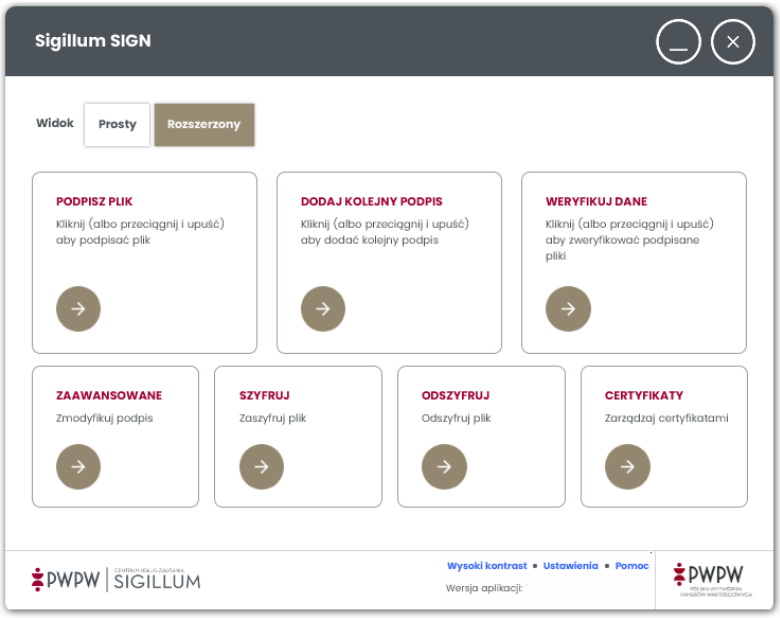


Po prawej stronie dolnego paska umieszczone są stałe polecenia aplikacji tj. ***Wysoki kontrast***, ***Ustawienia*** i ***Pomoc.***

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

6.2 Strona główna – widok rozszerzony

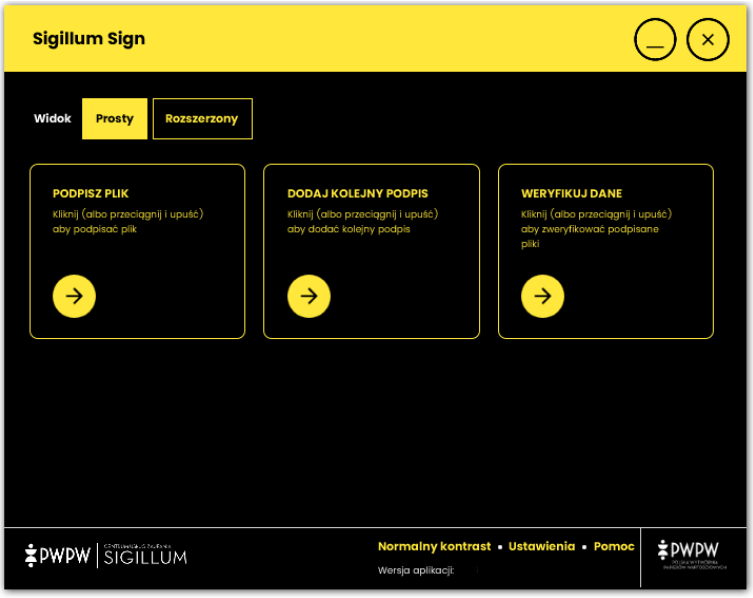
Poza kafelkami ***Podpisz plik***, ***Dodaj kolejny podpis*** oraz ***Weryfikuj dane***, *dostępne* są jeszcze ***Zaawansowane, Szyfruj***, ***Odszyfruj*** oraz ***Certyfikaty***.



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

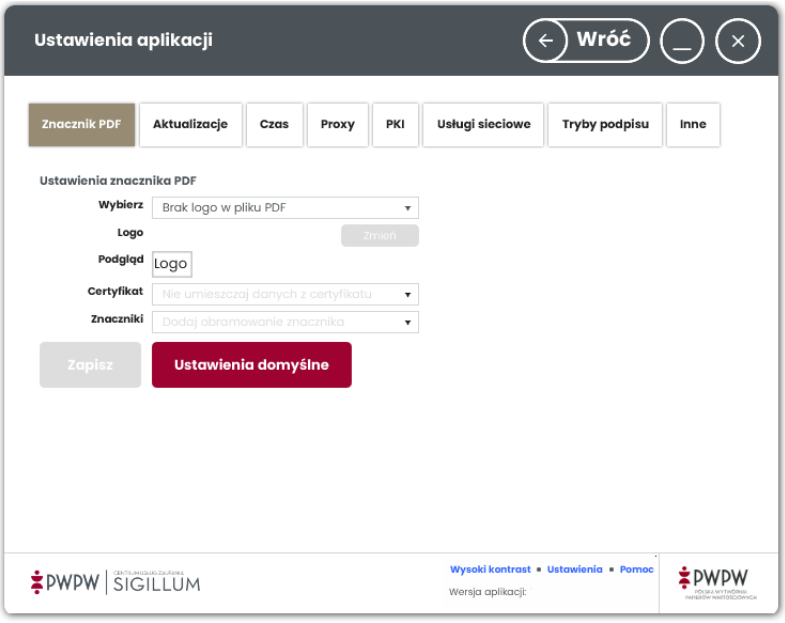
Wersja kontrastowa przeznaczona jest dla osób niedowidzących. Po kliknięciu w link *Wysoki kontrast* na dolnym pasku aplikacji, zmieniony zostaje kontrast ekranu aplikacji. Po kliknięciu w link *Normalny kontrast* na dolnym pasku aplikacji kontrast ekranu zostaje przywrócony.



Domyślnie przy uruchomieniu aplikacji ustawiany jest kontrast, który można też skonfigurować w Ustawieniach (6.4.8).

6.4 Ustawienia

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

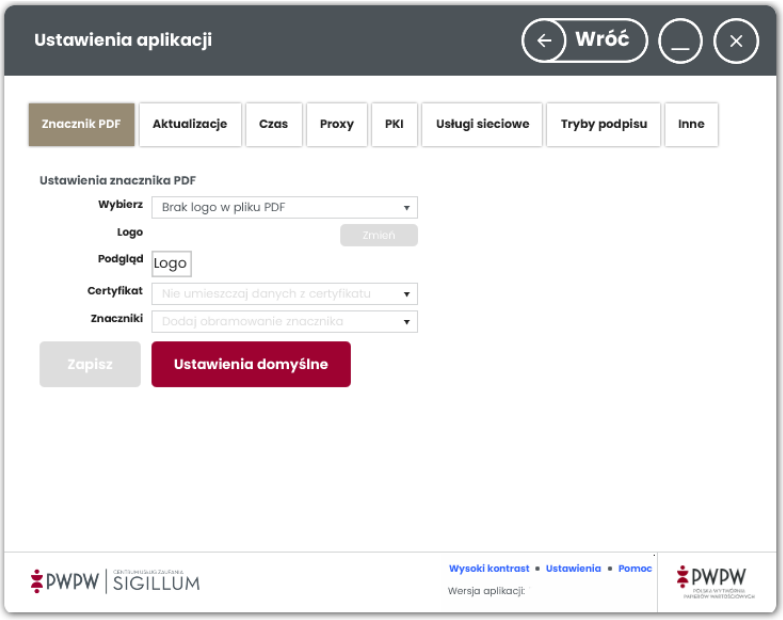


W tym widoku użytkownik może dokonywać zmian oraz zarządzać ustawieniami aplikacji prezentowanymi w poszczególnych zakładkach.

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

Znacznik PDF	Możliwość umieszczenia oraz pozycjonowania znacznika 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, LDAP, NTP, OCSP
Tryby podpisu	Umożliwiają ustawienie domyślnych: Typu zobowiązania, Wariantu i Funkcji skrótu dla kolejnego podpisu oraz kontrasygnaty.
Inne	Umożliwia ustawienie języka oraz folderu, z którego wybierane są pliki.

6.4.1 Znacznik PDF



Menu tej zakładki umożliwia zarządzanie ustawieniami znacznika PDF:

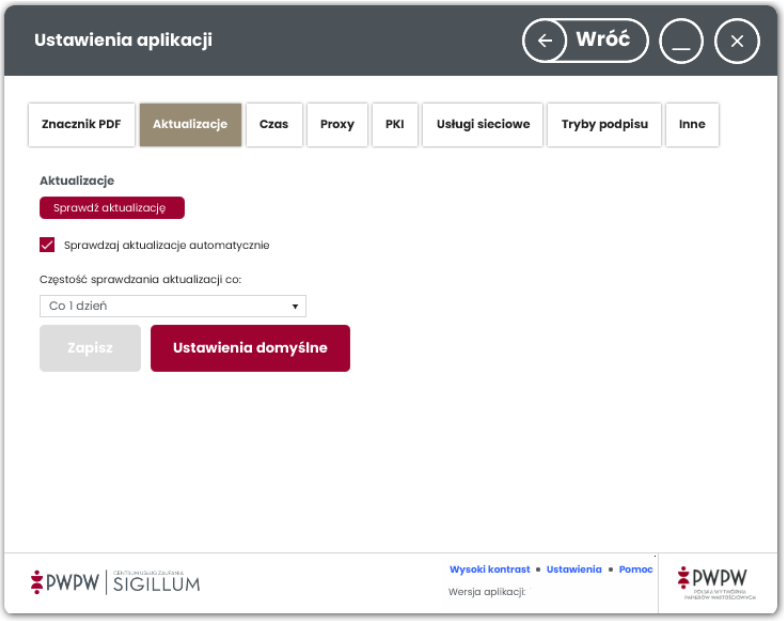
- Lista wyboru „**Wybierz**" – opcja umożliwia umieszczenie zdefiniowanego logo w pliku PDF,
- **Logo** – przycisk **Zmień** umożliwia wybór/zmianę pliku graficznego,
- **Podgląd** – tu wyświetlana jest miniatura wybranego pliku graficznego,
- Lista wyboru **Certyfikat** – opcja umożliwia umieszczenie danych z certyfikatu w pliku

- Lista wyboru **Znaczniki** – opcja umożliwia umieszczenie obramowania wstawianego znacznika

System umożliwia umieszczenie znacznika na każdej stronie dokumentu, zgodnie z wolą Użytkownika.

Szczegółowy opis składania podpisu na dokumentach PDF z użyciem znacznika opisany został w punkcie 7.1.6 niniejszej instrukcji.

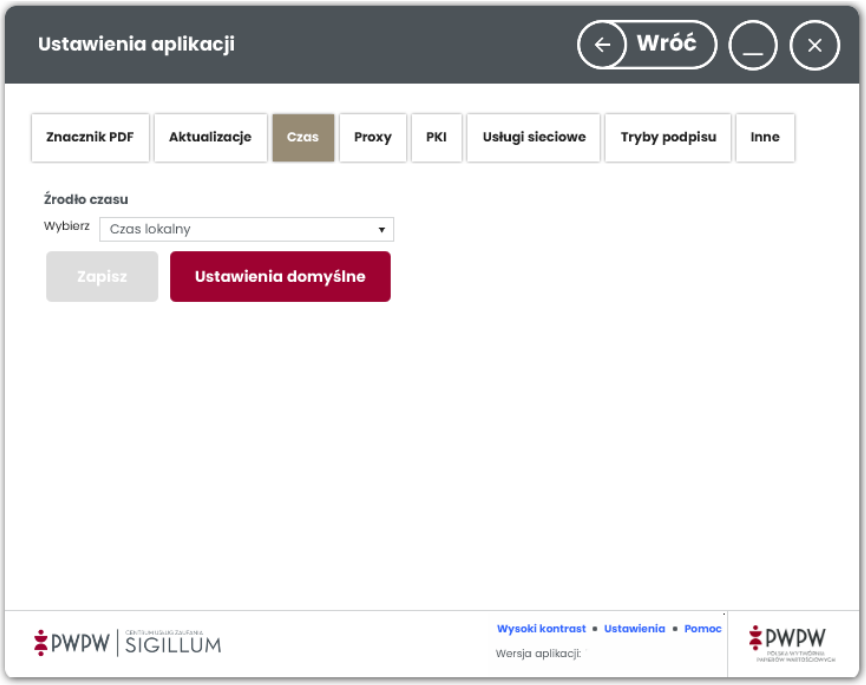
6.4.2 Aktualizacje



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).

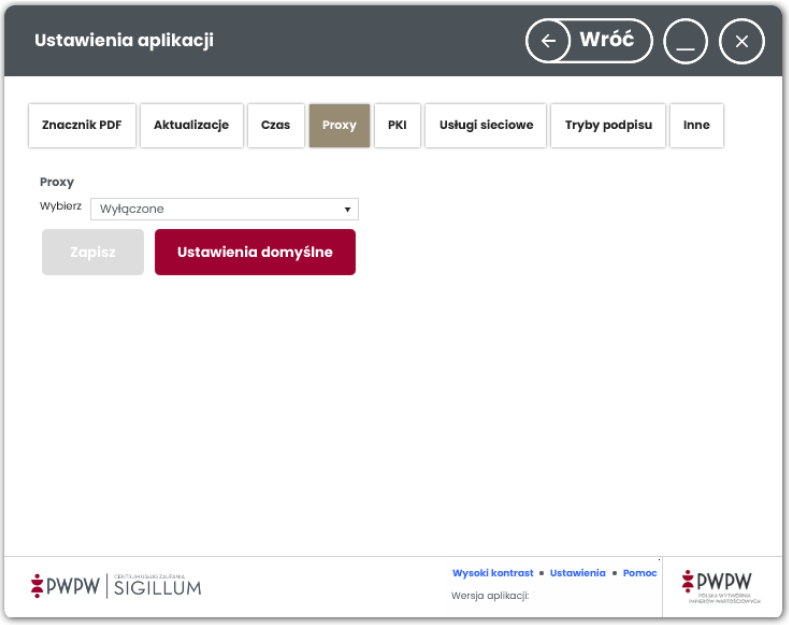
W przypadku wybrania opcji *1 dzień* (codziennie), aplikacja będzie sprawdzać i informować o nowej dostępnej wersji przy pierwszym uruchomieniu danego dnia.

6.4.3 Czas



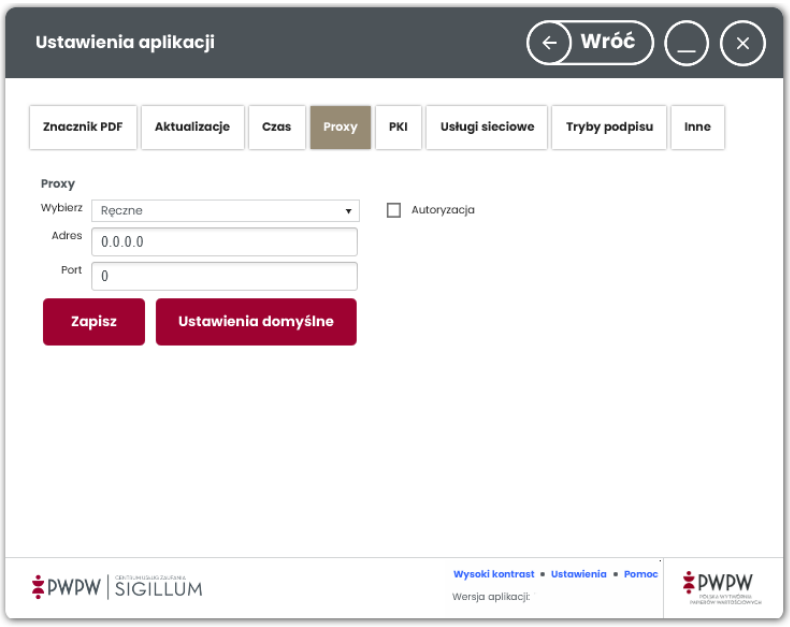
W zakładce ustawień źródła czasu aplikacji można wybrać między czasem lokalnym (komputer), a źródłem czasu NTP (dedykowany serwer czasu). Wskazanie dedykowanego serwera czasu jest możliwie z poziomu zakładki ***Usługi sieciowe / Serwery NTP***.

6.4.4 Proxy



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

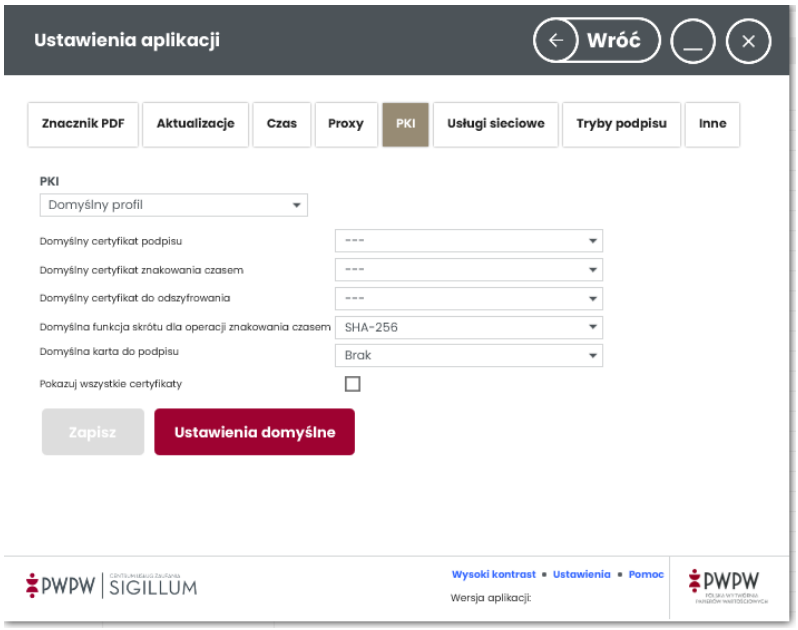
Po wyborze w polu ***Proxy*** wartości ***Ręczne***, wyświetlone zostaną szczegóły konfiguracji.



