Instrukcja obsługi

SECUREDOC v 2.0

Wersja 1.4

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
KRS: 0000408592
NIP: 9512352379

Dział handlowy:
+48 22 490 36 45
handlowy@eurocert.pl

Dział techniczny:
+48 22 490 49 86
wsparcie@eurocert.pl

+48 22 390 59 95
biuro@eurocert.pl
www.eurocert.pl

Spis treści

1. Informacje o programie 3
2. Wymagania techniczne 3
3. Instalacja aplikacji 3
4. Podpisywanie 5
   - 4.1 Sekcja **Format podpisu** 5
   - 4.2 Sekcja **Parametry podpisu** 5
     - 4.2.1 Wariant podpisu 6
     - 4.2.2 Typ podpisu 6
     - 4.2.3 Funkcja skrótu 8
     - 4.2.4 Rodzaj zobowiązania 8
   - 4.3 Sekcja **Dane** 9
   - 4.4 Proces złożenia podpisu z reprezentacją graficzną 9
   - 4.5 Dodawanie kolejnych podpisów do pliku 13
5. Weryfikowanie 14
   - 5.1 Proces weryfikacji plików 14
6. Ustawienia 15
   - 6.1 Sekcja **Ustawienia aplikacji** 15
     - 6.1.1 Ustawienia ogólne 15
     - 6.1.2 Ustawienia podpisywania 16
     - 6.1.3 Ustawienia znacznika czasu 17
   - 6.2 Sekcja **Zarządzanie kartą** 17
     - 6.2.1 Zmiana PIN-u 18
     - 6.2.2 Odblokowanie PIN-u 18
     - 6.2.3 Zmiana SO PIN 19
7. Odnowienie certyfikatu 20
8. Pomoc 20
9. O programie 20

1. Informacje o programie

SecureDoc 2.0 to aplikacja przeznaczona do składania i weryfikacji podpisów elektronicznych z możliwością wystawienia podpisu wraz ze znacznikiem czasu. Dodatkowo można za jej pomocą przeprowadzić odnowienie certyfikatu kwalifikowanego (tylko w przypadku podpisu karcianego).

Aplikacja pozwala wykonać podpis elektroniczny: PAdES-BES, PAdES-T, XAdES-BES, XAdES-T w typie Zewnętrznym, Wewnętrznym i Otoczonym (Detached, Enveloping i Enveloped).

2. Wymagania techniczne

- System operacyjny Windows 10, 11 (64bit)
- Połączenie internetowe (niezbędne przy podpisie chmurowym ECSigner, znaczniku czasu, weryfikacji oraz odnowieniu)

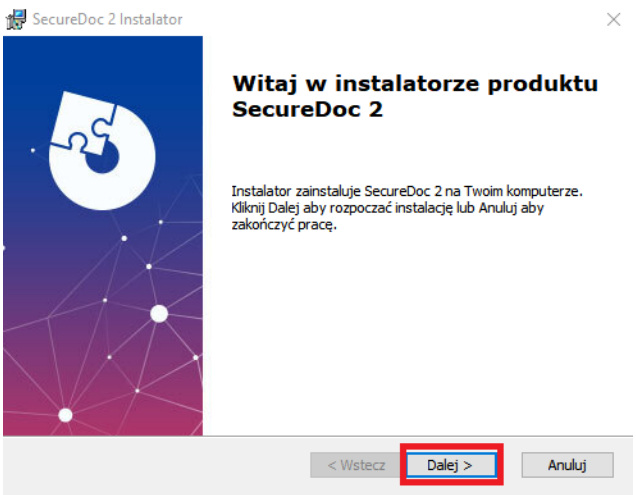
Aby korzystać z podpisu elektronicznego w aplikacji SecureDoc, na komputerze należy dodatkowo zainstalować:

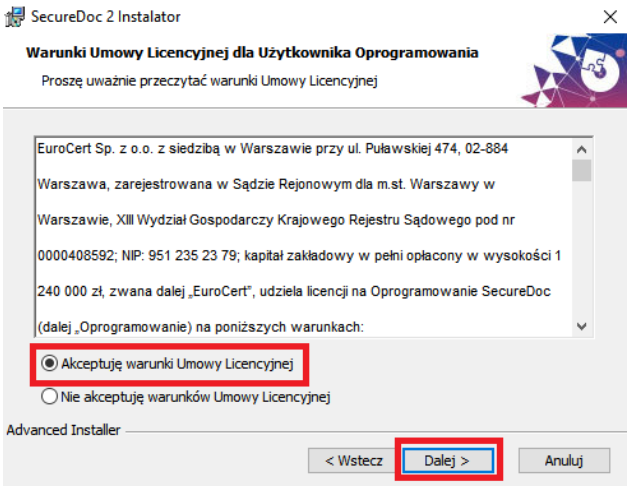
- Aplikację do zarządzania kartą - **Charismathics Smart Security Interface** – w przypadku podpisu na urządzeniu (czytnik USB z kartą)
- Aplikację **ECSigner** – w przypadku podpisu chmurowego ECSigner

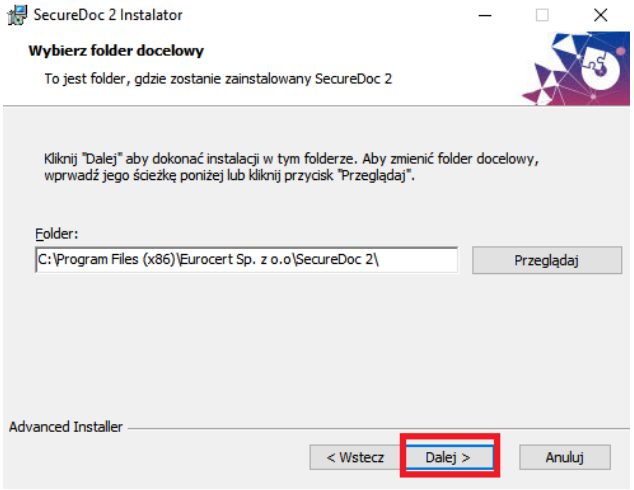
3. Instalacja aplikacji

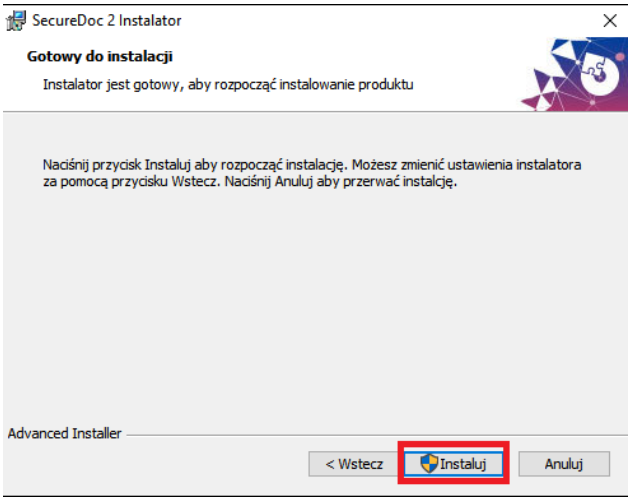
Wejdź na stronę eurocert.pl i pobierz ***SecureDoc 2 - aplikacja do składania i weryfikacji podpisu kwalifikowanego***.

