Instrukcja obsługi

SECUREDOC v 2.0

Wersja 1.3

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

SecureDoc v2.0 to aplikacja przeznaczona do składania i weryfikacji podpisów elektronicznych z możliwością wystawienia podpisu wraz ze znacznikiem czasu.

W programie SecureDoc v2.0 podpis elektroniczny może zostać złożony przy użyciu certyfikatów wydanych przez: EuroCert, CenCert (Enigma), KIR, PWPW oraz Certum (Asseco).

Formaty, w których można złożyć podpis za pomocą programu SecureDoc: PAdES-BES, PAdES-T, XAdES-BES, XAdES-T typami wewnętrznym, zewnętrznym lub otoczonym.

Wykorzystywany zestaw kryptograficznych funkcji skrótu: SHA-256.

2. Minimalne wymagania systemowe

- System operacyjny MacOS High Sierra i nowsze
- Połączenie internetowe (niezbędne przy korzystaniu z funkcji weryfikacji oraz przy korzystaniu z podpisu chmurowego ECSigner)

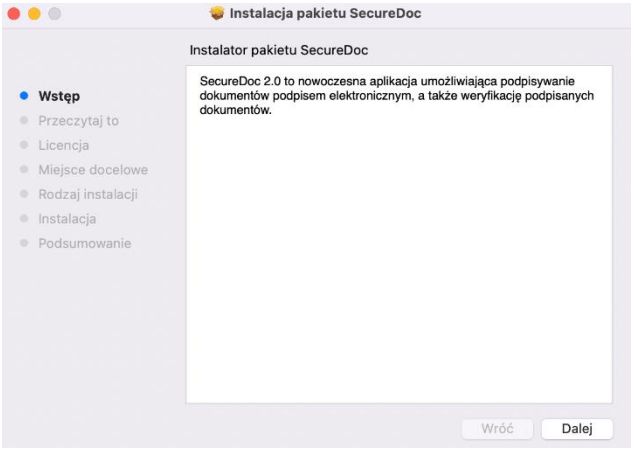
Aby korzystać z podpisu elektronicznego w aplikacji SecureDoc, wymagane są:

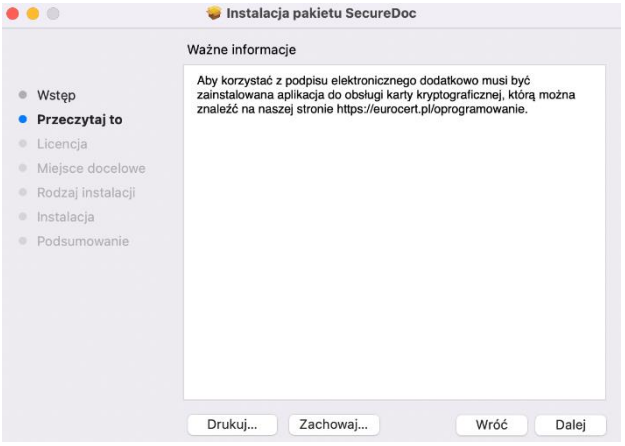
- Oprogramowanie do zarządzania kartą - Charismathics Smart Security Interface – w przypadku podpisu na karcie
- Aplikacja ECSigner – w przypadku podpisu chmurowego ECSigner