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

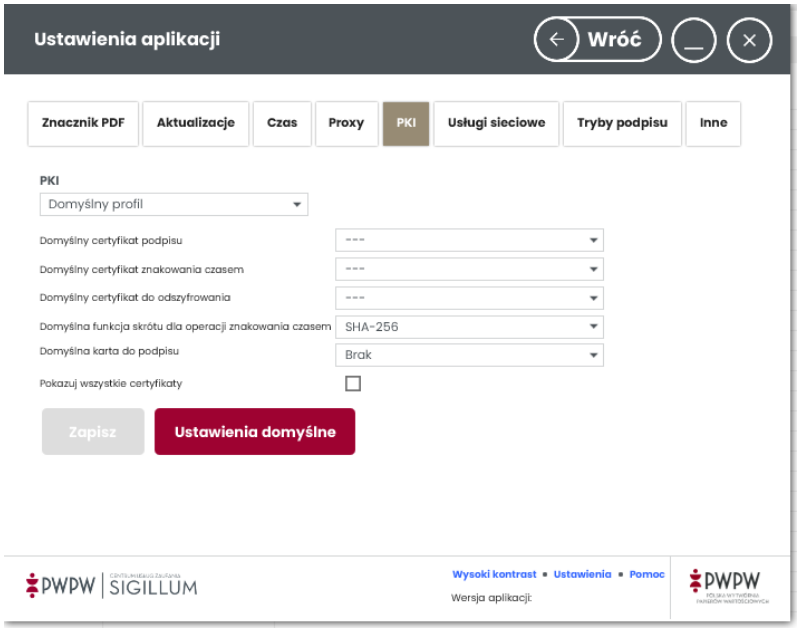
Jeśli dodatkowo serwer proxy wymaga autoryzacji, wówczas należy zaznaczyć checkbox ***Autoryzacja*** oraz wypełnić pola: ***Użytkownik, Hasło, Domena*** oraz wybrać typ autentykacji (BASIC lub NTLM). Jeśli zaznaczone zostanie pole ***Autoryzacja podczas startu***, przy uruchamianiu aplikacji trzeba będzie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

6.4.5 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***.

6.4.5.1 Domyślny profil



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

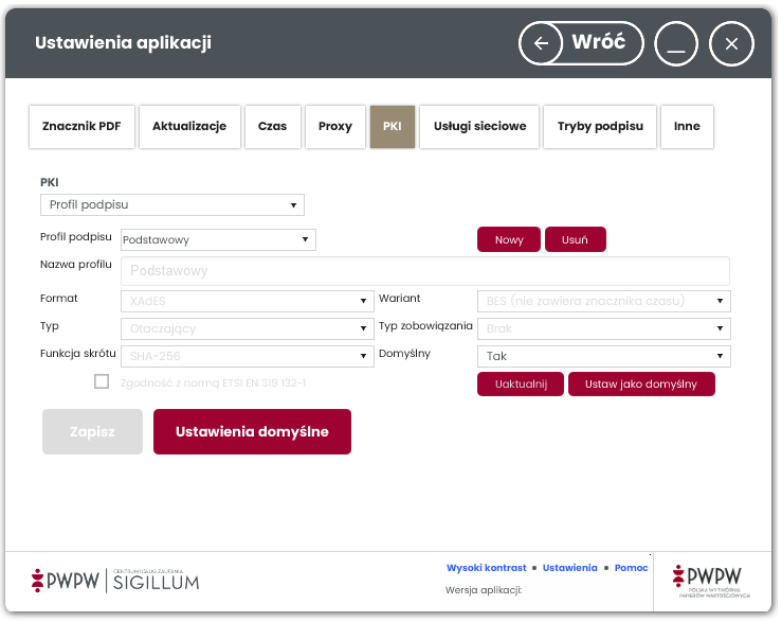
- podpisu,
- znakowania czasem,
- odszyfrowania,

, 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.

6.4.5.2 *Profil podpisu*



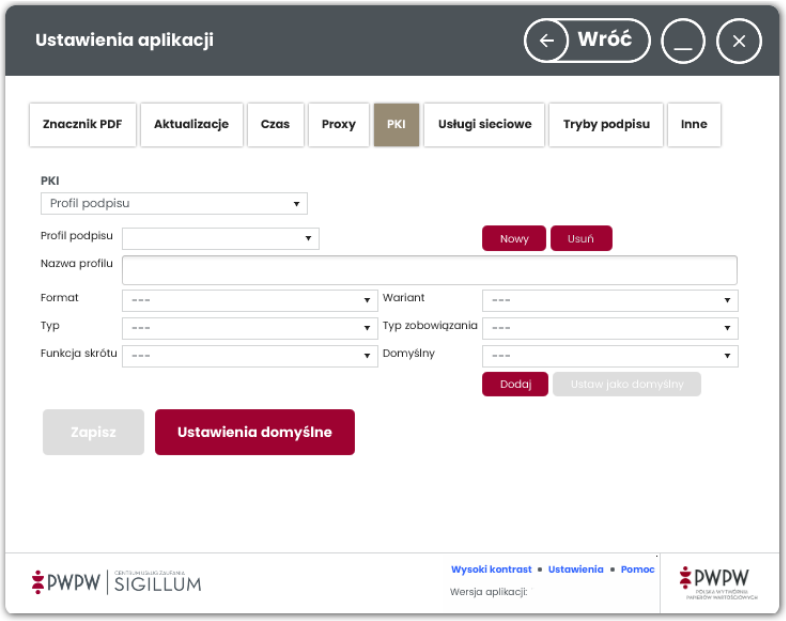
Zakładka ***Profil podpisu*** służy do przygotowania dedykowanych profili użytkownika.

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, ASiC-E, ASiC-S,
   - *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.
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.
   - ASiC-S – tworzy strukturę kontenera pliku podpisywanego oraz podpisu
   - ASiC-E – 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 ASiC-E, ASiC-S: BES, T.

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

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 ASiC-E, ASiC-S: 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-1 – najstarsza spośród dostępnych funkcji skrótu. Rozmiar skrótu to 160 maks. bitów. Mimo, iż funkcja skrótu jest nadal dostępna, zaleca się używanie jej nowszych wariantów, tj. SHA-256 lub SHA-512.

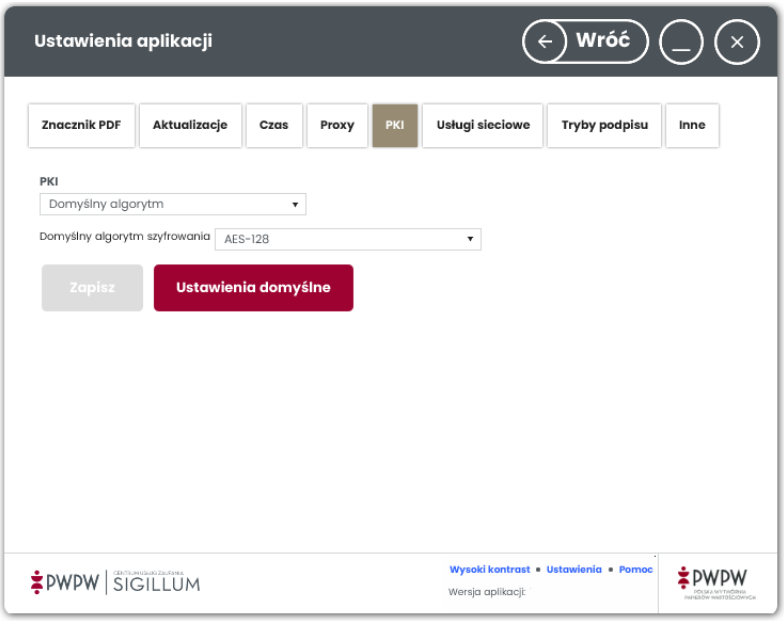
     Ważne: z dniem 1 lipca br. zakończył się przewidziany w artykule 137 ustawy z dn. 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016, Poz. 1579) okres stosowania funkcji skrótu SHA1 w zastosowaniach dotyczących zaawansowanego podpisu elektronicznego i pieczęci.
   - 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.

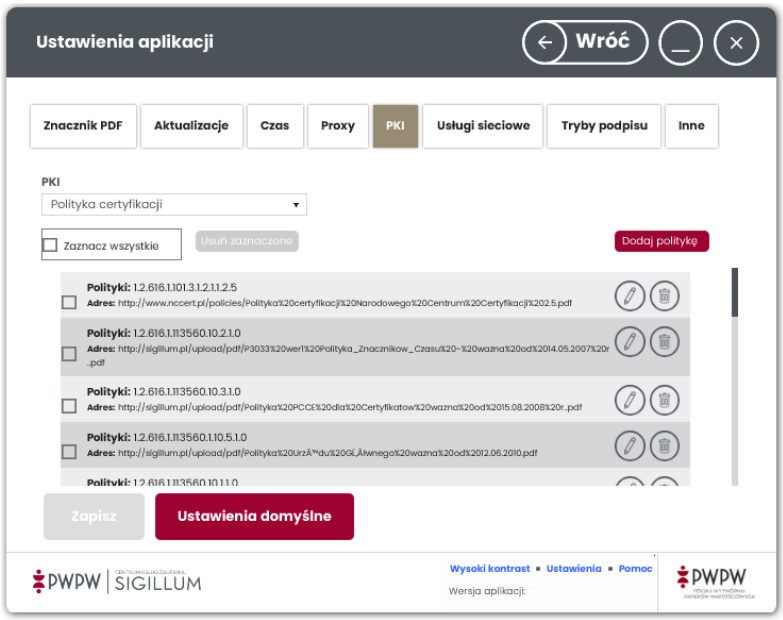
6.4.5.3 *Domyślny algorytm (szyfrowania)*



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.

6.4.5.4 *Polityka certyfikacji*

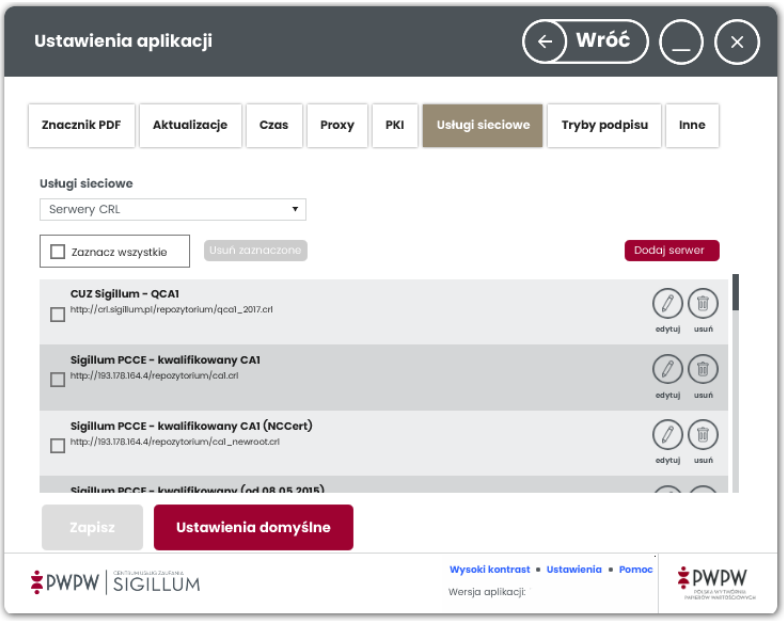


W zakładce ***Polityka certyfikacji*** wyświetlane są nazwy Polityki certyfikacji oraz ich adresy.

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.

6.4.6 Usługi sieciowe



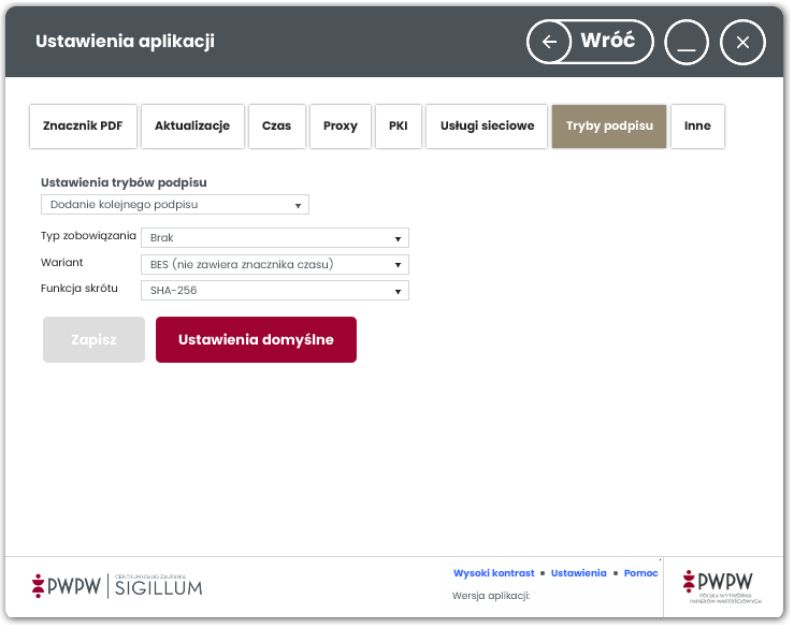
Menu tej zakładki umożliwia zarządzanie serwerami:

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.
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.

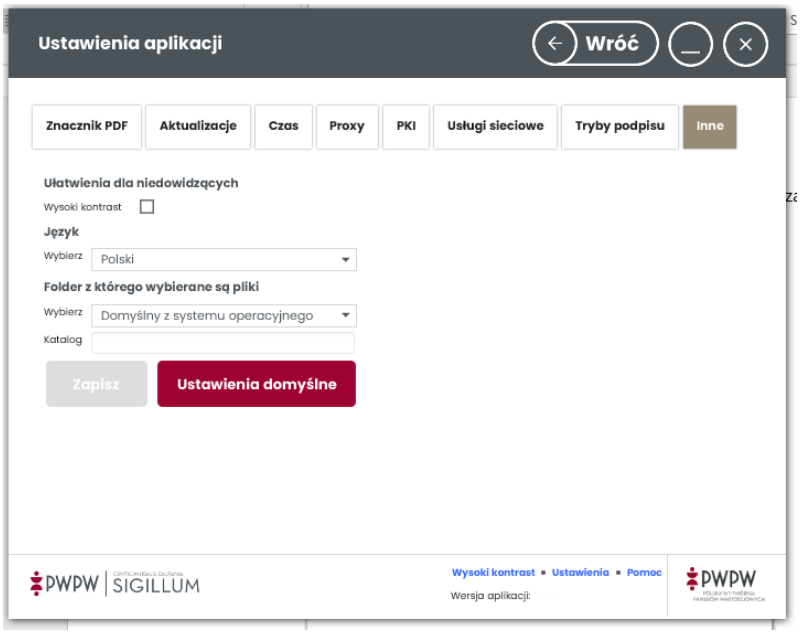
Brak dostępu jest komunikowany przy składaniu oraz weryfikacji podpisu.

6.4.7 Tryby podpisu



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

6.4.8 Inne



Zaznaczenie opcji ***Wysoki kontrast*** i zapis konfiguracji spowoduje, że domyślnie aplikacja będzie uruchamiana z wysokim kontrastem.

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

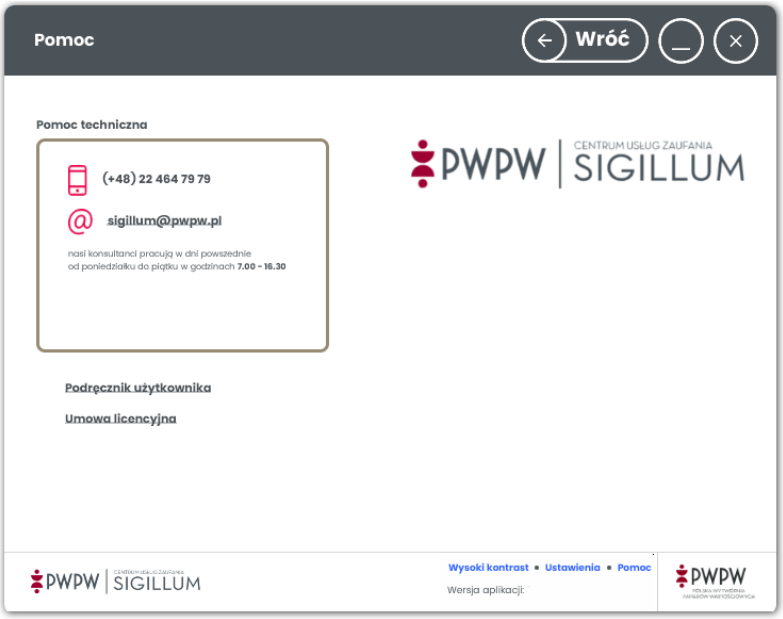
Przełączenie języka nastąpi dopiero po wybraniu opcji i ponownym uruchomieniu Aplikacji.

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.

6.5 Pomoc

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



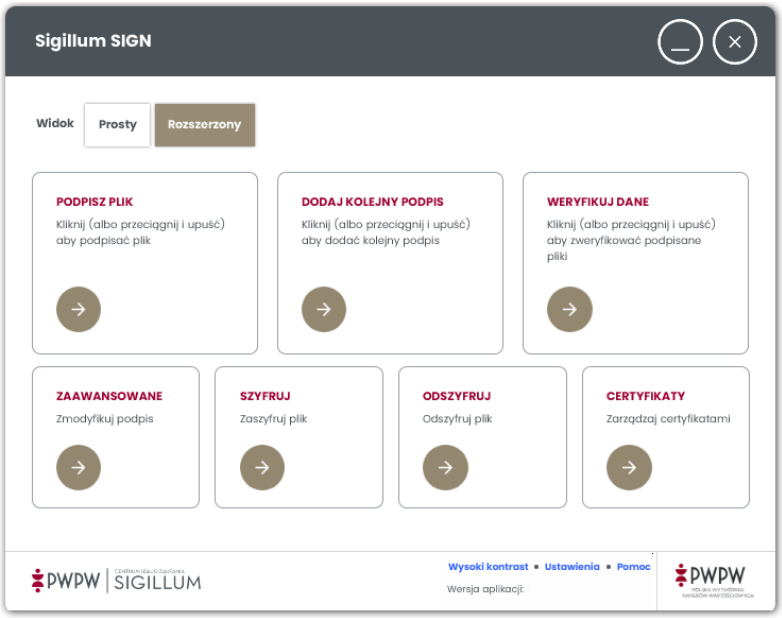
Pomoc techniczna – informacje dotyczące możliwych form kontaktu.