Po pobraniu i uruchomieniu instalatora postępuj zgodnie z poniższymi oknami:









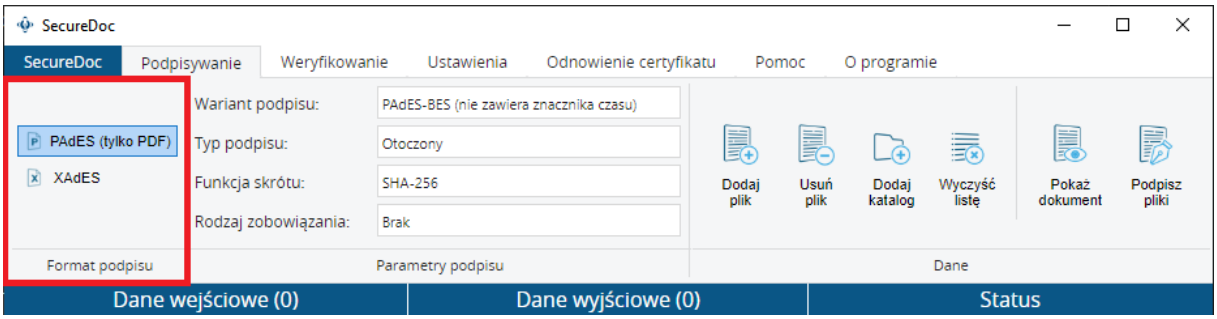
Po zakończeniu tego etapu aplikacja jest gotowa do użycia.

4. Podpisywanie

Zakładka **Podpisywanie** jest przeznaczona do składania podpisów elektronicznych. Proces podpisywania składa się z wybrania odpowiedniego formatu i parametrów podpisu, dodania plików do listy, wybrania odpowiedniego certyfikatu i autoryzacji. Cały proces jest dokładnie opisany w dalszej części instrukcji.

4.1 Sekcja **Format podpisu**

W sekcji **Format podpisu** dostępne są dwa formaty podpisu elektronicznego:

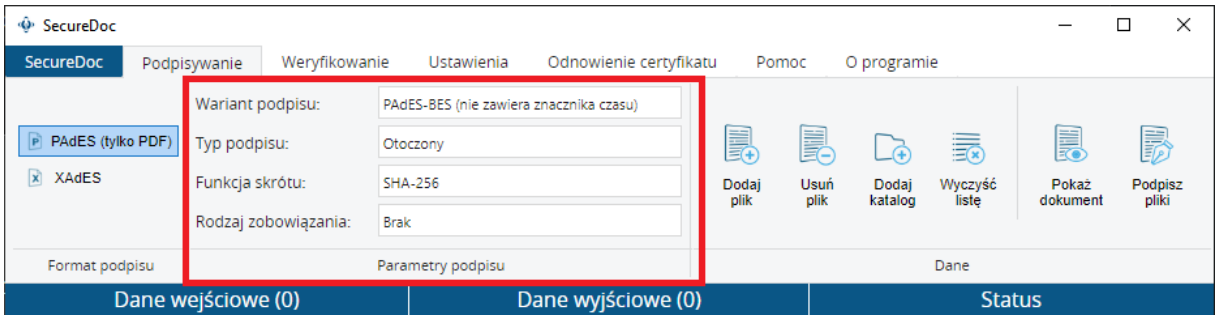


Format PAdES jest dedykowany dla plików PDF. Tylko przy nim możliwe jest dodanie reprezentacji graficznej podpisu.

Formatem XAdES mogą zostać podpisane pliki o dowolnym rozszerzeniu (.xml, .docx, .odt itd.). Mimo, że jest to technicznie możliwe, nie zalecamy podpisywania plików PDF formatem podpisu XAdES.

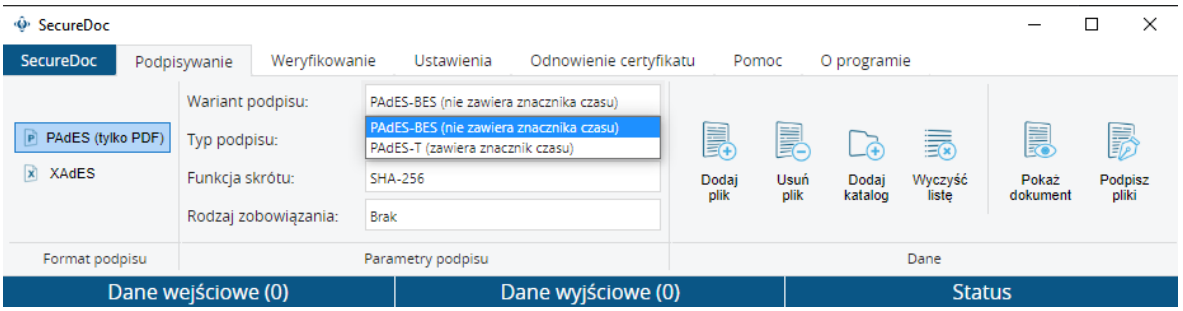
4.2 Sekcja **Parametry podpisu**

W tej sekcji znajdziemy najważniejsze parametry, które zostaną zastosowane na obecnej liście plików po kliknięciu **Podpisz pliki**. Poszczególne parametry wpływają na to jakie pliki będziemy mogli dodać do tej listy oraz w dużej mierze na ostateczny efekt po złożeniu podpisu. Jako użytkownik aplikacji SecureDoc mamy pewną swobodę wyboru sposobu, w jaki podpiszemy dany plik – zazwyczaj jest więcej niż jeden sposób. Musimy być jednak świadomi tego, jak dane parametry wpłyną na podpisywany plik. Nierzadko musimy dostosować się do wymagań jakiegoś zewnętrznego systemu, do którego ostatecznie będziemy przesyłać pliki po podpisie.



4.2.1 Wariant podpisu

W zależności od wybranego formatu podpisu dostępne są następujące opcje: PAdES-BES / PAdES-T lub XAdES-BES / XAdES-T.



Wariant **-BES** oznacza, że przy podpisywaniu dokumentu w danym formacie, nie będzie on zawierał znacznika czasu.

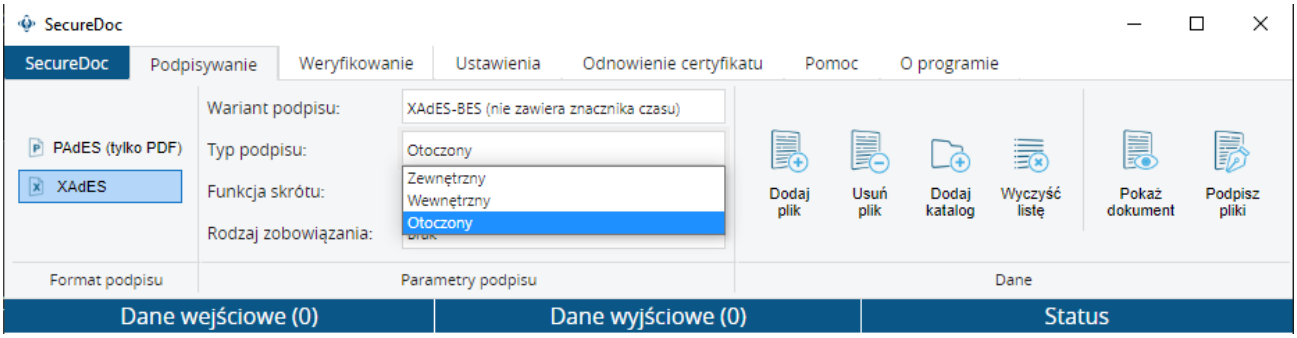
Wariant **-T** oznacza, że podpis zostanie złożony ze znacznikiem czasu. Usługa kwalifikowanego znakowania czasem („znacznik czasu" wspomniany wyżej) jest usługą dodatkową i umożliwia dokładne określenie daty i czasu czynności realizowanych w środowisku elektronicznym.

Znacznik czasu umożliwia więc potwierdzenie czasu w jakim został złożony podpis elektroniczny, czy określenie, że dany dokument istniał w określonym czasie i nie został zmieniony. W rozumieniu przepisów obowiązującego prawa wywołuje to skutki daty pewnej.