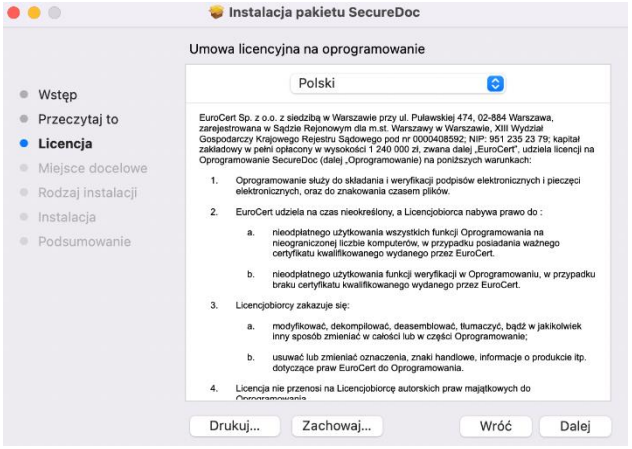
3. Instalacja aplikacji

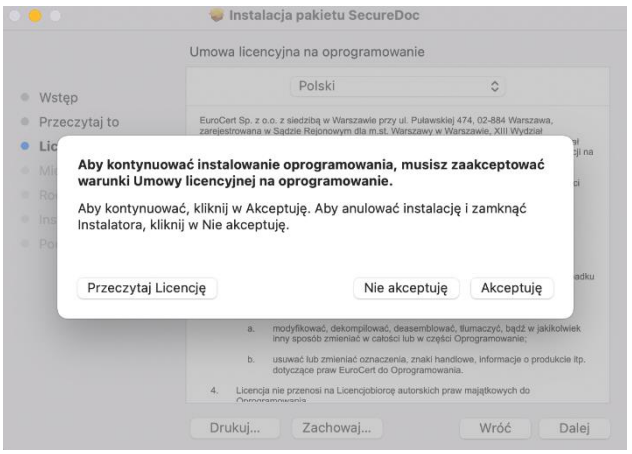
W celu rozpoczęcia instalacji aplikacji wejdź na stronę eurocert.pl/oprogramowanie i pobierz „*SecureDoc 2 - aplikacja do składania i weryfikacji podpisu kwalifikowanego*”.

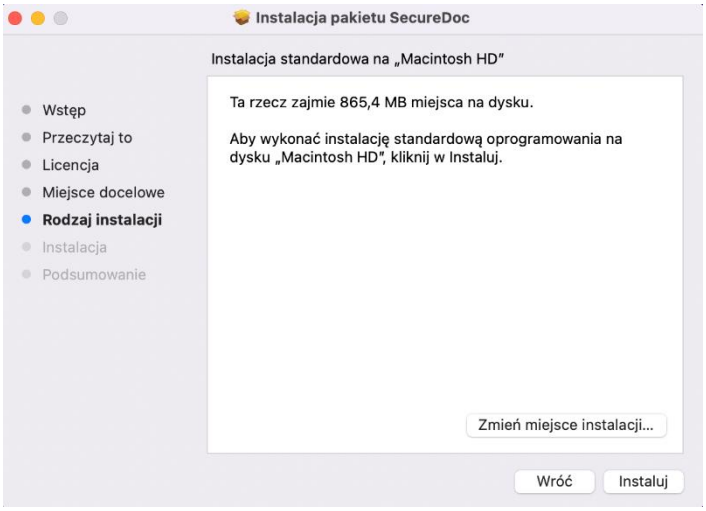
Po uruchomieniu pobranego instalatora podążaj zgodnie z poniższymi oknami dialogowymi:

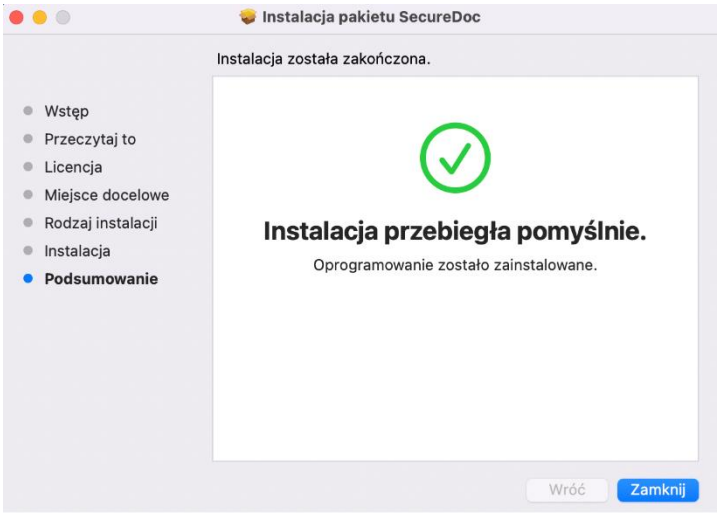



Instalacja pakietu SecureDoc
Ważne informacje
Wstęp
Przeczytaj to
Licencja
Miejsce docelowe
Rodzaj instalacji
Instalacja
Podsumowanie
Aby korzystać z podpisu elektronicznego dodatkowo musi być zainstalowana aplikacja do obsługi karty kryptograficznej, którą można znaleźć na naszej stronie https://eurocert.pl/oprogramowanie.
Drukuj...
Zachowaj...
Wróć
Dalej