Instrukcja – dostęp do informacji, dostępnych w tym materiale.

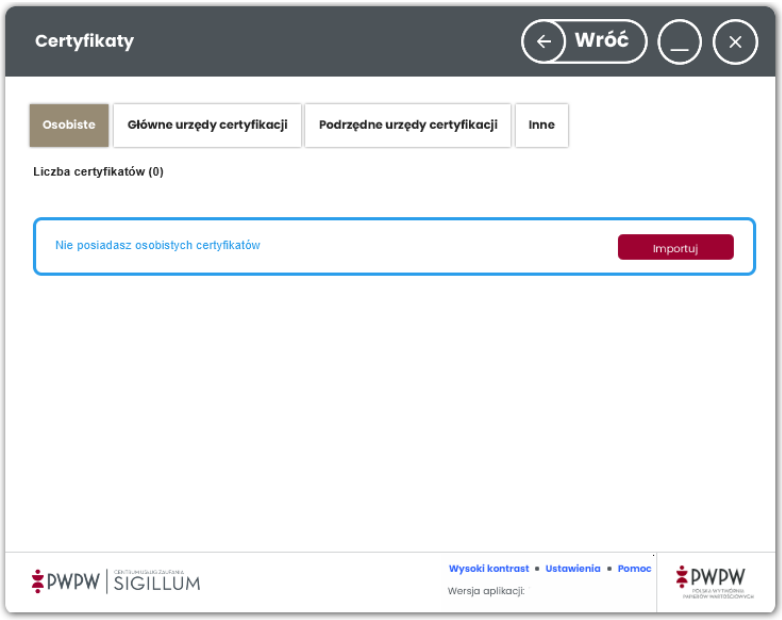
Umowa licencyjna – możliwość zaprezentowania użytkownikowi treści umowy licencyjnej.

6.6 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 i 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:

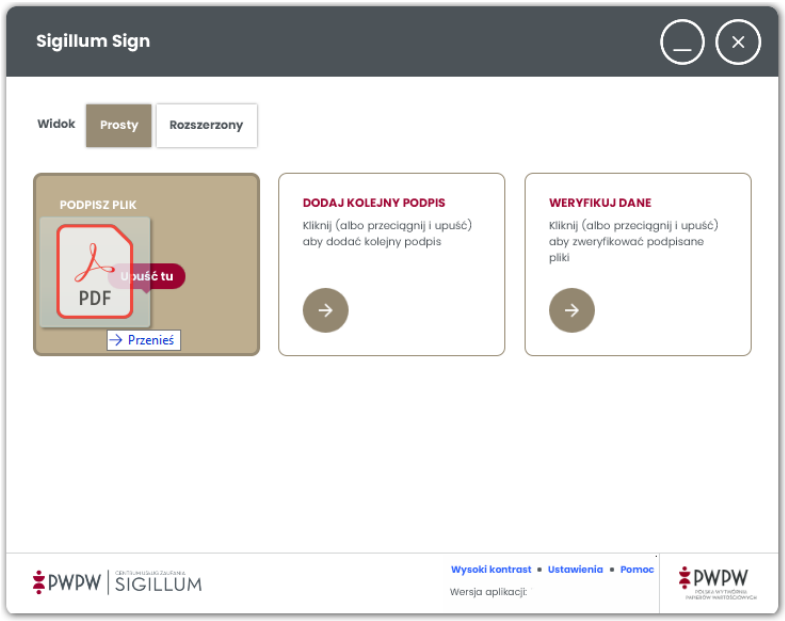
1. przycisk **Importuj** – umożliwia dodanie do magazynu certyfikatów aplikacji plik z certyfikatem (postaci pliku crt lub pkcs12),
2. ikona kosza **(Usuń)** – umożliwia usunięcie wybranego certyfikatu z magazynu certyfikatów aplikacji,
3. ikona strzałki **(Podgląd certyfikatu)** – umożliwia podgląd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

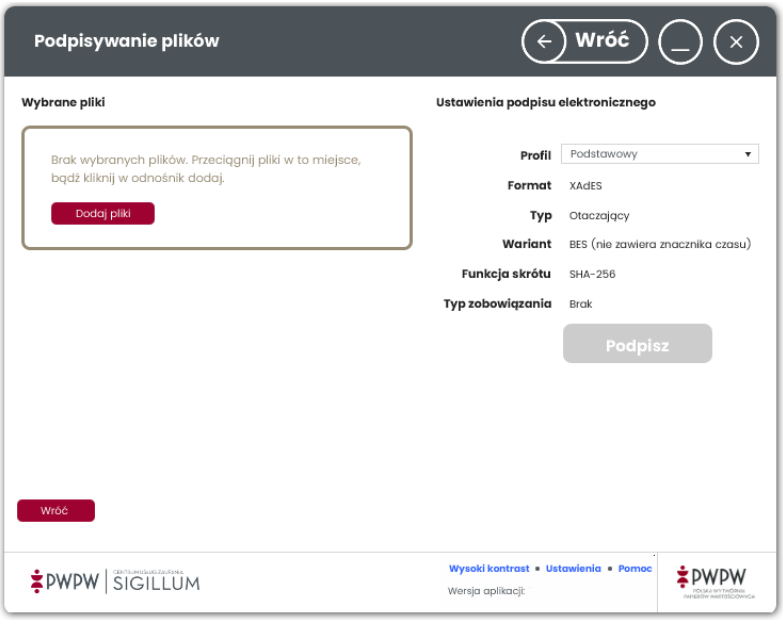


UWAGA!

Pliki o rozmiarze powyżej 50 MB mogą być podpisane tylko podpisem zewnętrznym.

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.

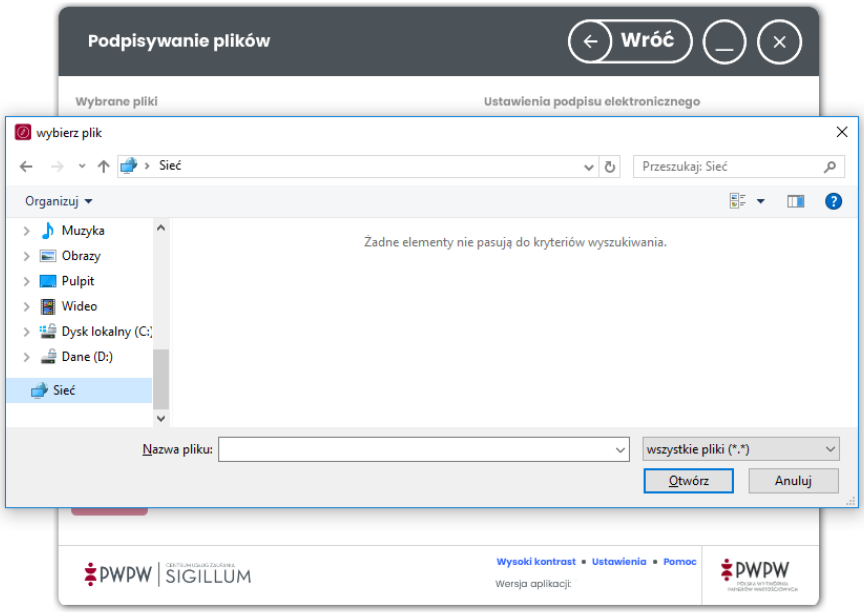
UWAGA!

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.

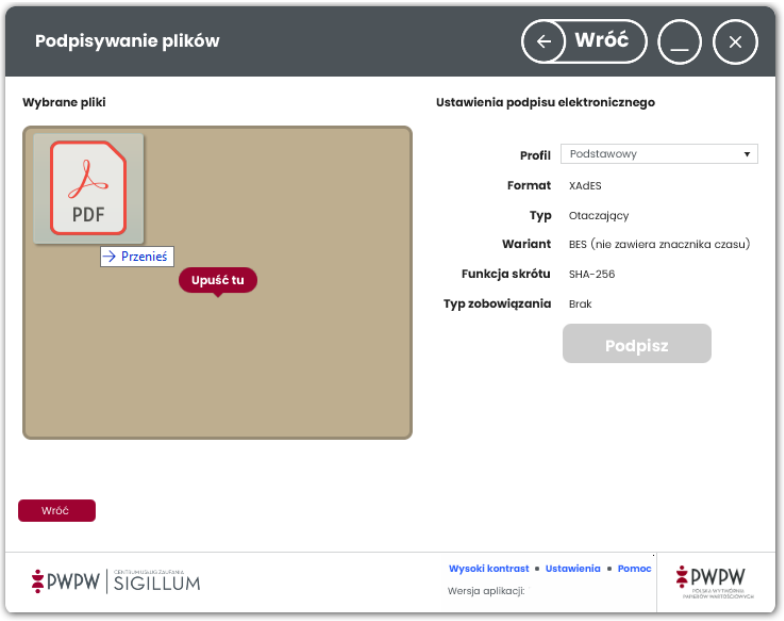
7.1.3 Dodanie pliku do obszaru roboczego

Aby podpisać plik lub 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*.

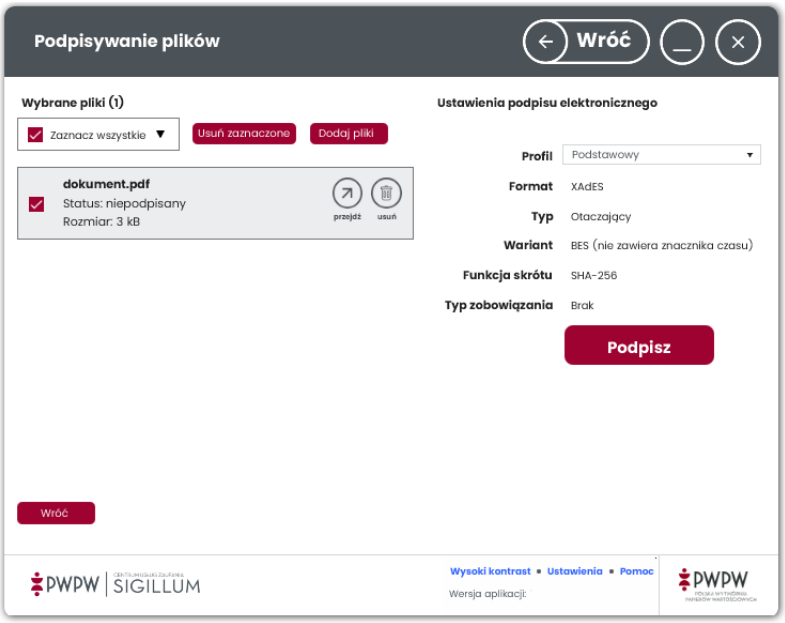
Po kliknięciu opcji ***Dodaj pliki*** pojawi się okno przeglądania zawartości stacji roboczej użytkownika.



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:

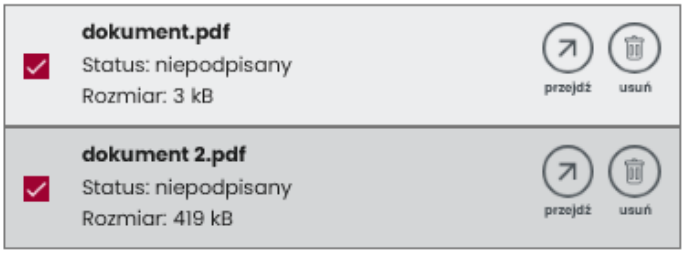
Nazwa dokumentu, Status oraz rozmiar.

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)**.

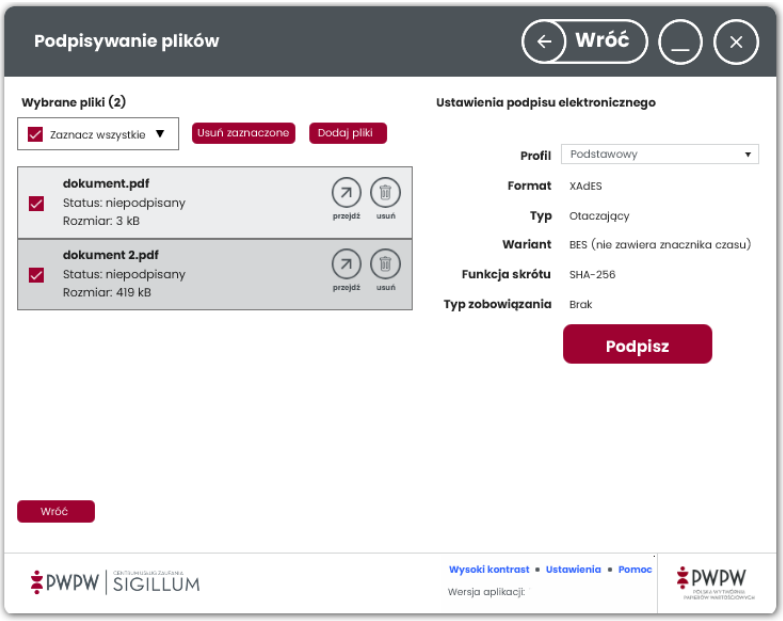
Po prawej stronie ekranu, w obszarze ustawień podpisu użytkownik może wybrać profil podpisu.

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 6.4.5.2 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"**.

7.1.4 Ekran wyboru certyfikatów i złożenie podpisu

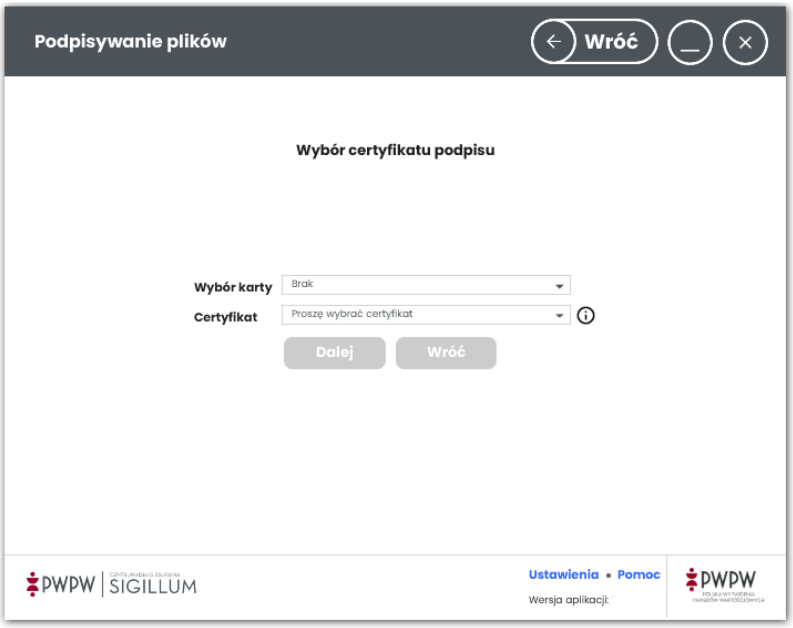
Po wyborze opcji ***„Podpisz"*** użytkownik przeniesiony zostaje do ekranu wyboru karty i certyfikatów, wprowadzenia kodu PIN oraz informacji o złożeniu podpisu.

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 (6.4.5.1).

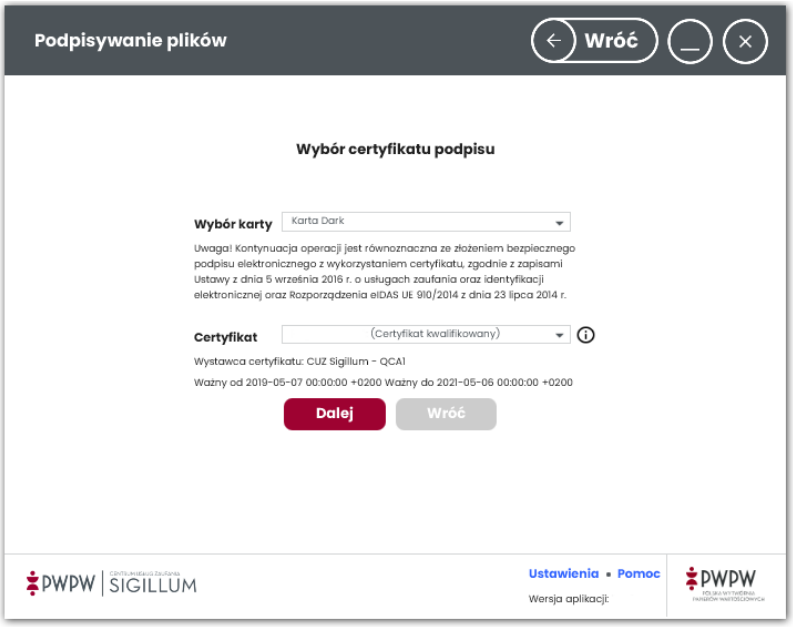
Wybór karty to wskazanie biblioteki pkcs11 umieszczonej w określonej lokalizacji. Jeśli biblioteki nie ma w określonej lokalizacji, wyświetlone zostaje okno wyboru pliku. Po wskazaniu poprawnego pliku pkcs11 do listy wyboru karty zostaje dodana nowa pozycja.

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.

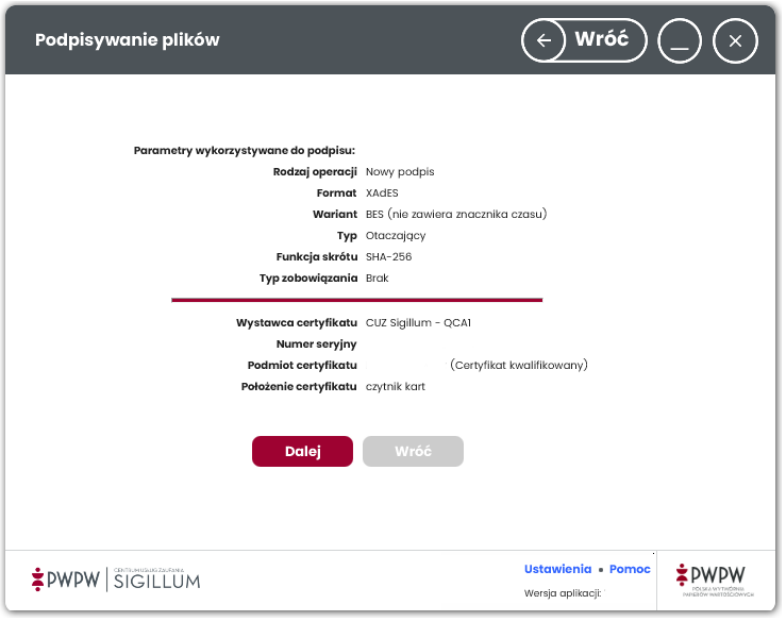
Po wyborze karty i certyfikatu, pojawia się informacja na temat certyfikatu i skutku prawnego wywołanego jego użyciem.