Używając znacznika czasu wydanego przez kwalifikowany podmiot, otrzymujesz gwarancję niepodważalności terminu podpisania dokumentu względem: sądów, instytucji, firm, klientów indywidualnych itp.

Znacznik czasu nie pobiera aktualnego czasu z komputera, na którym jest wystawiany podpis, lecz zwraca się do dedykowanego serwera, aby uzyskać informacje o czasie.

4.2.2 Typ podpisu



4.2.2.1 Zewnętrzny

Typem podpisu **Zewnętrzny** można podpisać pliki o dowolnym rozszerzeniu. Podczas składania podpisu zewnętrznego sam podpis elektroniczny będzie utworzony w odrębnym pliku i zapisany w tym samym folderze, w którym znajduje się plik podpisywany. Plik podpisu zewnętrznego zapisywany jest w formacie .XAdES

Należy pamiętać, że podczas weryfikacji takiego podpisu trzeba posiadać plik źródłowy (zawierający treść dokumentu) **oraz** plik podpisu (zawierający poświadczenie złożenia podpisu). Także podczas wysyłania podpisu zewnętrznego konieczne jest załączenie pliku podpisywanego (pliku zawierającego treść dokumentu).

Po złożeniu podpisu **Zewnętrznego**, unikamy jakichkolwiek modyfikacji zarówno pliku źródłowego jak i nowoutworzonego pliku. Modyfikacja treści jednego z plików spowoduje naruszenie integralności danych i podpis nie będzie mógł zostać zweryfikowany poprawnie. W przypadku programu SecureDoc istotne jest również, aby nie modyfikować również nazw tych plików.

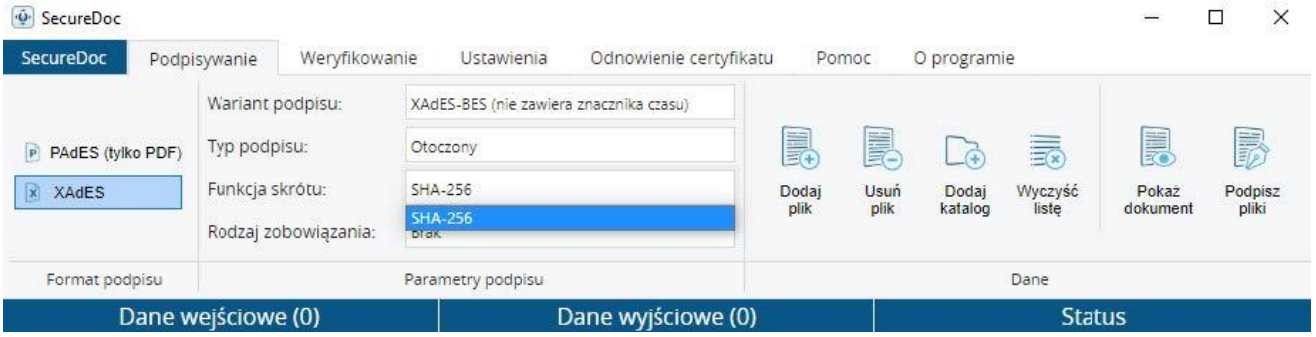
4.2.2.2 Wewnętrzny

Dany typ podpisu powinien być wykorzystywany dla jakichkolwiek plików podpisywanych w formacie XAdES, w których chcemy, aby podpis był zawarty w pliku podpisywanym. Czyli plik podpisu, podpisanego typem **Wewnętrznym** będzie zawierał zarówno treść dokumentu źródłowego jak i poświadczenie złożenia podpisu (2w1). Plik podpisany typem wewnętrznym będzie zapisany w formacie XAdES. Utworzony w ten sposób plik jest wystarczający do poprawnej weryfikacji podpisu.

4.2.2.3 Otoczony

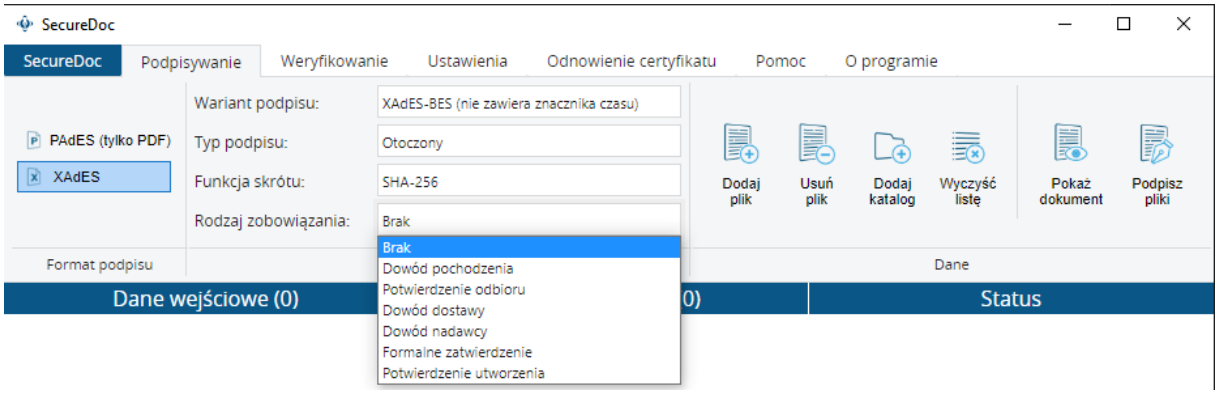
Przy formacie podpisu PAdES jedynym dostępny typem podpisu jest **Otoczony** – jest on automatycznie wybrany po wyborze tego formatu. Przy formacie podpisu XAdES typ podpisu **Otoczony** jest dedykowany dla plików XML. Przy domyślnych ustawieniach aplikacji SecureDoc podpisując plik z użyciem typu podpisu **Otoczony** efektem operacji będzie modyfikacja pliku źródłowego. To znaczy, że plik wskazany do podpisania w ten sposób zostanie nadpisany - nie zmieni się jego rozszerzenie, nazwa ani lokalizacja.

4.2.3 Funkcja skrótu



Ten parametr wskazuje na konkretny algorytm, który zostanie użyty do wyliczenia tzw. skrótu pliku (hash pliku), który jest podpisywany.

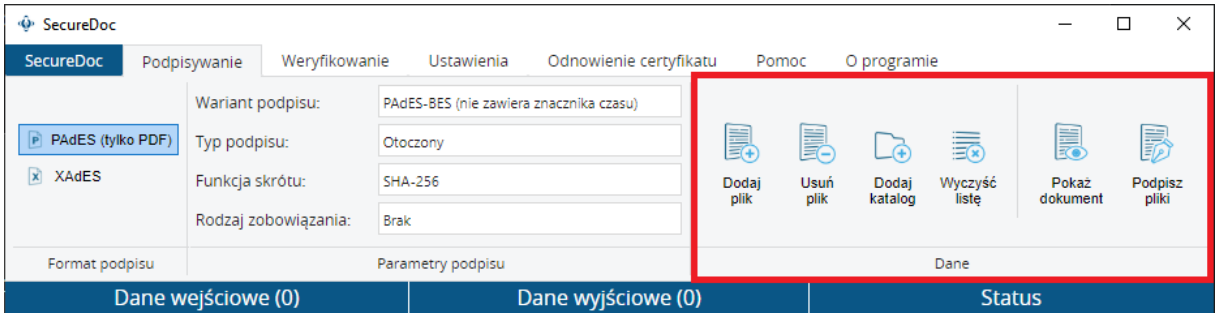
4.2.4 Rodzaj zobowiązania



Ten opcjonalny parametr dodaje do podpisu informacje na temat powodu jego złożenia. Poza domyślną wartością „Brak” do wyboru dostępnych jest 6 rodzajów zobowiązań:

- Dowód pochodzenia
- Potwierdzenie odbioru
- Dowód dostawy
- Dowód nadawcy
- Formalne potwierdzenie
- Potwierdzenie utworzenia

4.3 Sekcja **Dane**



Po wciśnięciu „Dodaj plik” otworzy się okno, w którym należy wybrać pliki do podpisania. Pliki zostaną dodane do listy. Alternatywnie możemy przeciągnąć wybrane pliki i upuścić je na okno aplikacji.