Instalacja pakietu SecureDoc
Umowa licencyjna na oprogramowanie
Polski
Wstęp
Przeczytaj to
Licencja
Miejsce docelowe
Rodzaj instalacji
Instalacja
Podsumowanie
EuroCert Sp. z o.o. z siedzibą w Warszawie przy ul. Puławskiej 474, 02-884 Warszawa, zarejestrowana w Sądzie Rejonowym dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr 0000408592; NIP: 951 235 23 79; kapitał zakładowy w pełni opłacony w wysokości 1 240 000 zł, zwana dalej „EuroCert", udziela licencji na Oprogramowanie SecureDoc (dalej „Oprogramowanie) na poniższych warunkach:
1. Oprogramowanie służy do składania i weryfikacji podpisów elektronicznych i pieczęci elektronicznych, oraz do znakowania czasem plików.
2. EuroCert udziela na czas nieokreślony, a Licencjobiorca nabywa prawo do :
a. nieodpłatnego użytkowania wszystkich funkcji Oprogramowania na nieograniczonej liczbie komputerów, w przypadku posiadania ważnego certyfikatu kwalifikowanego wydanego przez EuroCert.
b. nieodpłatnego użytkowania funkcji weryfikacji w Oprogramowaniu, w przypadku braku certyfikatu kwalifikowanego wydanego przez EuroCert.
3. Licencjobiorcy zakazuje się:
a. modyfikować, dekompilować, deasemblować, tłumaczyć, bądź w jakikolwiek inny sposób zmieniać w całości lub w części Oprogramowanie;
b. usuwać lub zmieniać oznaczenia, znaki handlowe, informacje o produkcie itp. dotyczące praw EuroCert do Oprogramowania.
4. Licencja nie przenosi na Licencjobiorcę autorskich praw majątkowych do
Drukuj...
Zachowaj...
Wróć
Dalej


Instalacja pakietu SecureDoc
Umowa licencyjna na oprogramowanie
Polski
Wstęp
Przeczytaj to
Aby kontynuować instalowanie oprogramowania, musisz zaakceptować warunki Umowy licencyjnej na oprogramowanie.
Aby kontynuować, kliknij w Akceptuję. Aby anulować instalację i zamknąć Instalatora, kliknij w Nie akceptuję.
Przeczytaj Licencję
Nie akceptuję
Akceptuję
Drukuj...
Zachowaj...
Wróć
Dalej





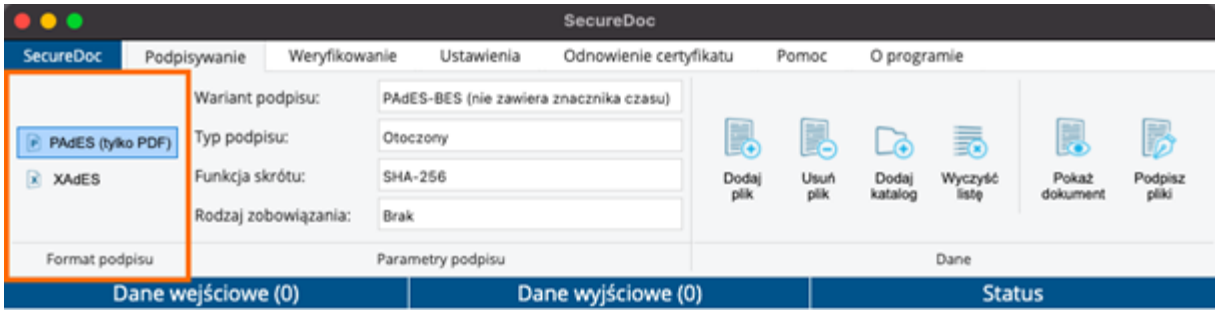
Po zakończeniu tego etapu aplikacja jest gotowa do użytku.

4. Podpisywanie

Zakładka „Podpisywanie" jest wyznaczona do wystawienia podpisów elektronicznych.

W sekcji „Format podpisu" dostępne są dwa formaty podpisu elektronicznego:

- PAdES
- XAdES

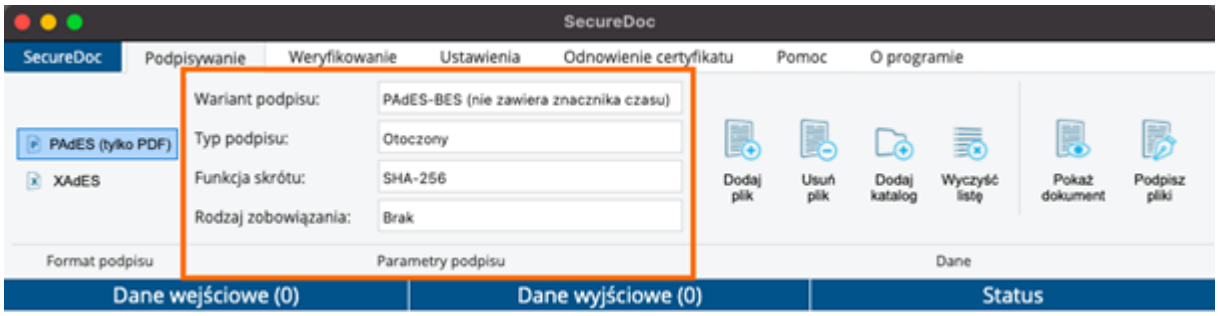


Format PAdES jest dedykowany i wyłączny dla plików PDF.

Formatem XAdES mogą zostać podpisane wszystkie formaty plików (.xml, .docx, .jpeg, .odt itd.). Formatem XAdES można także złożyć podpis pod dokumentem PDF. Zalecamy jednak korzystanie z dedykowanego formatu PAdES.

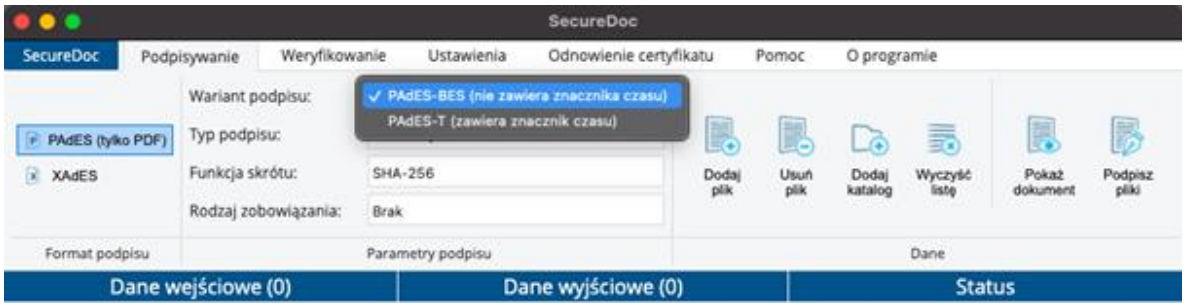
4.1 Sekcja „Parametry podpisu”

Sekcja „Parametry podpisu” zawiera główne ustawienia dla wykonywanego podpisu.



4.1.1 Wariant podpisu

W zależności od wybranego formatu podpisu możliwe 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.

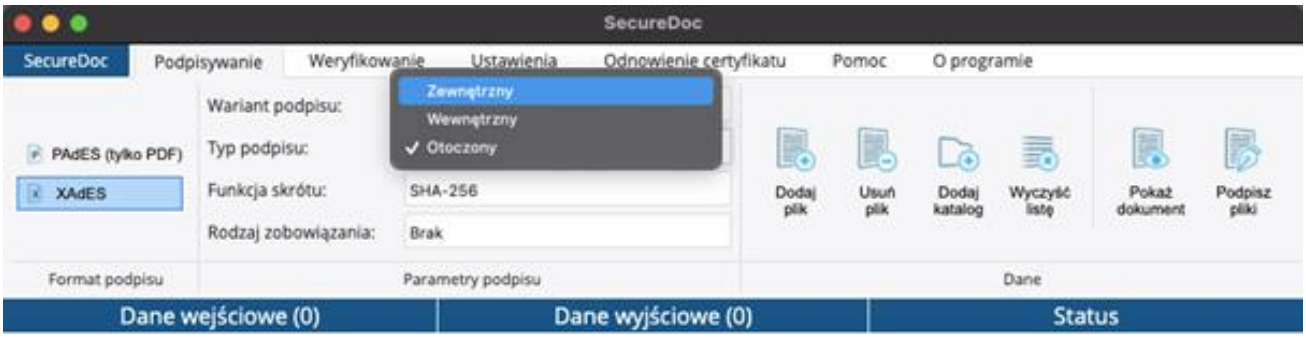
Wariant -T oznacza, że podpis zostanie złożony ze znacznikiem czasu. Usługa kwalifikowanego znakowania czasem („znacznik czasu" wspomniany wyżej) jest usługą dodatkową i umożliwia dokładne określenie daty i czasu czynności realizowanych w środowisku elektronicznym.

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 odnośnie czasu.

4.1.2 Typ podpisu



4.1.2.1 Zewnętrzny

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.

Podpisem zewnętrznym podpisywać można dowolne pliki (o dowolnym formacie) i wielkości.