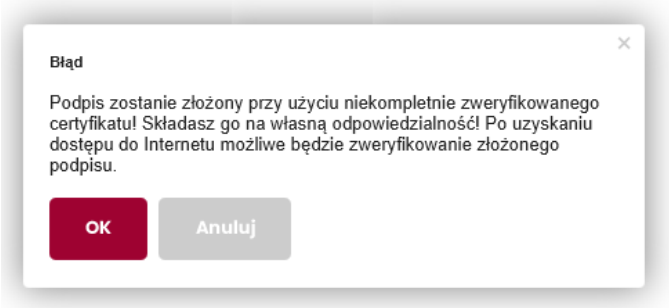
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny.

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

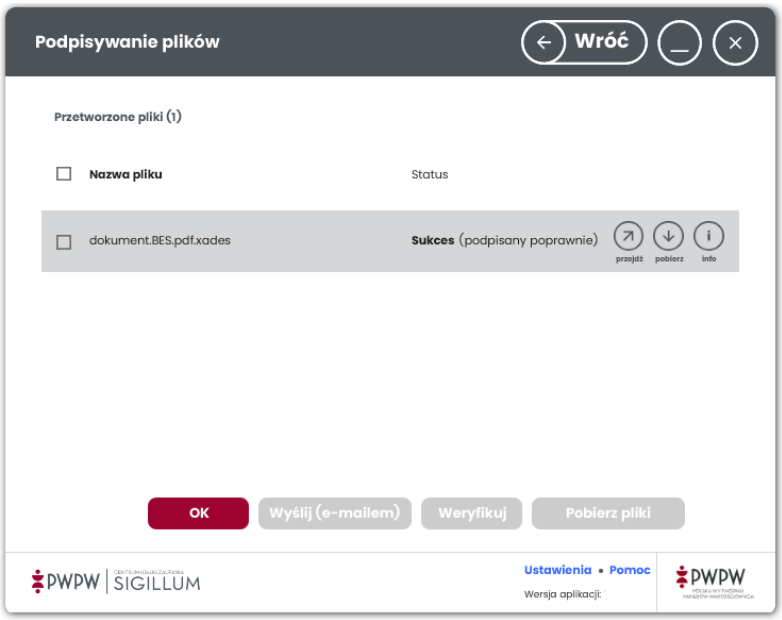
Po wpisaniu poprawnego kodu PIN i kliknięciu **Potwierdź**, system prezentuje ekran parametrów wykorzystanych do wykonania podpisu.



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 – zapisywanie podpisanego pliku,
- pobierz – zapisywanie pliku bez podpisu,
- info – szczegóły złożonego podpisu.

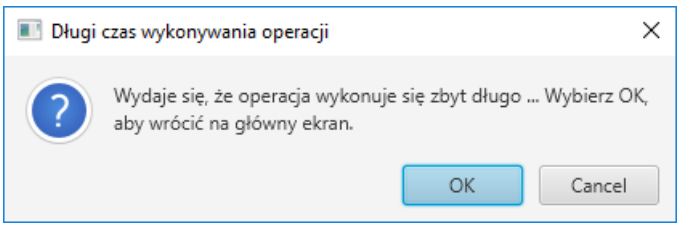
Po zaznaczeniu checkboxa w wierszu wybranych plików można wysłać podpisane dokumenty poprzez e-mail klikając przycisk ***Wyślij (e-mailem)***.

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 katalogach, gdzie znajdują się pliki źródłowe. Podpis można zweryfikować w procesie weryfikacji.

7.1.5 Podpisanie wielu plików

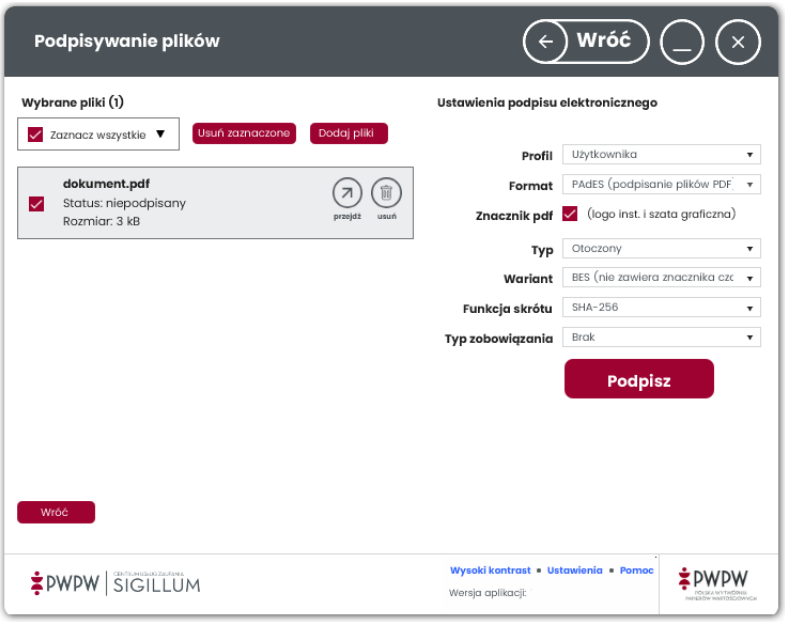
Jeśli jednocześnie podpisywanych jest wiele plików, w trakcie podpisywania może pojawić się okno informujące o długim czasie wykonywania operacji.



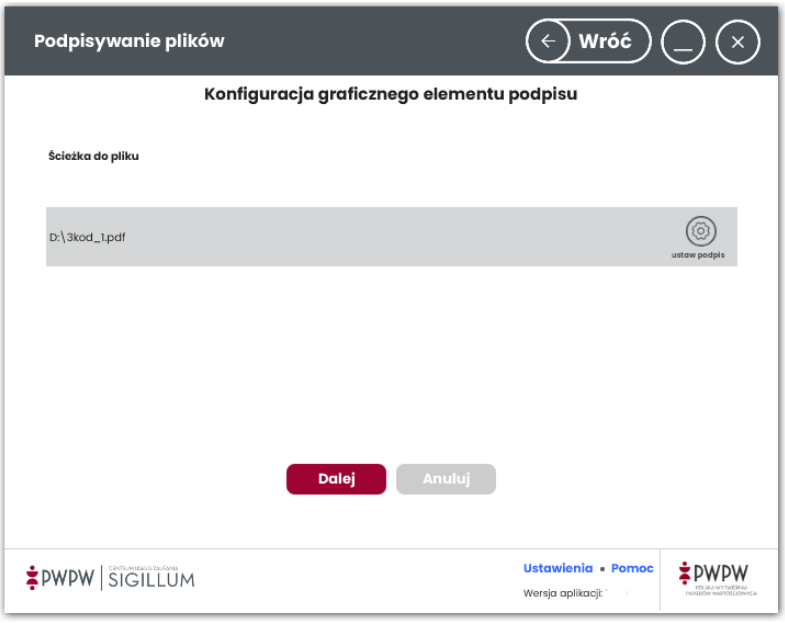
Okno można pozostawić na ekranie lub kliknąć przycisk Cancel – operacja podpisu będzie trwała nadal.

7.1.6 Podpisanie pliku PAdES ze znacznikiem

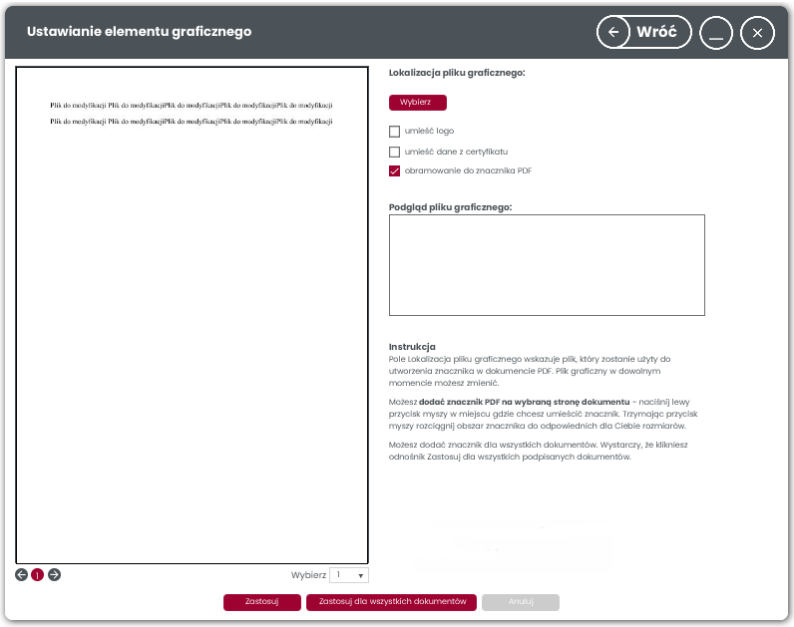
Aby rozpocząć podpisanie dokumentu w formacie PAdES ze znacznikiem PDF, w pierwszej kolejności należy ustawić w aplikacji znacznik PDF (6.4.1). Znacznik można też ustawić w trakcie składania podpisu. Po dodaniu pliku *.pdf, z menu bocznego wybieramy **Profil: Użytkownika, Format: PAdES** oraz zaznaczamy checkbox **Znacznik pdf.**



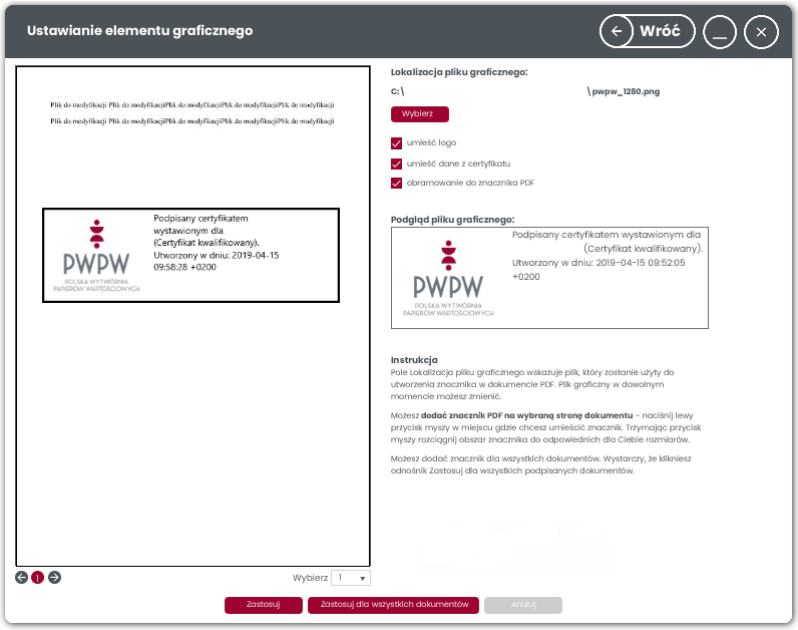
Po naciśnięciu przycisku **„Podpisz”**, aplikacja przechodzi do następnego okna konfiguracji. Wybieramy odpowiedni certyfikat oraz potwierdzamy jego wybór a następnie podajemy pin. Dodanie do dokumentu znacznika PDF (np. logo Firmy) a następnie możliwość jego edycji (umieszczenie we wskazanym miejscu oraz określenie wielkości) dostępne są po kliknięciu ikony ***ustaw podpis***.



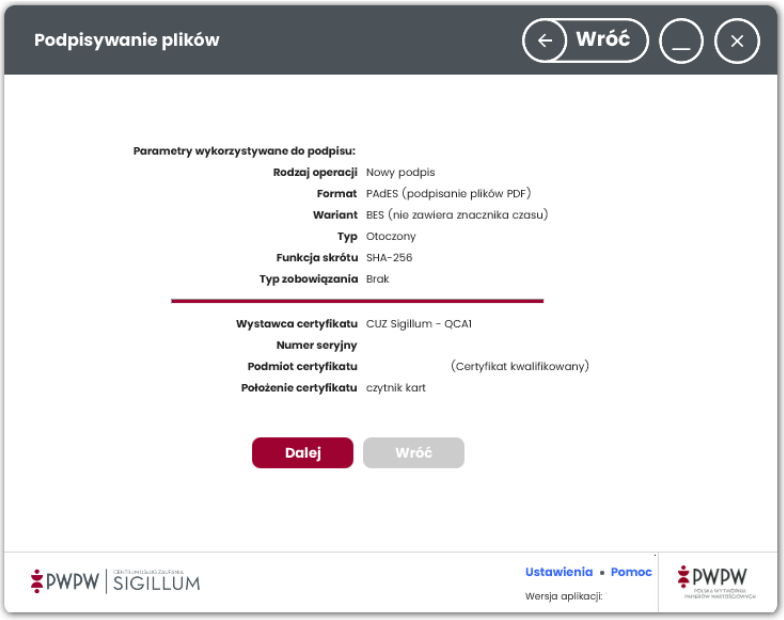
Po kliknięciu w wyżej wymienioną ikonę, aplikacja otwiera okno: **„Ustawianie elementu graficznego”.**



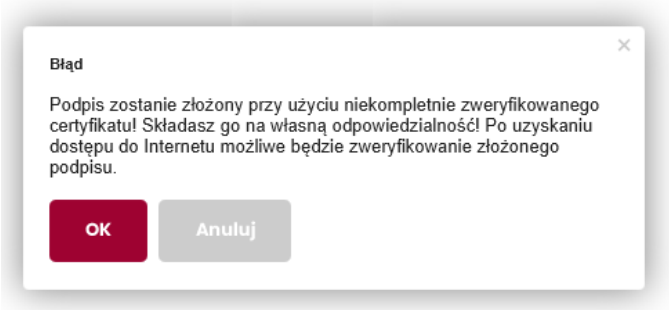
W tym oknie aplikacja umożliwia nanoszenie znaczników PDF, poprzez naciśnięcie lewego przycisku myszy i rozciągnięcie obszaru znacznika do oczekiwanych rozmiarów.
Z tego poziomu, możliwy jest również wybór innego znacznika PDF oraz opcja umieszczenia danych z certyfikatu.



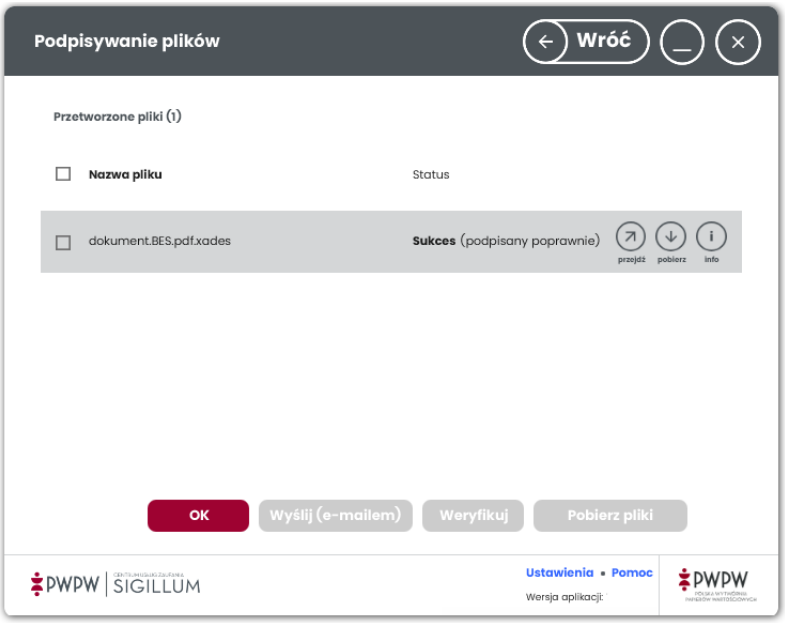
Po zastosowaniu znacznika do wybranego dokumentu i kliknięciu Dalej, system prezentuje ekran parametrów wykorzystanych do wykonania podpisu.



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.