"Dodaj katalog" – przycisk umożliwia dodanie wszystkich plików z wybranego folderu, które odpowiadają kryteriom z ustawień podpisu, np. jeżeli wybraliśmy format podpisu PAdES - z wybranego folderu zostaną zaciągnięte wszystkie pliki w formacie PDF, z kolei przy wybranym formacie XAdES i typie Zewnętrznym/Wewnętrznym zostaną zaciągnięte wszystkie dostępne pliki z wybranego folderu.

Możemy także usunąć pliki, które wybraliśmy do podpisywania przy pomocy przycisków „Usuń plik” – w celu pojedynczego usuwania (usunięty zostanie aktualnie wybrany, podświetlony plik) lub „Wyczyść listę” – aby usunąć wszystkie pliki z listy.

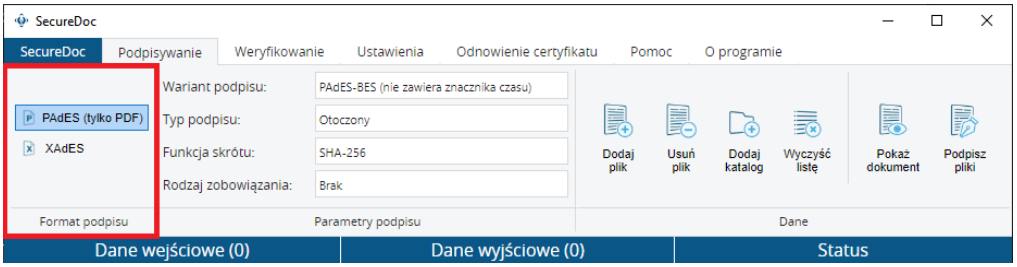
Wciśnięcie przycisku „Pokaż dokument” spowoduje wyświetlenie treści wybranego dokumentu w nowym oknie.

„Podpisz pliki” – po wciśnięciu danego przycisku rozpocznie się proces podpisywania wszystkich plików znajdujących się na liście.

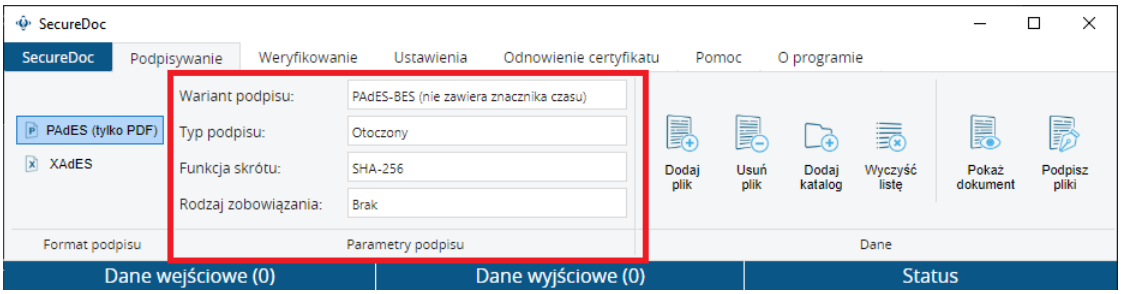
4.4 Proces złożenia podpisu z reprezentacją graficzną

Należy pamiętać, że w celu podpisania pliku podpisem kwalifikowanym urządzenie z kartą kryptograficzną musi być podłączone do komputera. Jeżeli używamy podpisu chmurowego ECSigner, aplikacja ECSigner musi działać w tle z zalogowanym kontem.

1. Wybieramy format podpisu PAdES (tylko PDF).



2. Wybieramy resztę pożądanych parametrów podpisu.

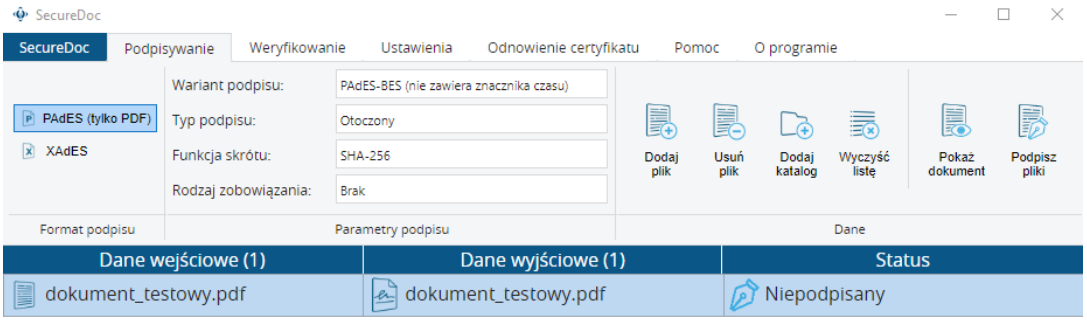


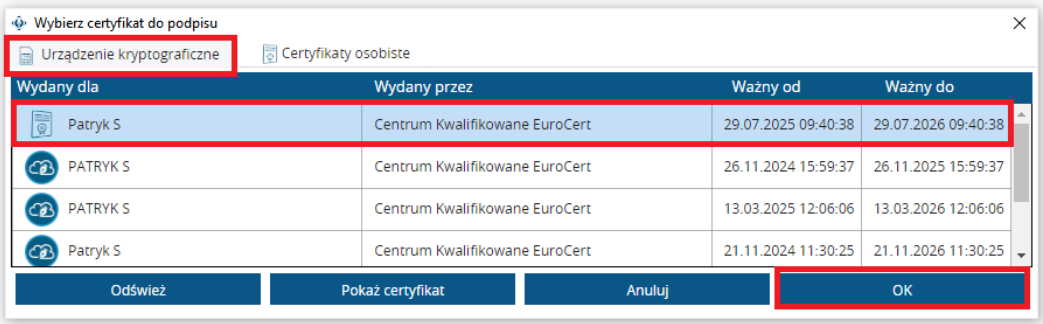
3. Dodajemy pliki, które chcemy podpisać za pomocą przycisku „Dodaj plik" lub przeciągamy je bezpośrednio z folderu na okno aplikacji SecureDoc.

4. Klikamy „Podpisz pliki". Warto zwrócić uwagę na to, że wszystkie dokumenty z listy wybranych do podpisania zostaną podpisane z takimi samymi parametrami podpisu.

   Po kliknięciu „Podpisz pliki" pojawi się okno wyboru certyfikatu. Wybieramy certyfikat, którym chcemy podpisać wybrane pliki i klikamy „OK". Zalecane jest korzystanie z zakładki **Urządzenie kryptograficzne**. W tej zakładce dostępne są certyfikaty, które znajdują się na aktualnie podłączonym urządzeniu oraz certyfikaty podpisu chmurowego ECSigner dostępne w danej chwili. Rodzaj podpisu można rozróżnić po ikonie widocznej przy imieniu i nazwisku właściciela certyfikatu.

   Uwaga: Zakładka **Certyfikaty osobiste** pozwala na odczytanie certyfikatów z magazynu systemu Windows. Często pojawią się tu certyfikaty niekwalifikowane, niezwiązane z EuroCert.