7.2 Dodaj kolejny podpis

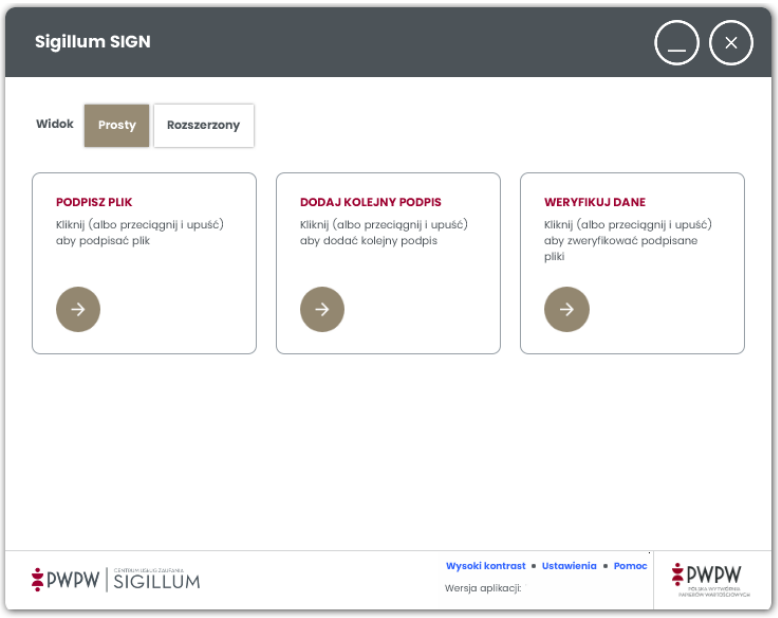
7.2.1 Ekran początkowy procesu weryfikacji

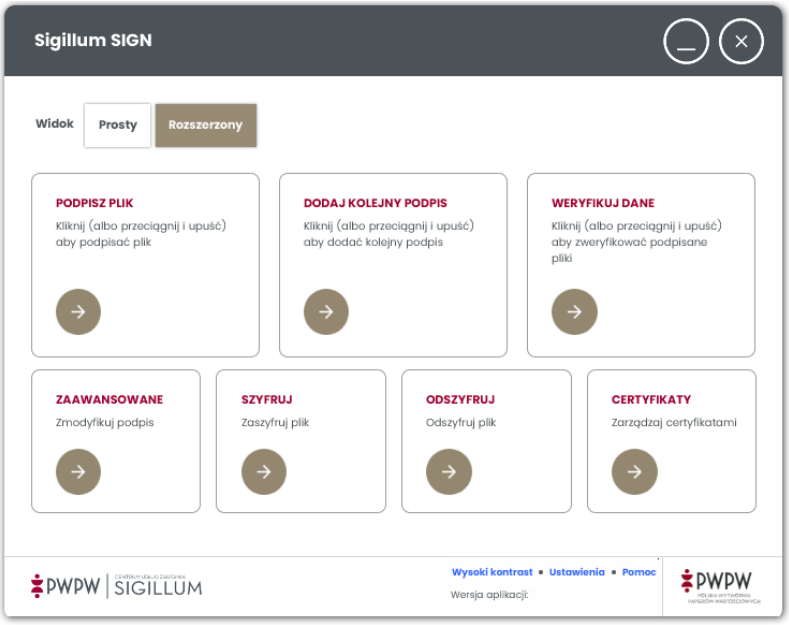
Wybranie opcji Dodaj kolejny podpis oznacza, że do podpisanego certyfikatem dokumentu dodany zostanie kolejny podpis wskazany przez użytkownika (podpis równoległy).

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.

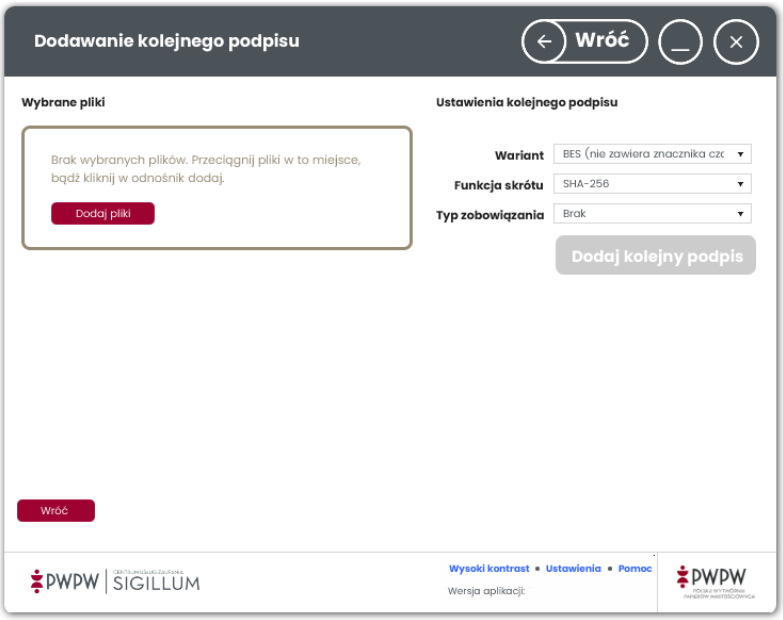




Po kliknięciu kafelka ***„Dodaj kolejny podpis”*** Użytkownik określa szczegóły składanego podpisu takie jak wariant (bez lub ze znacznikiem czasu), funkcję skrótu oraz typ zobowiązania.

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.

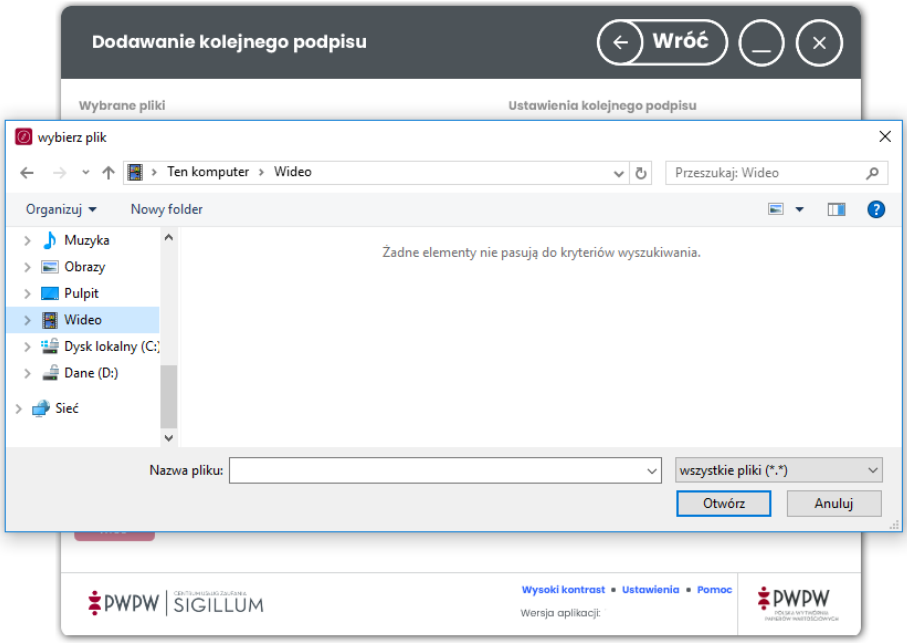


Ekran podzielony jest na dwie części: większą, centralną tzw. obszar roboczy, w którym prezentowane są pliki oraz mniejszą, z prawej strony tzw. obszar ustawień, zawierający ustawienia związane z podpisem oraz przycisk ***„Dodaj kolejny podpis”***.

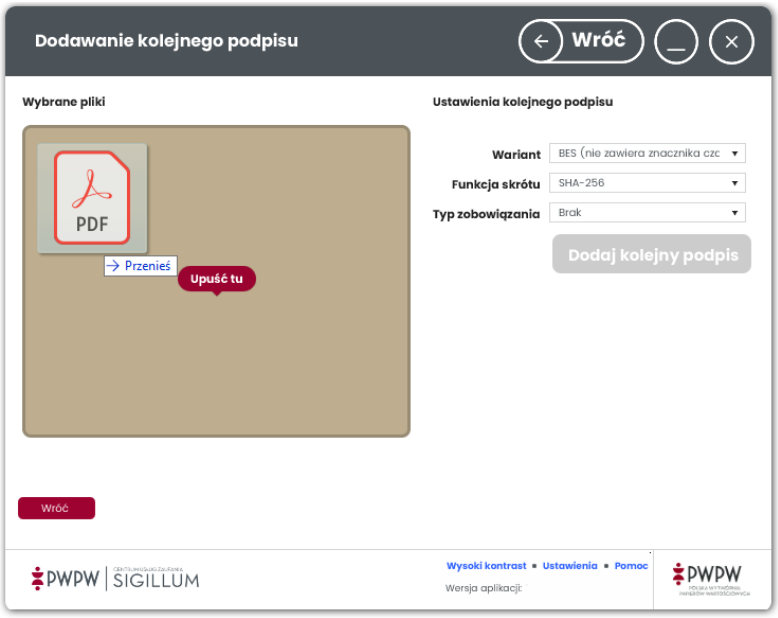
7.2.3 Dodanie pliku do obszaru roboczego

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

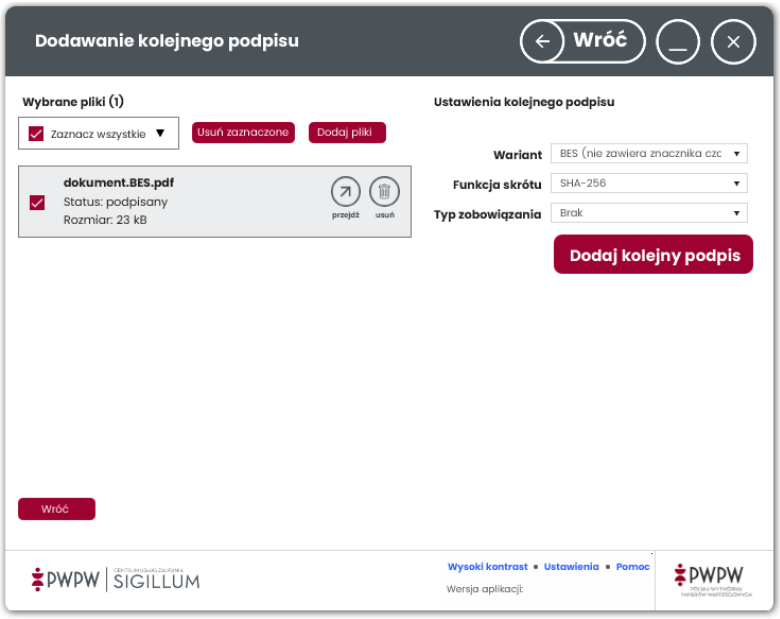
Po kliknięciu opcji ***Dodaj pliki*** pojawi się okno przeglądania zawartości stacji roboczej użytkownika.



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:

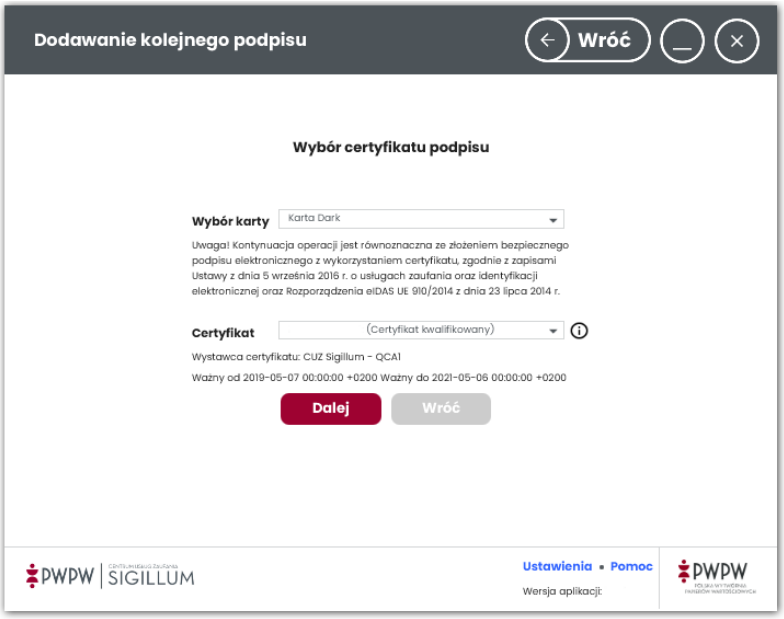
Nazwa dokumentu, Status oraz rozmiar.

Kliknięcie w ikonę ***przejdź*** na kafelku umożliwia otwarcie pliku. Kliknięcie w ikonę ***usuń*** na kafelku umożliwia usunięcie pliku z obszaru roboczego.

7.2.4 Ekran wyboru certyfikatów i złożenie podpisu

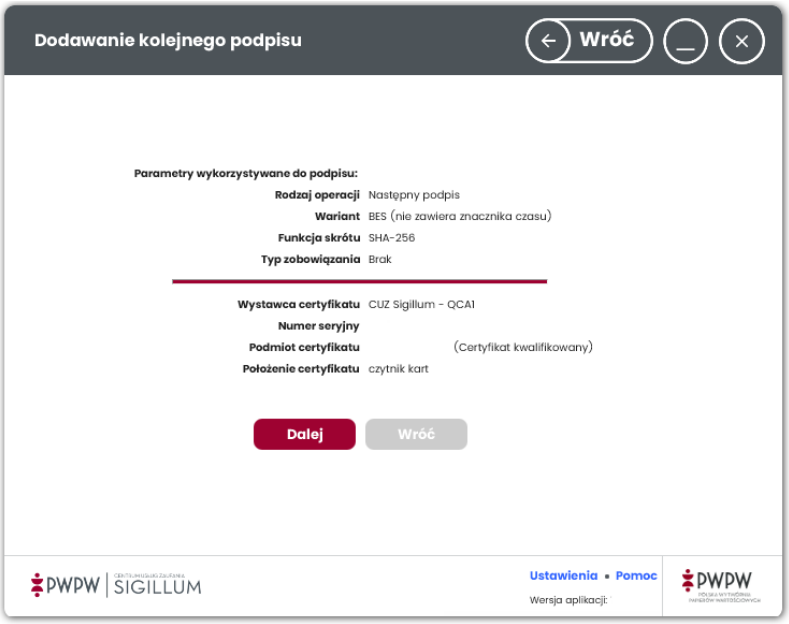
Po wyborze opcji ***„Dodaj kolejny podpis”*** użytkownik przeniesiony zostaje do ekranu wyboru karty i certyfikatów.

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.

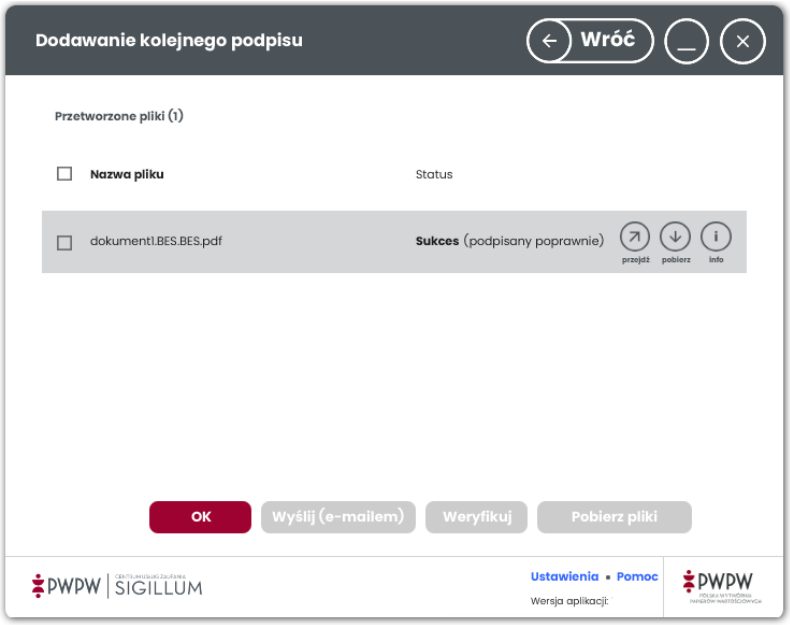


Po wyborze karty i certyfikatu, pojawia się informacja na temat certyfikatu i skutku prawnego wywołanego jego użyciem.
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny.
Po kliknięciu ***„Dalej”*** system otwiera okno wprowadzenia kodu PIN.

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 – zapisywanie podpisanego pliku,
- pobierz – zapisywanie pliku bez 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.

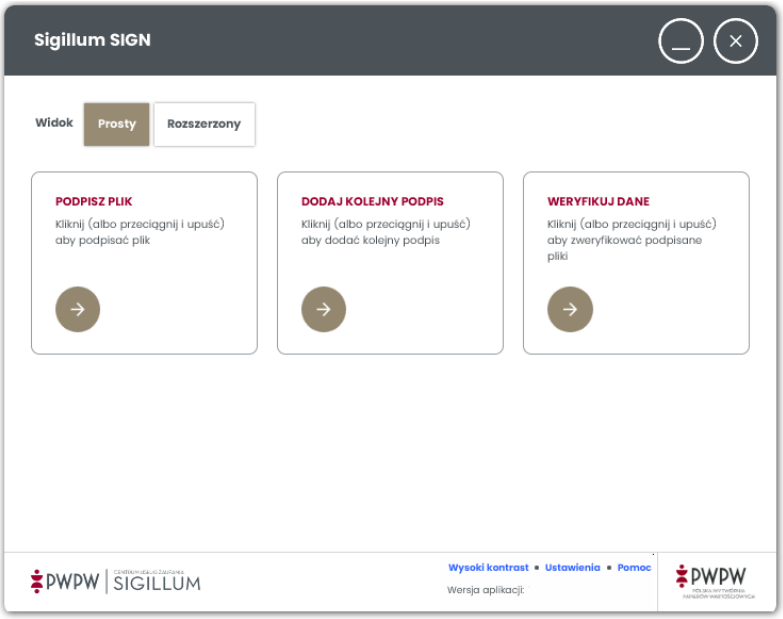
Potwierdzenie (OK) kończy proces podpisywania. Podpisane pliki odnaleźć można w katalogach, gdzie znajdują się pliki źródłowe. Podpis można zweryfikować w procesie weryfikacji.

7.3 Weryfikacja podpisu

7.3.1 Ekran początkowy procesu weryfikacji

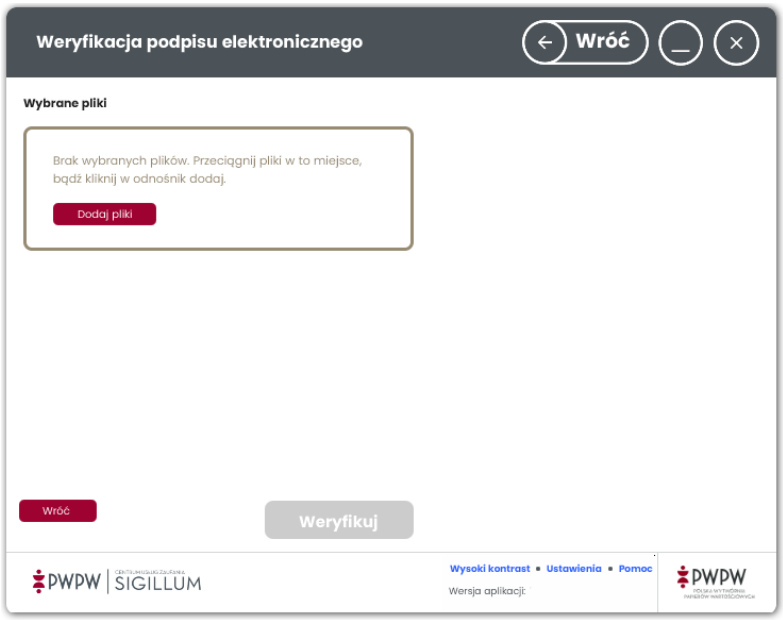
Kliknięcie, lub przeciągnięcie plików na obszar ***„Weryfikuj dane"*** na stronie głównej rozpoczynają proces weryfikacji. Opcja dostępna jest w widoku prostym oraz rozszerzonym.

UWAGA!
Aplikacja posiada limit wielkości dodawanego do weryfikacji pliku. Maksymalny rozmiar pliku dodawanego do weryfikacji nie może przekroczyć 70 MB.



7.3.2 Ekran weryfikacji i ustawień

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

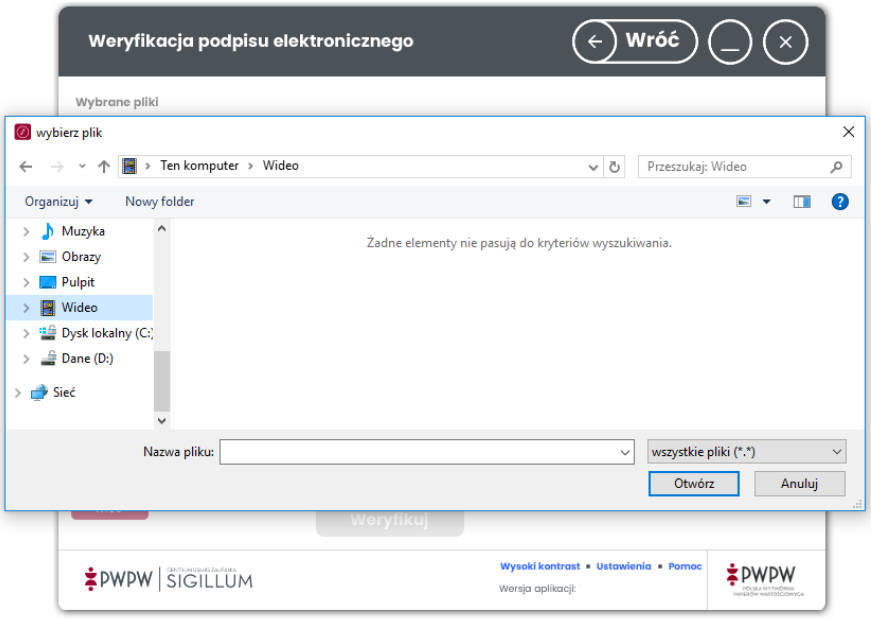


Ekran podzielony jest na dwie części: większą, centralną tzw. obszar roboczy, w którym prezentowane są pliki oraz mniejszą, z prawej strony wyświetlający wynik weryfikacji.

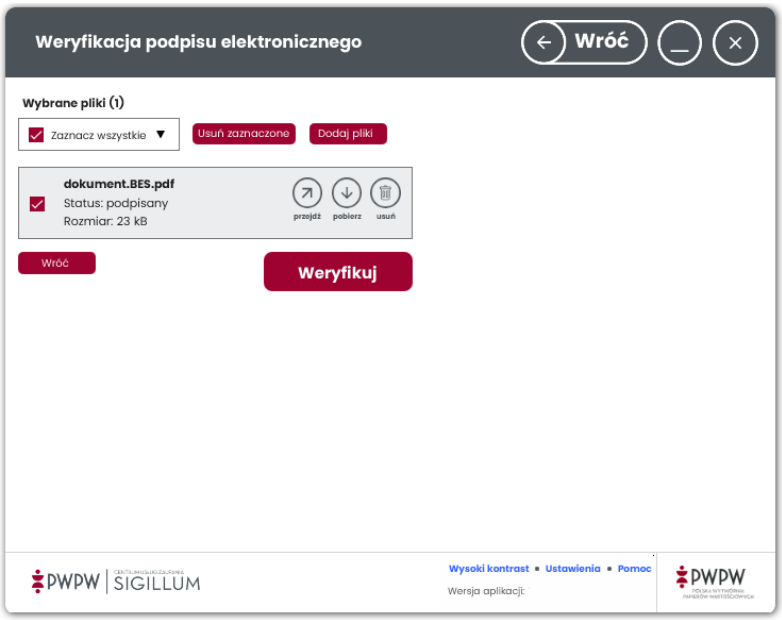
7.3.3 Dodanie pliku do obszaru roboczego

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

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.

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

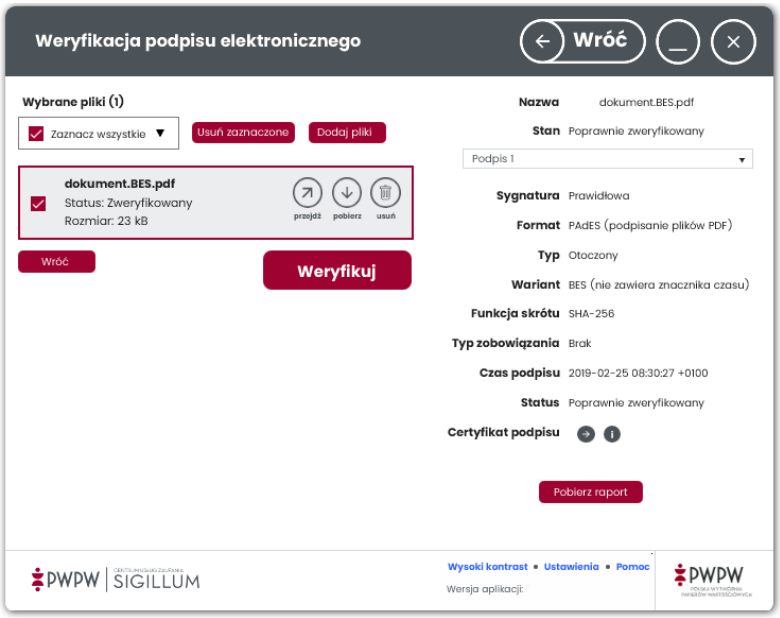
Kliknięcie w ikonę ***pobierz*** umożliwia zapis pliku.

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

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)*

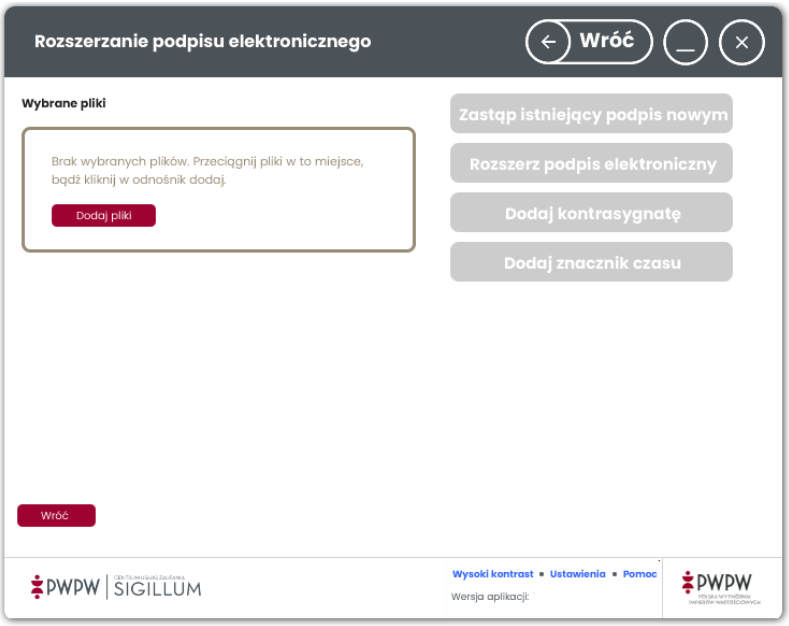
Użytkownik ma możliwość podglądu informacji o podpisie po kliknięciu ikony strzałki skierowanej w prawo lub ikony z literką i w oknie z wynikiem weryfikacji.

Można również pobrać raport z weryfikacji klikając przycisk Pobierz raport.

7.4 Proces operacji zaawansowanych

7.4.1 Ekran startowy procesu zaawansowane

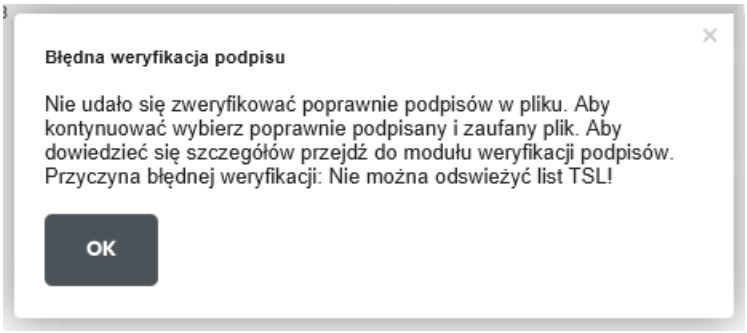
Wywołanie operacji rozszerzania podpisu (do już istniejącego) odbywa się przez kliknięcie przycisku ***„Rozszerzony"*** na stronie głównej a następnie kliknięcie kafelka **„Zaawansowane"**. Wywołanie funkcjonalności może odbyć się również przez akcję *Przeciągnij i upuść* wybrany plik na obszar **„Zaawansowane"**.



W zależności od formatu/typu/wariantu dodanego pliku, odpowiednie przyciski akcji staną się aktywne lub nieaktywne, co przedstawia poniża tabela.

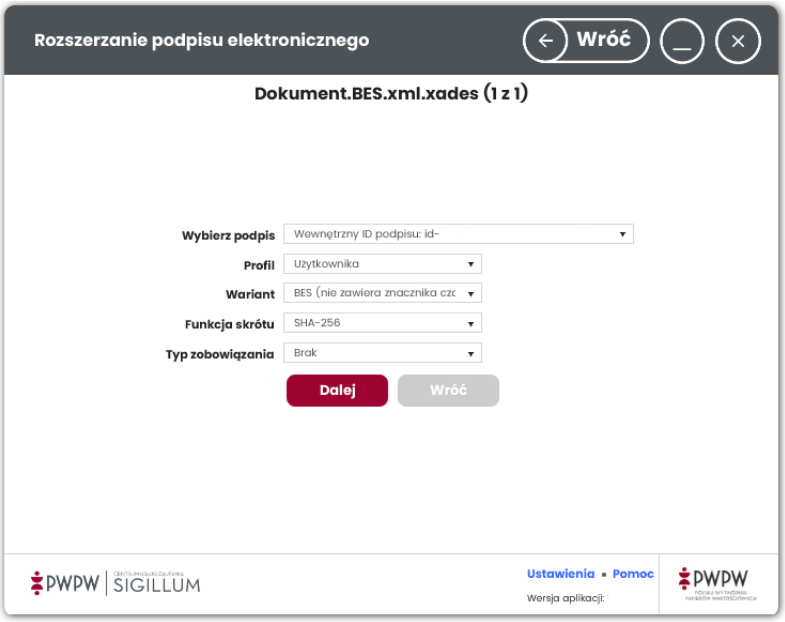
Format/typ/wariant	Zastąp istniejący podpis nowym	Rozszerz podpis elektroniczny	Dodaj kontrasygnatę	Dodaj znacznik czasu
XAdES Zewnętrzny BES		Tak	Tak	Tak
XAdES Zewnętrzny T		Tak	Tak	Tak
XAdES Otaczający BES		Tak		Tak
XAdES Otaczający T		Tak		Tak
XAdES Otoczony BES	Tak	Tak	Tak	Tak
XAdES Otoczony T	Tak	Tak	Tak	Tak
PadES Otoczony BES		Tak	Tak	Tak
PadES Otoczony T		Tak	Tak	Tak
CAdES Zewnętrzny BES		Tak	Tak	Tak
CAdES Zewnętrzny T		Tak	Tak	Tak
CAdES Otaczający BES		Tak	Tak	Tak
CAdES Otaczający T		Tak	Tak	Tak
ASiC-S Otoczony BES		Tak		Tak
ASiC-S Otoczony T		Tak		Tak
ASiC-E Otoczony BES		Tak		Tak
ASiC-E Otoczony T		Tak		Tak

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



7.4.2 Zastąp istniejący podpis nowym

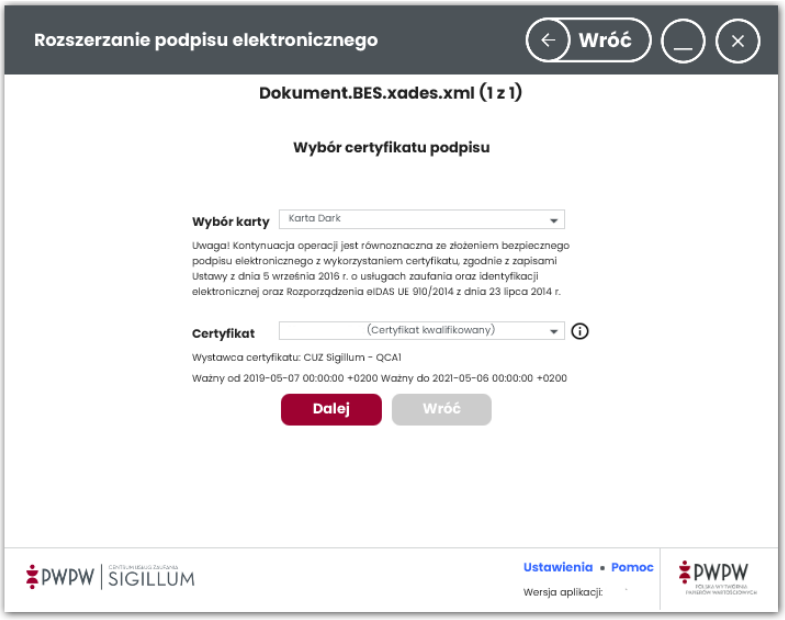
Po wybraniu tej opcji użytkownik wybiera podpis do zastąpienia oraz określa *Profil*, *Wariant*, *Funkcję skrótu* i *Typ zobowiązania*.



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.

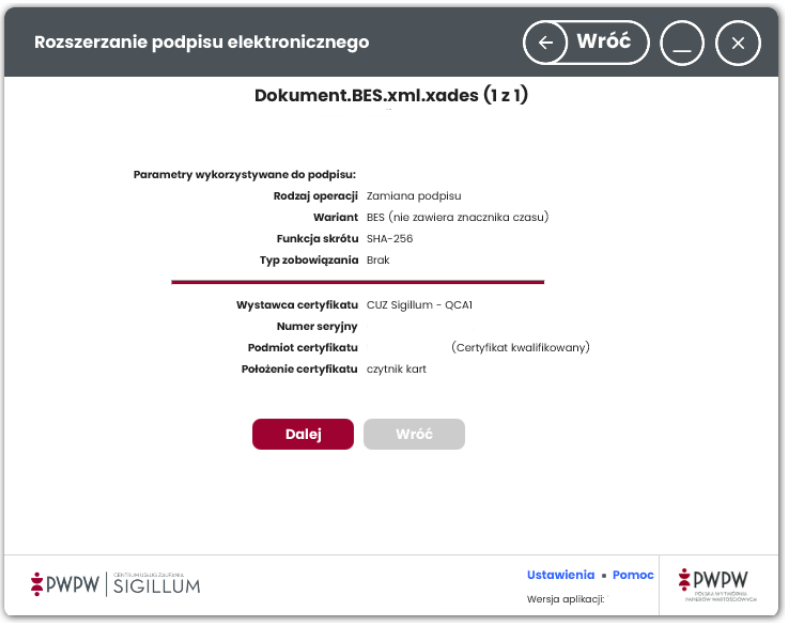
Po wyborze karty i certyfikatu, pojawia się informacja na temat certyfikatu i skutku prawnego wywołanego jego użyciem.



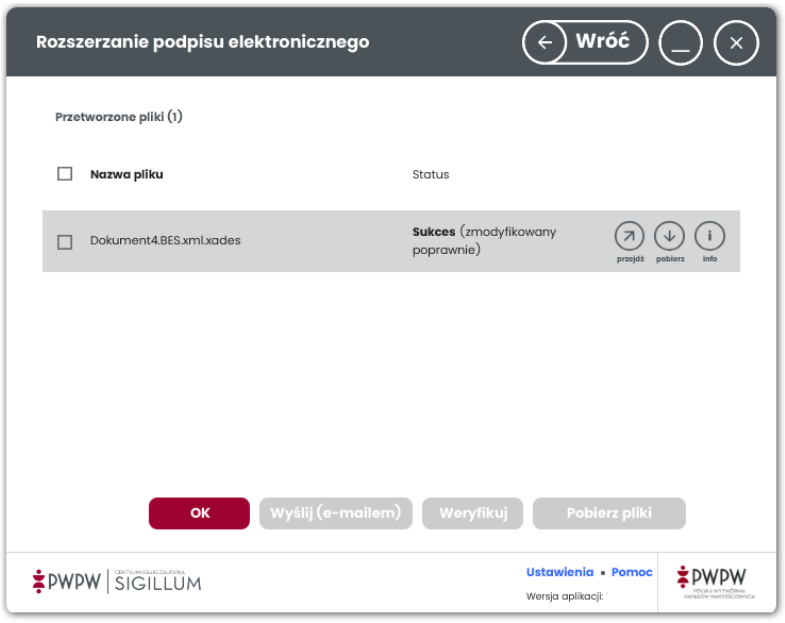
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny.

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 – zapisywanie podpisanego pliku,
- pobierz – zapisywanie pliku bez 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 katalogach, gdzie znajdują się pliki źródłowe. Podpis można zweryfikować w procesie weryfikacji.

7.4.3 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 poniższa tabela.