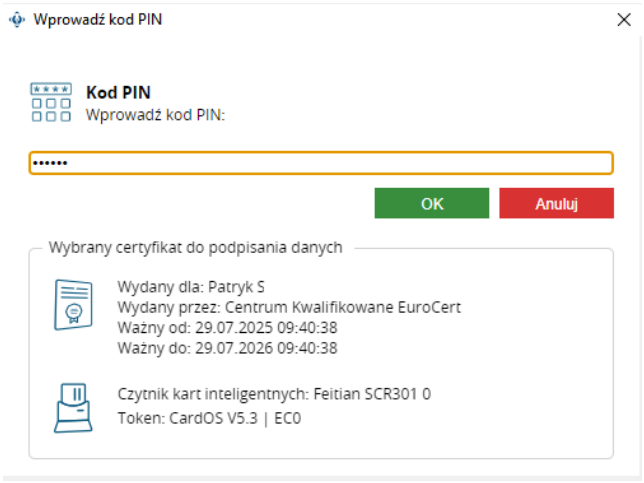




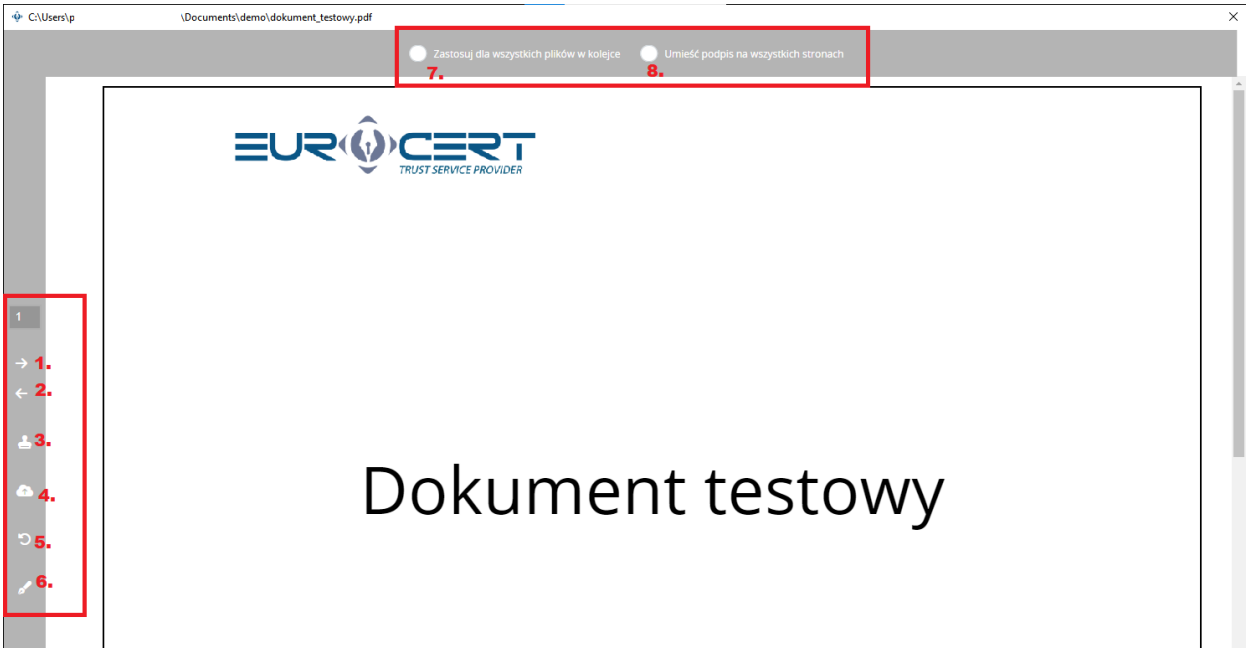
5. Po wybraniu certyfikatu i kliknięciu „OK" pojawi się komunikat dotyczący składanego podpisu. Po zapoznaniu się z komunikatem klikamy „OK".

6. Przy podpisie karcianym wprowadzamy kod PIN i klikamy „OK”.

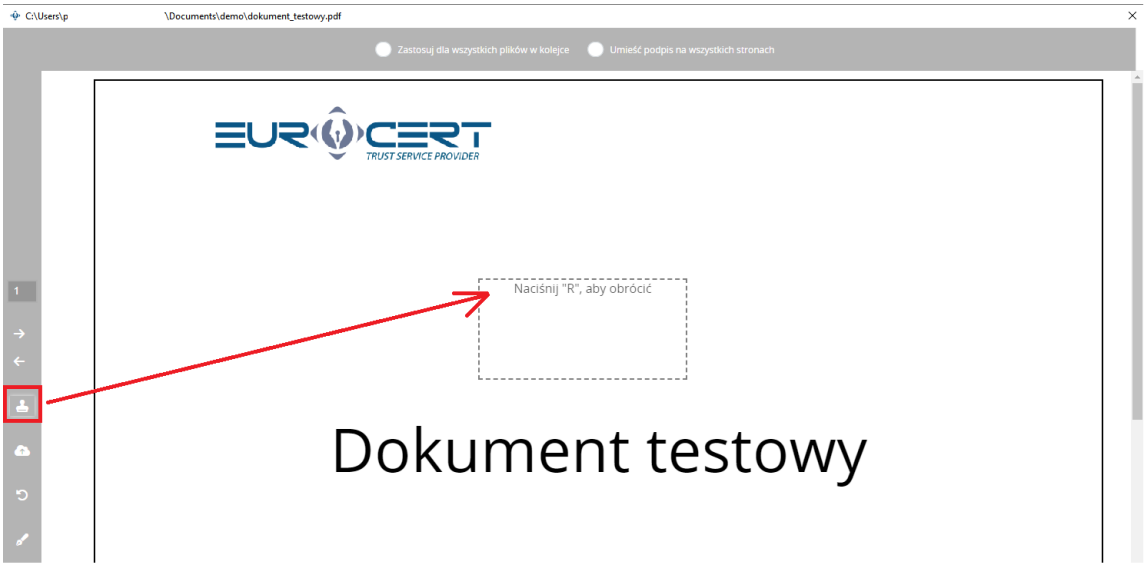
   Korzystając z podpisu chmurowego ECSigner, należy zalogować się do swojego konta, a następnie wprowadzić kod autoryzacyjny (kod OTP) z aplikacji mobilnej ECSigner.



7. Przy domyślnych ustawieniach aplikacji, w trakcie podpisywania pliku PDF formatem podpisu PAdES na tym etapie wyświetli się podgląd podpisywanego pliku. Na tym etapie użytkownik może dodać reprezentację graficzną podpisu w wybranym przez siebie miejscu na dokumencie. Nie ma to wpływu na moc prawną podpisu, jest to jedynie kwestia kosmetyczna. Dokładny opis przycisków zaznaczonych na poniższym obrazku znajduje się w kolejnych punktach.