Format/typ/wariant	**Rozszerz do T**	**Rozszerz do XL**	**Rozszerz do A**
XadES Zewnętrzny BES	Tak	Tak	Tak
XadES Zewnętrzny T, XL		Tak	Tak
XadES Zewnętrzny A			Tak

XadES Otaczający BES	Tak	Tak	Tak
XadES Otaczający T, XL		Tak	Tak
XadES Otaczający A			Tak
XadES Otoczony BES	Tak	Tak	Tak
XadES Otoczony T, XL		Tak	Tak
XadES Otoczony A			Tak
PadES Otoczony BES	Tak	Tak	Tak
PadES Otoczony T, XL		Tak	Tak
PadES Otoczony A			Tak
CadES Zewnętrzny BES	Tak	Tak	Tak
CadES Zewnętrzny T, XL		Tak	Tak
CadES Zewnętrzny A			Tak
CadES Otaczający BES	Tak	Tak	Tak
CadES Otaczający T, XL		Tak	Tak
CadES Otaczający A			Tak
ASIC-S Otoczony BES	Tak	Tak	Tak
ASIC-S Otoczony T, XL		Tak	Tak
ASIC-E Otoczony A			Tak
ASIC-E Otoczony BES	Tak	Tak	Tak
ASIC-E Otoczony T, XL		Tak	Tak
ASIC-E Otoczony A			Tak

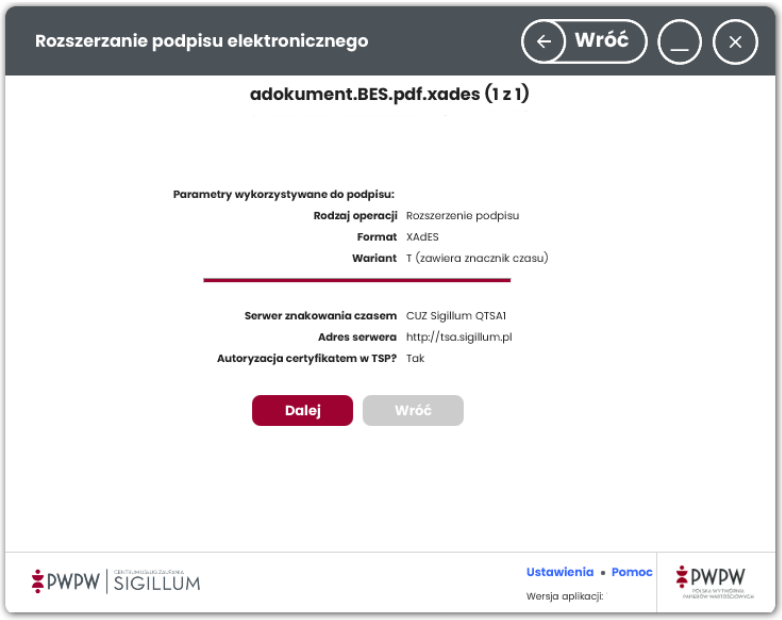
Po wyborze formatu rozszerzenia i kliknięciu przycisku Dalej prezentowany jest ekran wyboru karty i certyfikatu.

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.

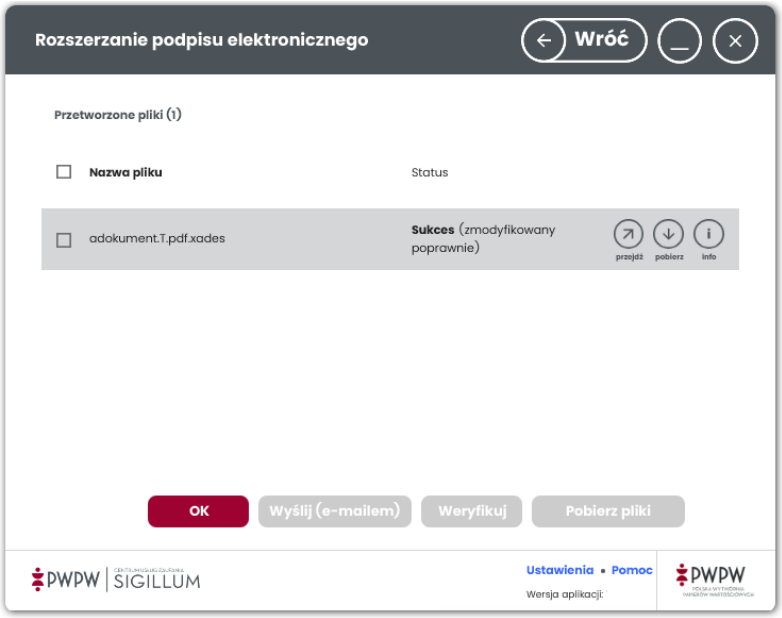
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny. Po wyborze certyfikatu, pojawia się informacja na temat certyfikatu i skutku prawnego wywołanego jego użyciem.

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 – zapisywanie podpisanego pliku,
- pobierz – zapisywanie pliku bez podpisu,
- info – szczegóły złożonego podpisu.

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

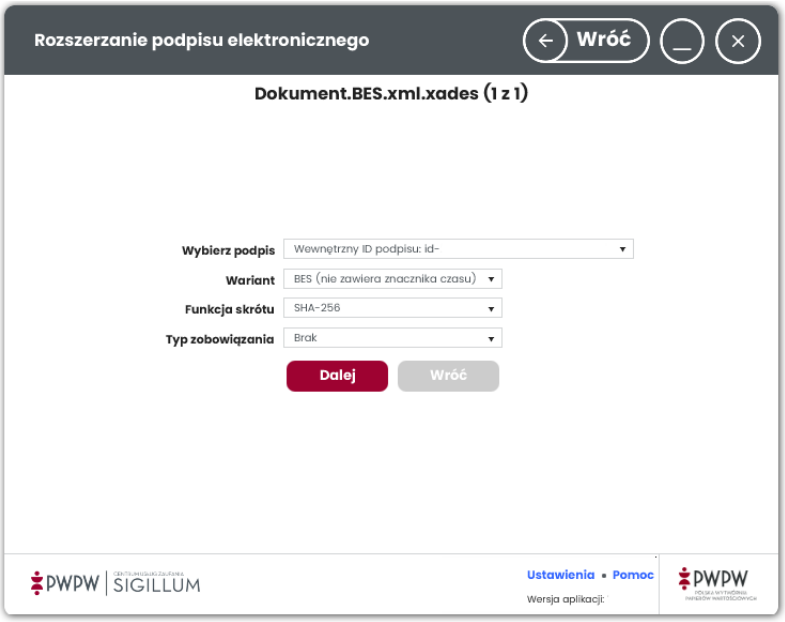
Po kliknięciu przycisku Weryfikuj wyświetlany jest ekran weryfikacji podpisanych plików.

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

7.4.4 Dodaj kontrasygnatę

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

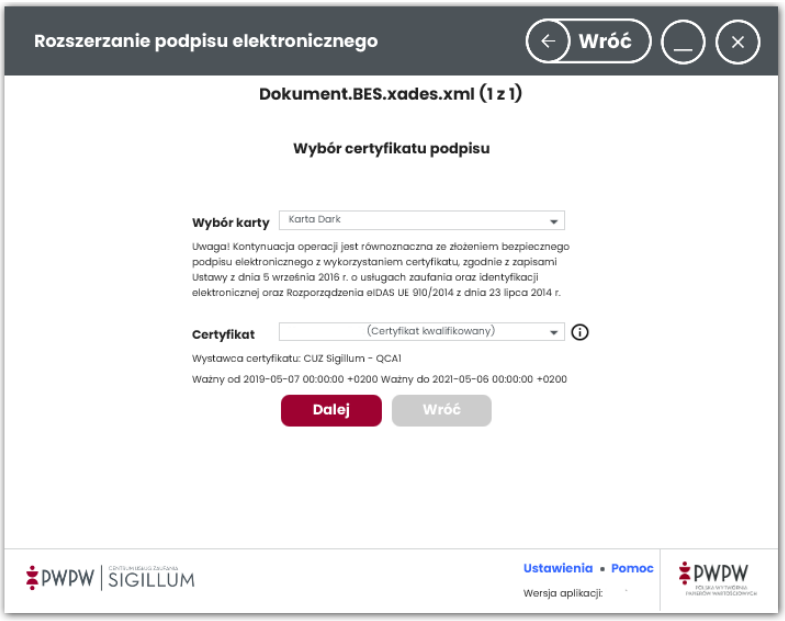
Użytkownik wybiera podpis do zastąpienia oraz określa *Wariant*, *Funkcję skrótu* i *Typ zobowiązania*.



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.

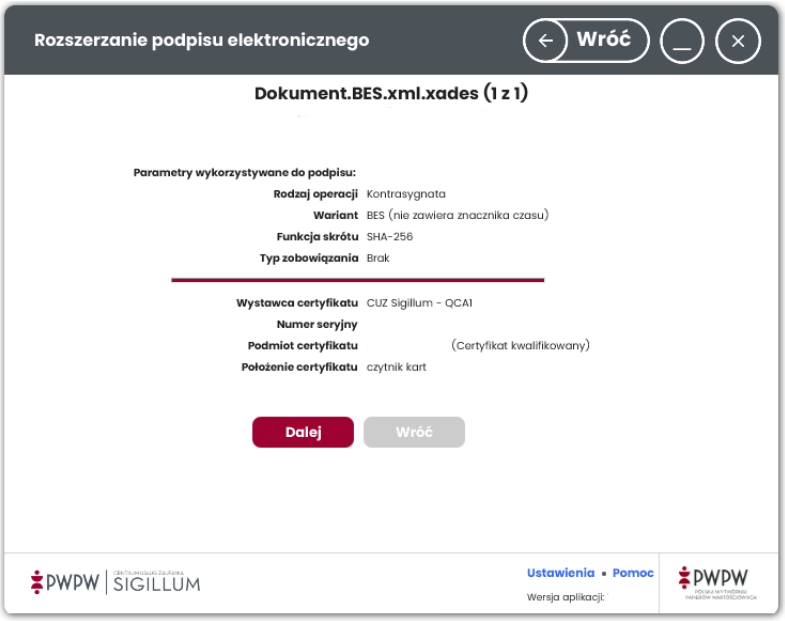
Po wyborze karty i certyfikatu, pojawia się informacja na temat certyfikatu i skutku prawnego wywołanego jego użyciem.



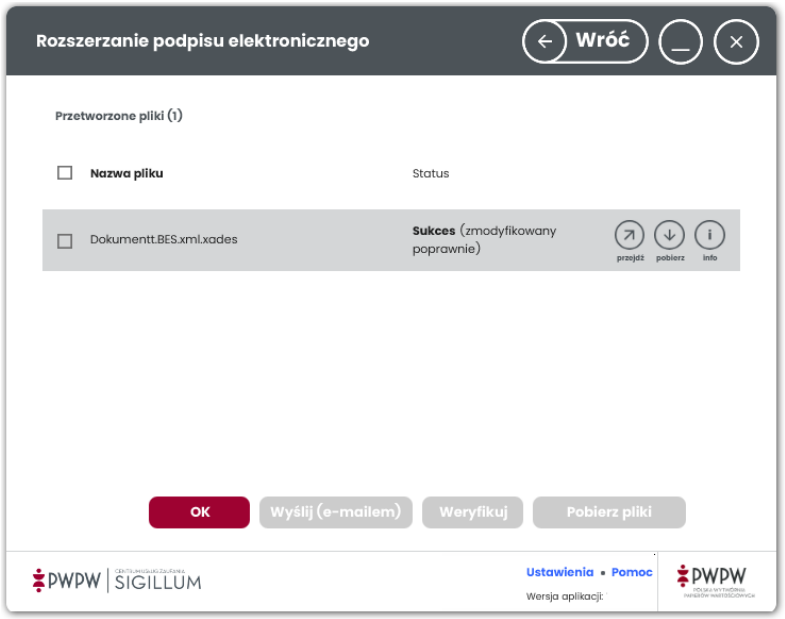
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny.

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 – zapisywanie podpisanego pliku,
- pobierz – zapisywanie pliku bez 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 katalogach, gdzie znajdują się pliki źródłowe. Podpis można zweryfikować w procesie weryfikacji.

7.4.5 Dodaj znacznik czasu

Wybranie opcji *Dodaj znacznik czasu oznacza, że do podpisu, przyporządkowanego do pliku dodany zostanie znacznik czasu.*

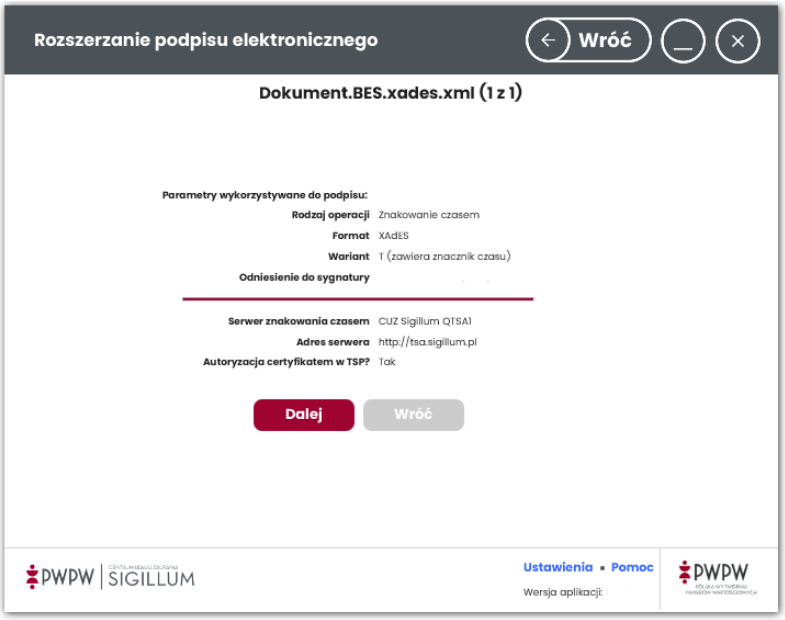
Użytkownik wybiera kartę i certyfikat znakowania czasem.

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.

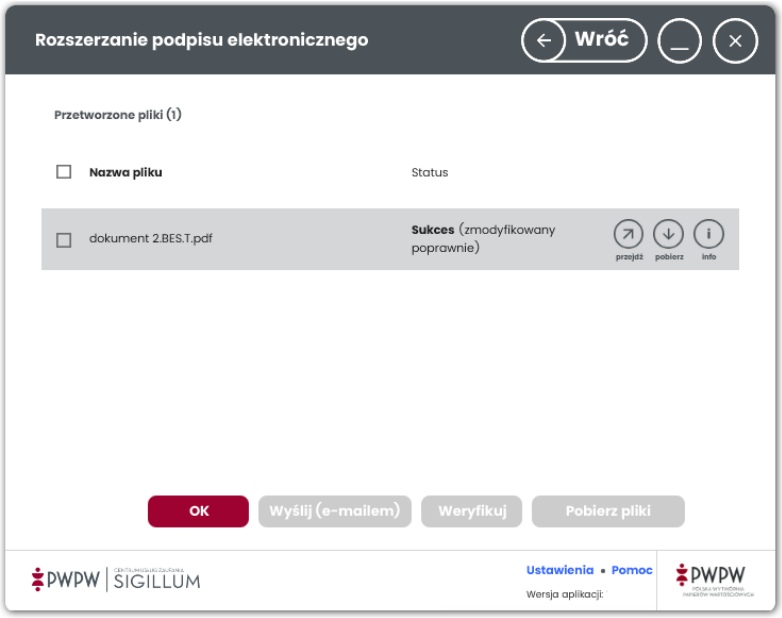
W zależności od preferencji użytkownik może wskazać certyfikat kwalifikowany lub komercyjny.

Po 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 – zapisywanie podpisanego pliku,
- pobierz – zapisywanie pliku bez podpisu,
- info – szczegóły złożonego podpisu.

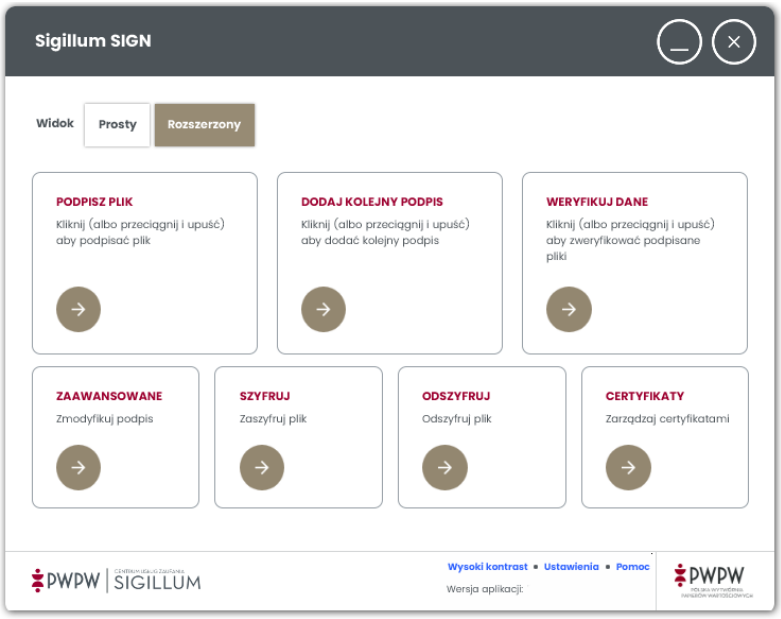
Po zaznaczeniu checkboxa w wierszu wybranych plików można wysłać podpisane dokumenty poprzez e-mail klikając przycisk Wyślij (e-mailem).
Po kliknięciu przycisku Weryfikuj wyświetlany jest ekran weryfikacji podpisanych plików.