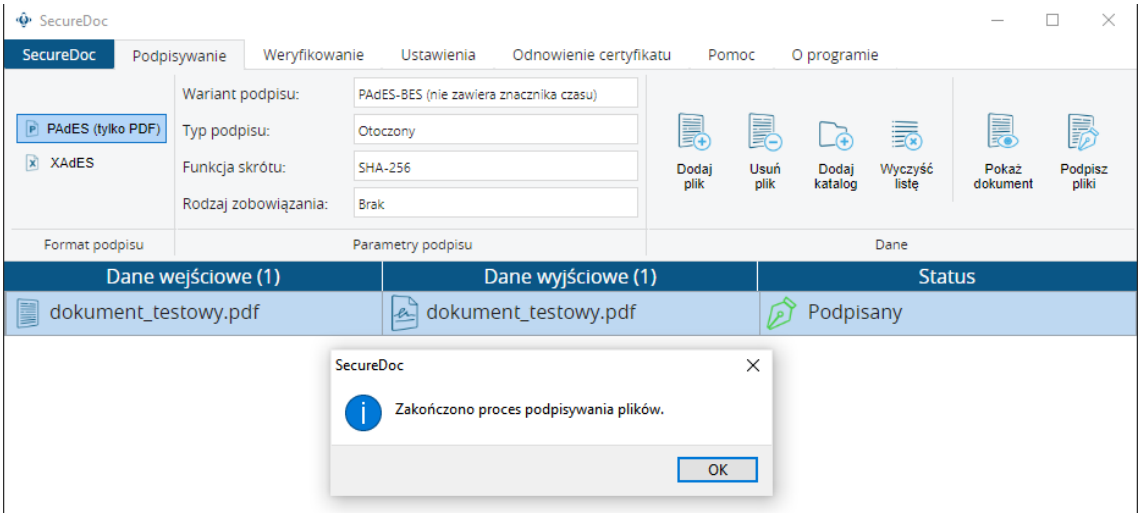


8. Klikamy na przycisk „Umieść pieczątkę” (3), następnie najeżdżamy kursorem myszy na miejsce, w którym chcemy dodać grafikę i klikamy lewy przycisk myszy. Aby przejść do innej strony dokumentu, możemy użyć odpowiednich strzałek (1) i (2), lub ręcznie wpisać numer strony w polu nad strzałkami.



Po dodaniu grafiki w wybranym miejscu klikamy przycisk „Podpisz” (6) z ikoną pióra, aby zakończyć proces.

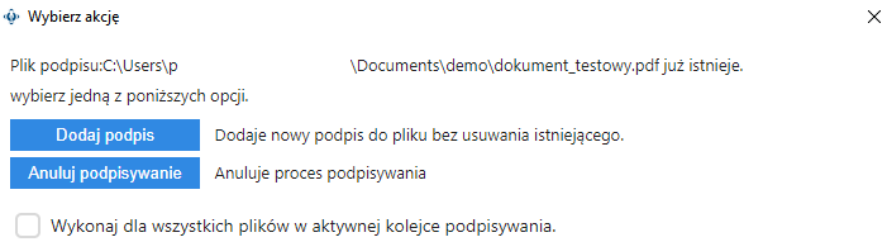
9. Sprawdzamy status dokumentu. Jeśli operacja się powiodła, w oknie statusu przy podpisanych plikach pojawi się status „Podpisany”. Jeśli wystąpił błąd, pojawi się status „Niepodpisany”.



10. (opcjonalnie)
Aplikacja SecureDoc umożliwia też zmianę domyślnego logo na swoje własne. W tym celu należy użyć przycisku „Załaduj logo” (4) i wybrać przygotowany wcześniej plik. Logo musi mieć taką samą szerokość i wysokość oraz być zapisane w formacie **.jpg** – w razie potrzeby można wrócić do domyślnego logo przy użyciu przycisku „Przywróć domyślne logo” (5). Podpisując wiele plików PDF na raz pomocna może się okazać funkcja „Zastosuj dla wszystkich plików w kolejce” (7) – w ten sposób ustawienia wybrane dla obecnie wyświetlonego pliku zostaną automatycznie zastosowane dla reszty plików w kolejce, bez potrzeby wyświetlania kolejno ich podglądu. Chcąc uzyskać efekt reprezentacji graficznej danego podpisu w tym samym miejscu na każdej stronie danego dokumentu należy użyć funkcji „Umieść podpis na wszystkich stronach” (8). Niezależnie od wybranych ustawień dotyczących reprezentacji graficznej, aby sfinalizować proces podpisywania należy użyć przycisku „Podpisz” (6).

4.5 Dodawanie kolejnych podpisów do pliku

Jeżeli plik zawiera już przynajmniej jeden podpis elektroniczny, proces podpisu będzie zawierał dodatkowe okno. W celu złożenia kolejnego podpisu na dokumencie, wybieramy w nim opcję „Dodaj podpis”.

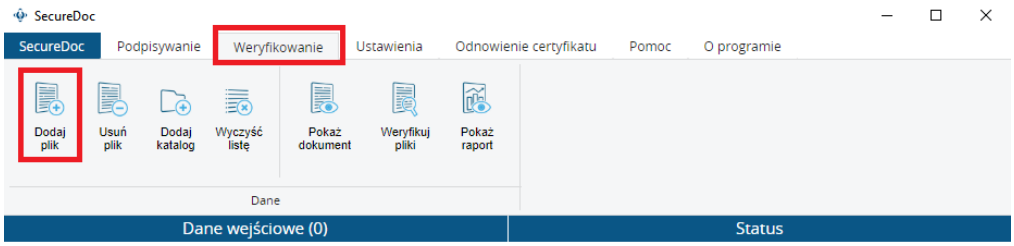


5. Weryfikowanie

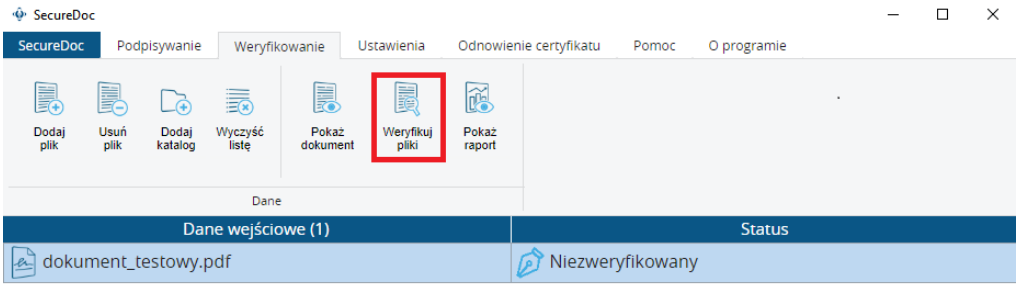
W danej zakładce mamy możliwość weryfikacji podpisanych plików oraz generowania raportów z weryfikacji. Możemy dodać na raz wiele plików nawet jeśli zostały one podpisane z użyciem innych formatów i parametrów podpisu. Przy plikach podpisanych XAdES'em Zewnętrznym musimy pamiętać o tym, aby zarówno plik źródłowy jak i nowo wygenerowany plik .XAdES znajdowały się w tym samym folderze. Inaczej weryfikacja nie będzie możliwa.

5.1 Proces weryfikacji plików

1. Dodajemy pliki, które chcemy zweryfikować za pomocą przycisku „Dodaj pliki" lub przeciągając i upuszczając je na okno aplikacji.



2. Klikamy „Weryfikuj pliki" (Należy pamiętać, że do weryfikacji wymagane jest połączenie z Internetem).



3. Czekamy na komunikat o statusie weryfikacji. Możliwe statusy to:

- **Pozytywnie zweryfikowany** – Wszystkie wykryte podpisy zweryfikowano pozytywnie
- **Negatywnie zweryfikowany** – Przynajmniej jeden podpis zweryfikowano negatywnie
- **Nieokreślony** – Wynik weryfikacji przynajmniej jednego podpisu nie jest jednoznaczny

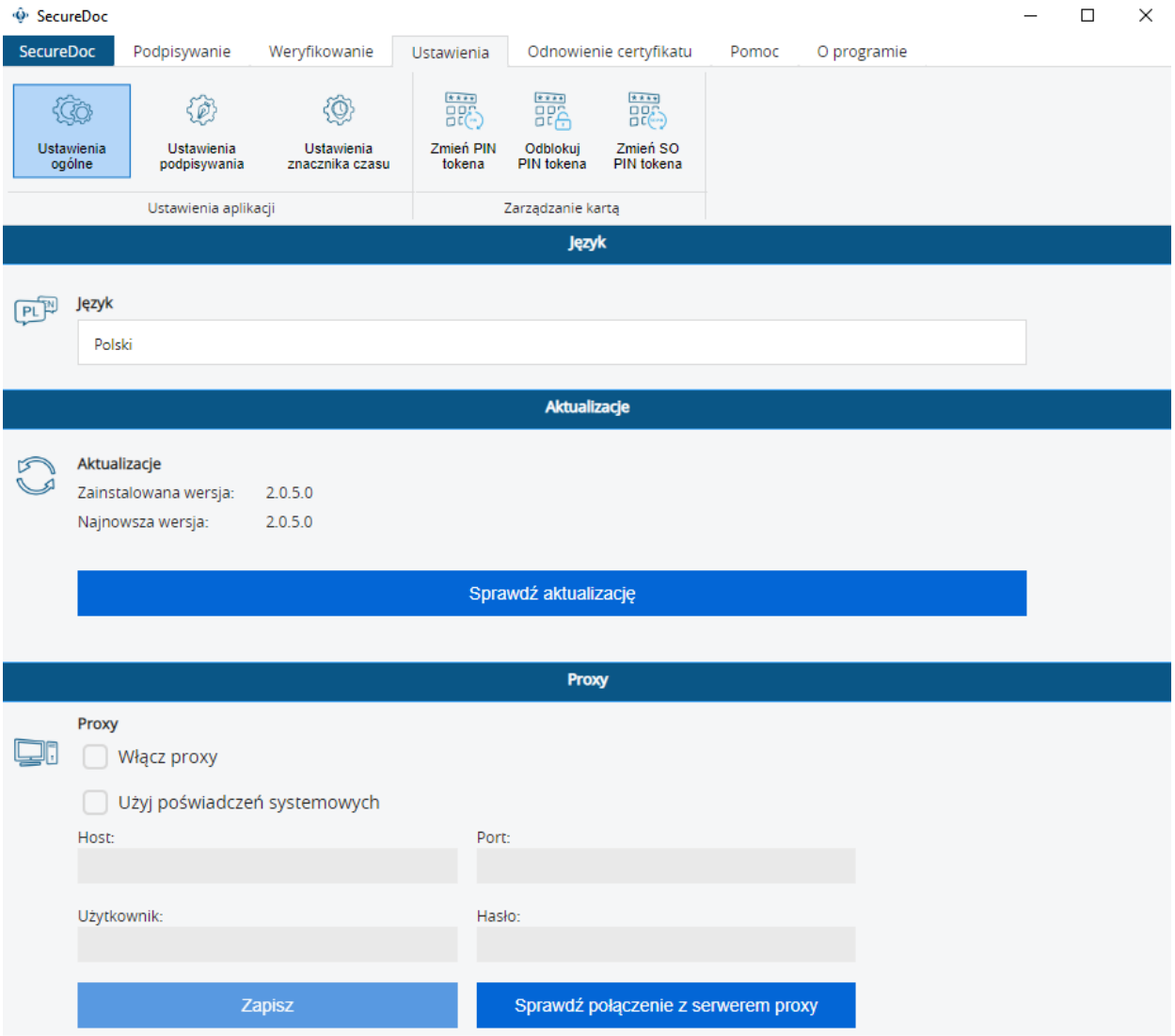
W celu wyświetlenia szczegółów dotyczących wykrytych podpisów klikamy na nazwę pliku, który nas interesuje, a następnie klikamy „Pokaż raport". Każda strona raportu jest poświęcona kolejnemu podpisowi. Strony można zmieniać strzałkami w menu po lewej stronie ekranu, już po wyświetleniu danego raportu.

6. Ustawienia

W tej zakładce znajdziemy wszelkie ustawienia dotyczące działania samej aplikacji SecureDoc oraz sposobu w jaki podpisujemy pliki. Dodatkowo znajdują się tu funkcje związane z kartą kryptograficzną. Wszystkie funkcje opisano poniżej.

6.1 Sekcja **Ustawienia aplikacji**

6.1.1 Ustawienia ogólne



6.1.1.1 Język

W celu zmiany języka w ustawieniach ogólnych, w sekcji **Język** należy wybrać jeden z dostępnych języków z listy. Aktualnie wspierany jest polski, angielski i niemiecki.

6.1.1.2 *Aktualizacje*

W momencie uruchomienia aplikacja SecureDoc 2.0 sprawdza dostępność aktualizacji. W przypadku wykrycia nieaktualnej wersji aplikacja wyświetli komunikat o dostępnej aktualizacji. Aby zainstalować nową wersję, należy zaakceptować wyświetlony komunikat i przejść do instalacji.

W sekcji **Aktualizacje** można sprawdzić numer zainstalowanej wersji i ręcznie wywołać aktualizację.

6.1.1.3 *Proxy*

W tej sekcji możliwe jest skonfigurowanie serwera proxy, który ma być wykorzystywany przez aplikację SecureDoc. Aby to wykonać, należy zaznaczyć opcję „Włącz proxy", podać wszystkie niezbędne informacje w dostępnych polach oraz kliknąć przycisk „Zapisz".

Alternatywnie można użyć poświadczeń systemowych. W tym celu należy zaznaczyć opcje „Włącz proxy" oraz „Użyj poświadczeń systemowych", a pola pozostawić puste.

Przed podpisywaniem plików, zalecamy przetestować połączenie za pomocą przycisku „Sprawdź połączenie z serwerem proxy".

6.1.2 Ustawienia podpisywania

6.1.2.1 *Domyślny format i parametry podpisu*

W tej sekcji możemy wybrać domyślny format, wariant i typ podpisu, funkcję skrótu oraz rodzaj zobowiązania. W ten sposób, nasze domyślne parametry będą automatycznie wybrane w zakładce **Podpisywanie** od razu po uruchomieniu aplikacji. Nowo wybrane domyślne ustawienia będą obowiązywać dopiero po zamknięciu i ponownym uruchomieniu aplikacji.

6.1.2.2 *Dodatkowe opcje podpisywania*

W tej sekcji mamy możliwość konfiguracji następujących opcji:

„Nadpisz dokument PDF, gdy tworzony jest podpis w formacie PAdES" - wyłączenie tej opcji spowoduje, że podpisywany plik PDF po podpisaniu będzie zapisany w osobnym pliku w tym samym folderze, co plik źródłowy, z dopiskiem „-sig" na końcu nazwy.

Przy włączonej opcji, podpisywany plik zostanie nadpisany, bez zmiany jego nazwy. Przy podpisywaniu nie tworzy się wtedy żaden nowy plik.

„Wykonuj podpis graficzny, gdy tworzony jest podpis w formacie PAdES" – opcja ta umożliwia dodanie reprezentacji graficznej podpisu na dokumencie PDF. W trakcie podpisywania można również pominąć ten krok.

Wyłączenie tej opcji pomija całkowicie etap wyświetlania podglądu pliku PDF w trakcie

podpisu, skracając cały proces.

„Nie koduj danych XML do Base64 w przypadku tworzenia podpisu w formacie XAdES w typie wewnętrznym” - wyłączenie tej opcji spowoduje zapisanie podpisywanego pliku XML jako zakodowanego w Base64. Włączenie tej opcji pozwoli na zapisywanie plików XML w standardowym kodowaniu UTF-8.

„Nadpisz dokument XML, gdy tworzony jest podpis w formacie XAdES w typie otoczonym” – Przy włączonej opcji format dokumentu (.XML) nie zmieni się przy podpisie.

Jeżeli potrzebujemy, aby plik XML po podpisaniu został zapisany w formacie .XAdES – należy wyłączyć daną opcję.

„Twórz podpis w formacie XAdES w typie otoczonym w wersji standardowej – Podpis złożony w tej konfiguracji uniemożliwia dodanie kolejnych podpisów na tym samym dokumencie.