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

7.5 Szyfrowanie plików

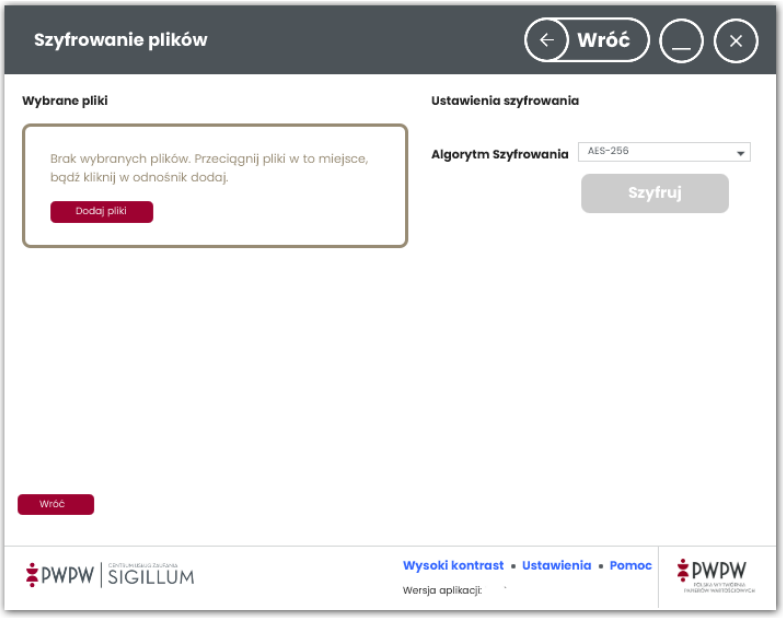
7.5.1 Ekran startowy procesu szyfrowania

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.



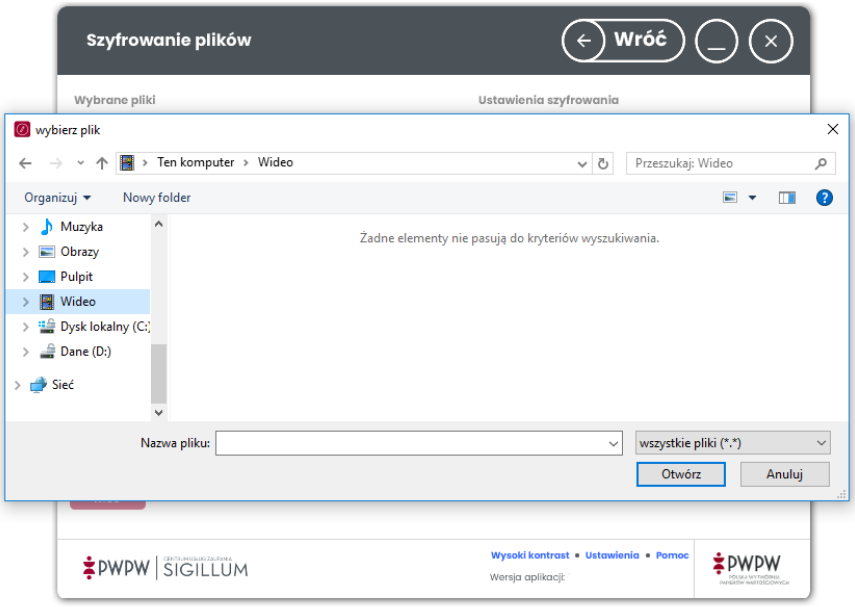
7.5.2 Ekran ustawień szyfrowania

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

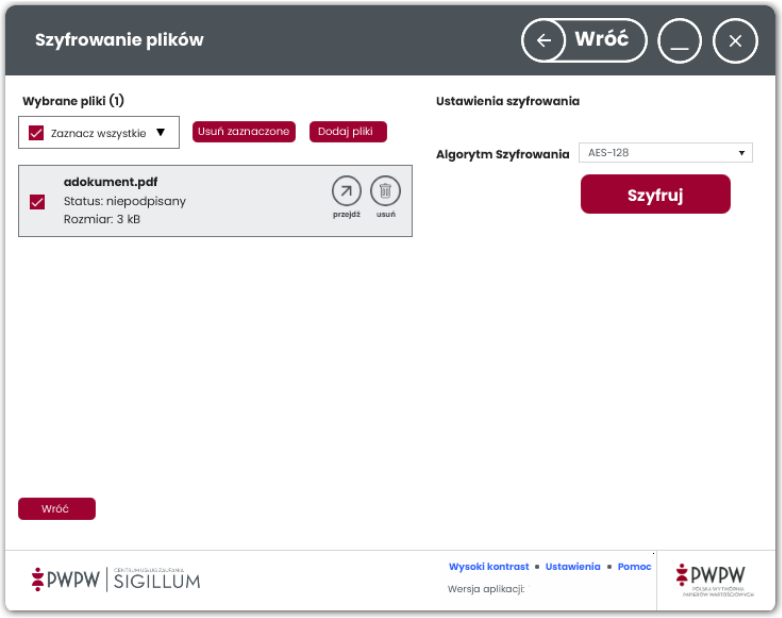


Ekran podzielony jest na dwie części: lewą tzw. obszar roboczy, w którym prezentowane są pliki oraz prawą tzw. obszar ustawień, zawierający ustawienia związane z szyfrowaniem oraz przycisk ***„Szyfruj”***.

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.*

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

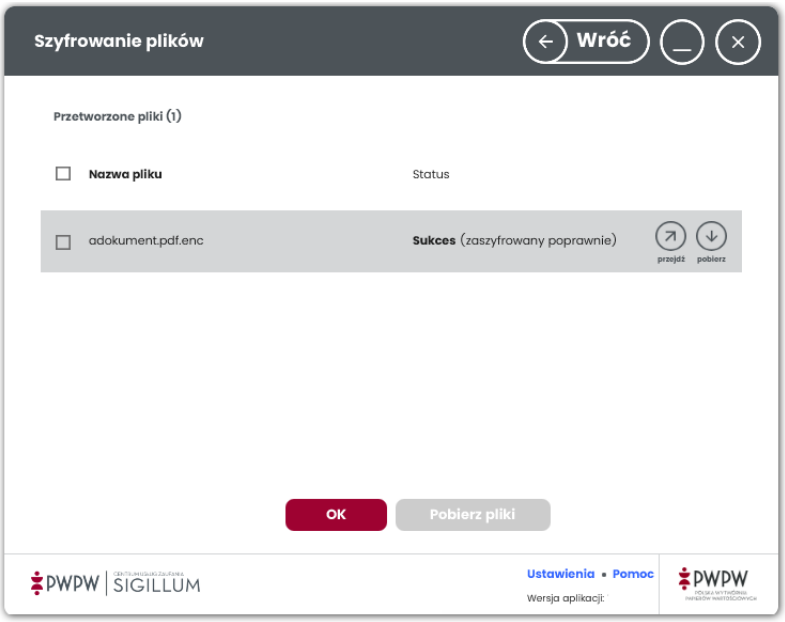
Okno szyfrowania prezentuje użytkownikowi dostępne certyfikaty służące do szyfrowania plików.

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 6.6), 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.



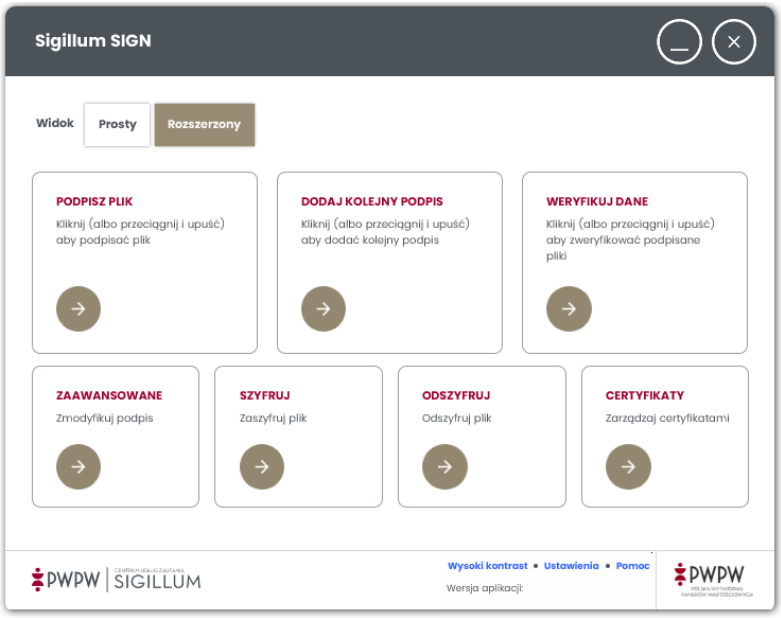
W kolumnie „Status" wyświetlany jest status otrzymany po wykonaniu operacji.

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

7.6 Odszyfrowywanie plików

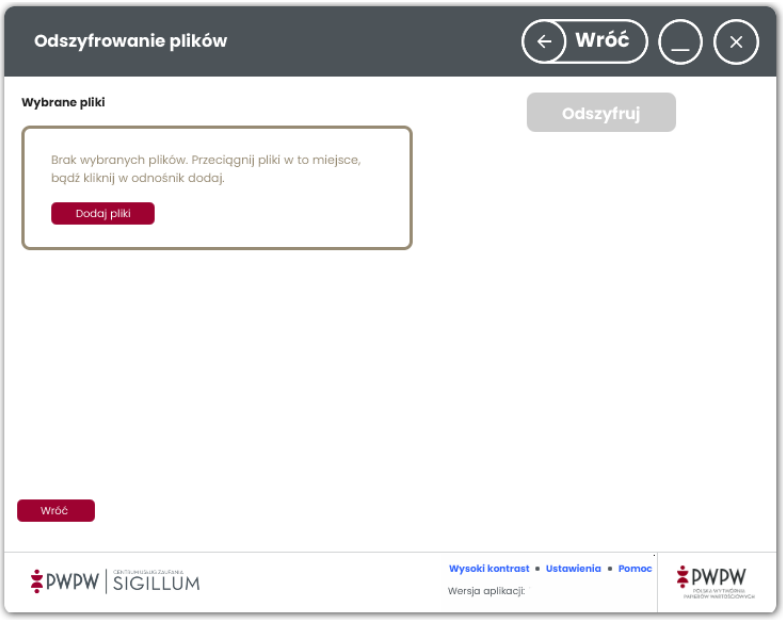
7.6.1 Ekran startowy procesu odszyfrowania

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

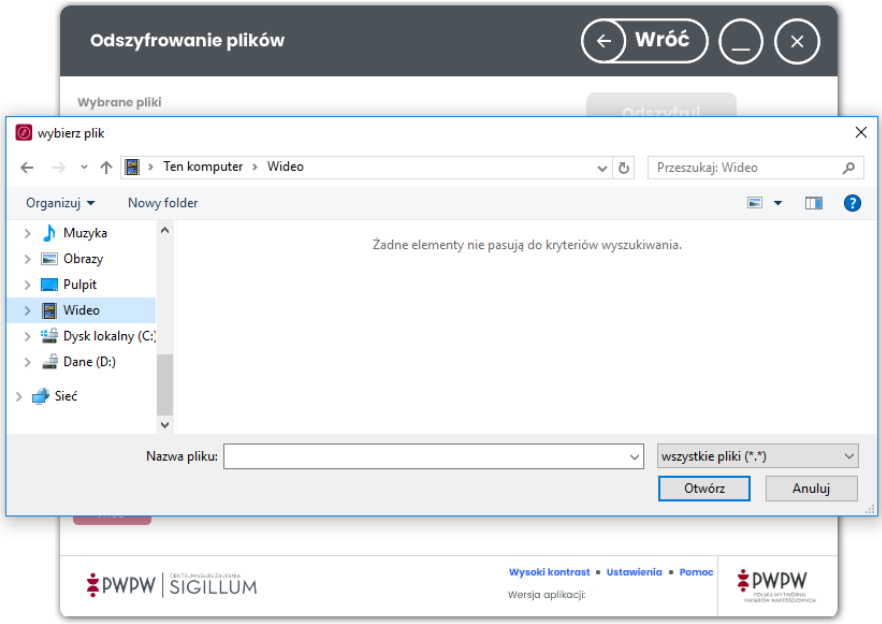
Po wyborze opcji ***„Odszyfruj”*** użytkownikowi prezentowany jest ekran odszyfrowania plików.



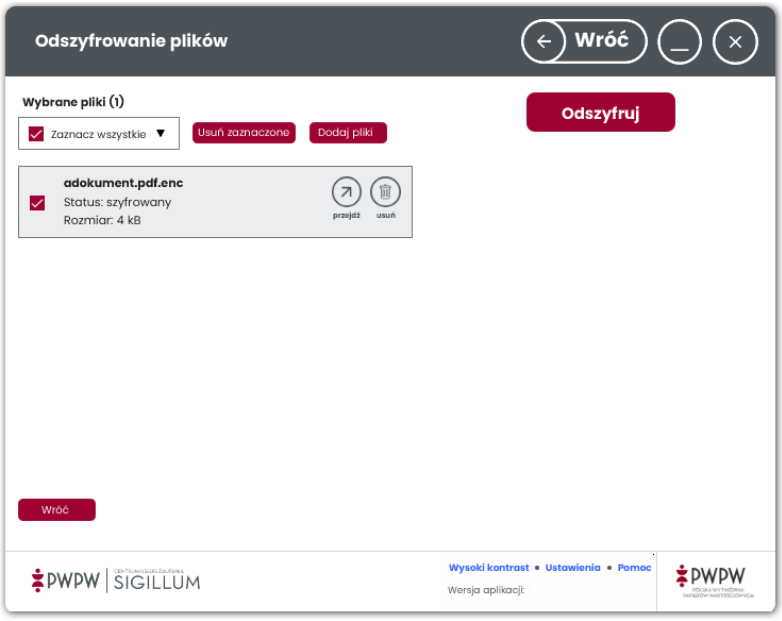
Okno podzielone jest na dwie części: lewą tzw. obszar roboczy, w którym prezentowane są pliki oraz prawą zawierającą przycisk ***„Odszyfruj”***.

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.*

Po kliknięciu w ikonę strzałki można otworzyć plik.

Kliknięcie w ikonę kosza pozwala usunąć plik z obszaru roboczego.

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

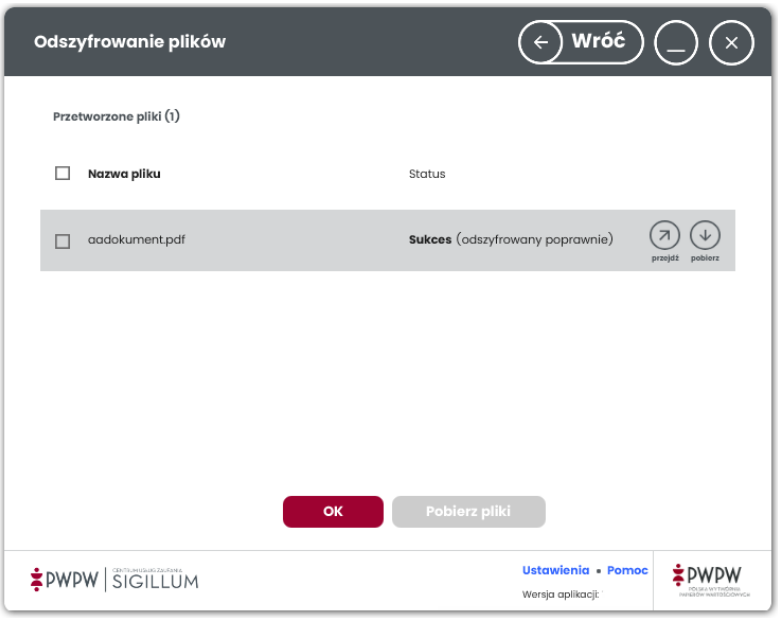
Po wykonaniu tej czynności prezentowany jest kolejny widok Ekran szyfrowania.

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 system odszyfrowuje plik i wyświetla ekran podsumowania.



W kolumnie „Status" wyświetlany jest status otrzymany po wykonaniu operacji.

Potwierdzenie (OK) kończy proces szyfrowania. Zaszyfrowane pliki odnaleźć można w katalogach, 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,
- 800 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:
    - CryptoCard Suite w wersji 2.00.00261 i wyższej
    - 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

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 Commitmen 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.
-cert	-c	

8.5 Przełącznik –help

Użycie tego polecenia powoduje wyświetlenie pomocy aplikacji w postaci listy przełączników i opcji, które użytkownik może wykorzystać.
Przykład użycia: 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 | 2013-12-13 12:52:05 - 2015-12-13 12:52:05 | SIGNER ENCRYPTION
[1] Jan kowalski | komercyjny | 052aa3 | 2013-12-13 12:45:55 - 2015-12-13 12:45:55 | SIGNER ENCRYPTION
```

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 –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

8.9 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, SHA512] -cert <numer

certyfikatu z listy dla operacji sign> -pin <kod pin do karty> -ct <typ potwierdzenia, numer z listy ctlist> -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 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, które mogą być wykorzystane 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 Commitmen Type Indication, które mogą być wykorzystane do składania podpisu elektronicznego. Patrz przełącznik -ctlist
-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 -f "D:\podpis.txt"

8.10 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 [SHA 1, SHA 256, SHA 512] -cert <numer certyfikatu z listy dla operacji sign> -pin <kod pin do karty> -ct <typ potwierdzenia, numer z listy ctlist> -f <ścieżka do pliku> -of <ścieżka do pliku źródłowego>

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 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, które mogą być wykorzystane 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 Commitmen Type Indication, które mogą być wykorzystane do składania podpisu elektronicznego. Patrz przełącznik -ctlist
-f	Nie dotyczy	Ścieżka do pliku z podpisem elektronicznym lub katalogów
-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 -f "D:\podpis.BES.txt.xades"

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

8.11 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 [SHA 1, SHA 256, SHA 512] -cert <numer certyfikatu z listy> -pin <kod pin do karty> -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 ulegać będzie kontrasygnacie. 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
-hash	SHA1 SHA256 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, które mogą być wykorzystane 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, które mogą być wykorzystane do składania podpisu elektronicznego. Patrz przełącznik -ctlist
-f	Nie dotyczy	Ścieżka do pliku z podpisem elektronicznym lub katalogów
-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 -f "D:\podpis.BES.txt.xades"

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

8.12 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

8.13 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 z danymi, które mają ulec zaszyfrowaniu
-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"

8.14 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 z danymi, które mają ulec odszyfrowaniu
-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