6.1.3 Ustawienia znacznika czasu

Aby mieć możliwość korzystania ze znaczników czasu w programie SecureDoc, należy odpowiednio skonfigurować dostęp do serwera znacznika czasu. Po zakupie pakietu znaczników czasu i otrzymaniu od EuroCert niezbędnych danych konfiguracyjnych, należy uzupełnić wymagane pola, a następnie kliknąć przycisk „Zapisz”.

- Adres serwera znacznika czasu
- Użytkownik – spersonalizowany login
- Hasło – hasło do usługi znacznika czasu

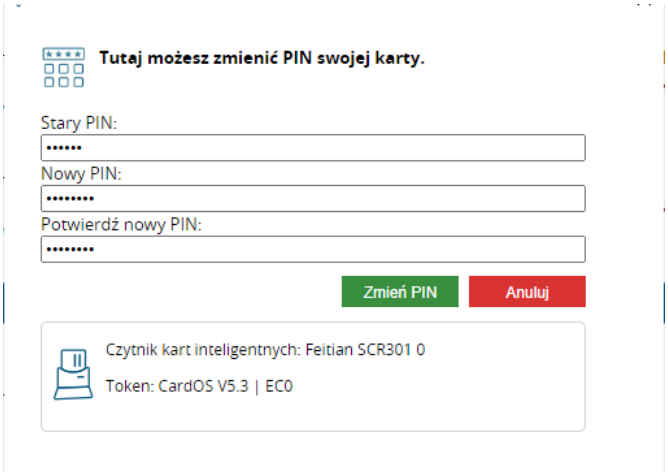
Adres serwera i nazwę użytkownika można sprawdzić na swoim koncie na stronie https://portal.eurocert.pl . Hasło do znacznika czasu użytkownik nadaje samodzielnie, również z poziomu swojego konta. Przed podpisywaniem dokumentów zaleca się przetestować konfigurację znaczników czasu, klikając na przycisk „Sprawdź konfigurację znacznika”.

6.2 Sekcja **Zarządzanie kartą**

Aplikacja umożliwia zarządzanie kodami PIN i SO PIN karty kryptograficznej wydanej przez EuroCert. Użytkownik może zmienić kod PIN oraz SO PIN, jeżeli nie są jeszcze zablokowane oraz odblokować kod PIN, jeżeli już doszło do jego zablokowania.

6.2.1 Zmiana PIN-u

W celu zmiany kodu PIN należy kliknąć „Zmień PIN tokena”, po czym pojawi się następujące okienko:



W polu „Stary PIN” należy wpisać obecnie używany PIN. W kolejnych dwóch polach należy wpisać nowy PIN, i kliknąć „Zmień PIN”. Jeżeli operacja się powiedzie, nowy PIN od tej pory będzie używany do autoryzacji.

6.2.2 Odblokowanie PIN-u

Trzykrotne wprowadzenie niepoprawnego PIN-u podczas składania podpisu elektronicznego lub próby zmiany PIN-u prowadzi do jego zablokowania. Przy zablokowanym kodzie PIN użytkownik nie jest w stanie podpisać żadnego dokumentu.

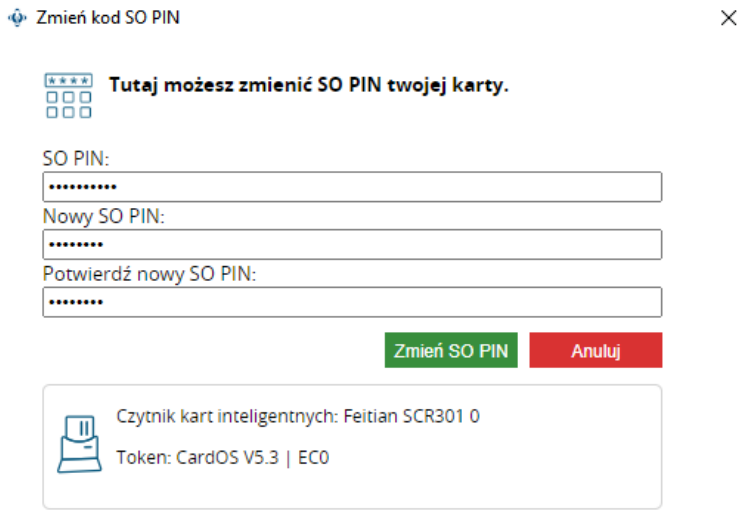
W celu odblokowania PIN-u należy kliknąć „Odblokuj PIN tokena”, po czym pojawi się następujące okienko:

Najpierw należy wprowadzić SO PIN, następnie dwukrotnie podać nowy PIN i kliknąć „Odblokuj PIN”.

UWAGA! Jeśli trzykrotnie wprowadzisz niepoprawny kod SO PIN, karta kryptograficzna zostanie nieodwracalnie zablokowana. W takiej sytuacji należy zakupić nowy certyfikat na nowej karcie.

6.2.3 Zmiana SO PIN

W celu zmiany kodu SO PIN należy kliknąć „Zmień SO PIN tokena", po czym pojawi się następujące okienko:



W polu „SO PIN" należy wpisać obecny SO PIN. W kolejnych dwóch polach należy wpisać nowy SO PIN.

Nowy SO PIN może składać się z dowolnych znaków liczb, liter (małych, dużych), symboli i innych znaków. Minimalna długość SO PIN-u to 4 znaki a maksymalna zależy od modelu karty kryptograficznej (najczęściej 8 lub 10 znaków).

Uwaga! Jeśli trzykrotnie wprowadzisz niepoprawny SO PIN, karta kryptograficzna zostanie nieodwracalnie zablokowana. W takiej sytuacji należy zakupić nowy certyfikat na nowej karcie.

Pozostałe informacje:

Podczas zmiany kodów PIN / SO PIN do komputera może być podłączona tylko jedna karta kryptograficzna. Podłączenie większej ilości może skutkować zablokowaniem niektórych z nich. EuroCert nie ponosi odpowiedzialności za skutki związane z nieprzestrzeganiem danego zalecenia.

7. Odnowienie certyfikatu

Zakup produktu

Produkt **Odnowienie podpisu elektronicznego na karcie EuroCert** można zakupić w sklepie internetowym TUTAJ lub kontaktując się z naszym działem handlowym: handlowy@eurocert.pl

Odnowienie certyfikatu

Sugerujemy rozpocząć procedurę na min. 7 dni przed wygaśnięciem aktualnego certyfikatu. Jeżeli rozpoczniesz procedurę później niż 72h przed wygaśnięciem certyfikatu, nie gwarantujemy pozytywnego ukończenia procesu odnowienia.

Aby rozpocząć procedurę odnowienia (już po zakupie produktu i otrzymaniu kodu odnowienia), należy przejść do programu SecureDoc do zakładki **Odnowienie certyfikatu** i kliknąć przycisk „Odnowienie certyfikatu". Po wprowadzeniu kodu odnowienia należy wypełnić wniosek i podpisać wygenerowaną umowę aktualnym podpisem kwalifikowanym.

Uwaga: Sam zakup produktu nie jest równoważny z przedłużeniem ważności podpisu kwalifikowanego. Nowy certyfikat zostanie wygenerowany dopiero w momencie zakończenia procedury opisanej w instrukcji dostarczonej wraz z kodem odnowienia.

8. Pomoc

Zakładka **Pomoc** poza przyciskiem do pobrania aktualnej wersji instrukcji do SecureDoc zawiera dane kontaktowe do działu wsparcia technicznego oraz umożliwia pobranie aplikacji **AnyDesk** do połączeń zdalnych.

9. O programie

Zakładka zawiera warunki licencji.