Po złożeniu podpisu zewnętrznego, plik podpisywany nie może zostać zmieniony w jakikolwiek sposób (nie może być zmieniana treść dokumentu ani nazwa dokumentu podpisanego), ponieważ spowoduje to naruszenie integralności danych i podpis nie będzie mógł zostać zweryfikowany poprawnie.

Należy pamiętać, że podczas weryfikacji 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).

4.1.2.2 *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 jak i poświadczenie złożenia podpisu (2w1). Warto pamiętać że plik podpisany typem wewnętrznym będzie zapisany w formacie XAdES.

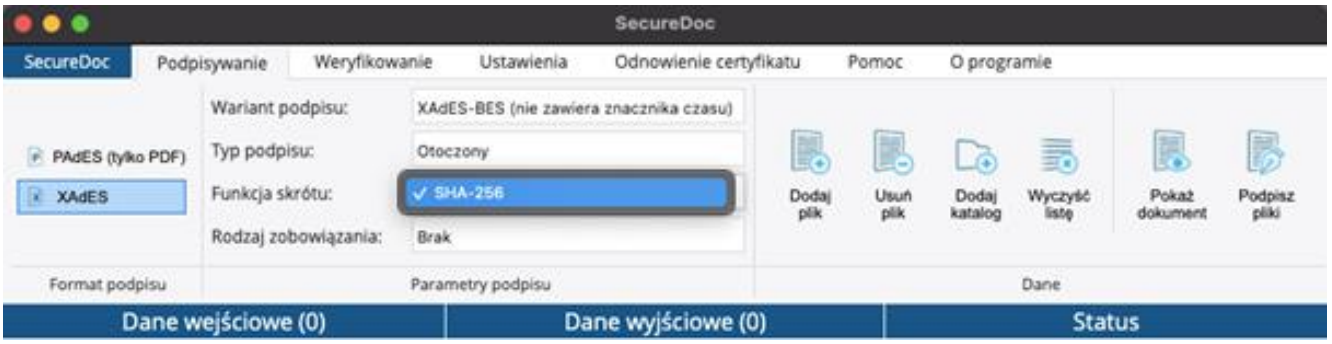
Jeżeli np. podpisujemy plik *dokument.txt*, to plik podpisany podpisem wewnętrznym będzie wyglądał następująco: *dokument.txt.XAdES* .

4.1.2.3 *Otoczony*

Dany typ podpisu jest odpowiednikiem typu wewnętrznego i stosuje się go do plików XML. Plik podpisu będzie zawierał zarówno treść dokumentu jak i poświadczenie złożenia podpisu (2w1).

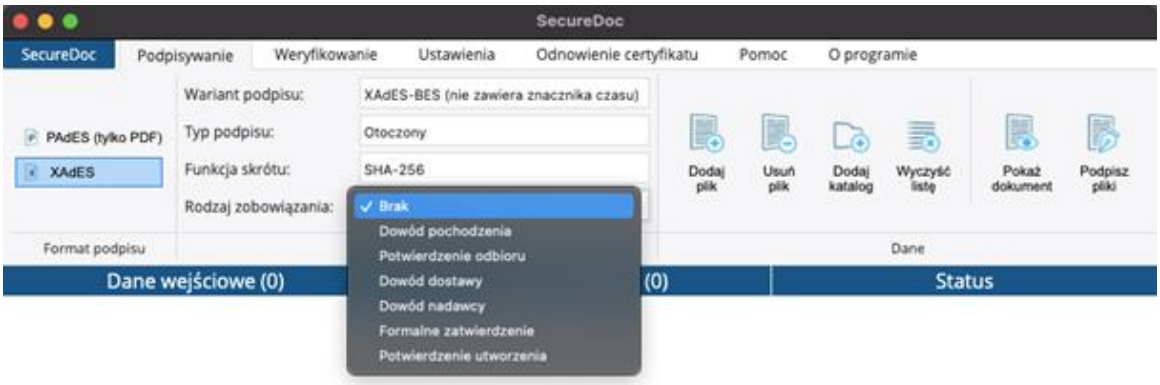
Jeżeli chcemy podpisać plik XML tak, aby zawierał on podpis oraz treść dokumentu, należy wybrać typ podpisu „otoczony”. Format XAdES, typ podpisu „otoczony” dotyczy jedynie plików w formacie XML.

4.1.3 Funkcja skrótu



SHA-256 jest typem zabezpieczenia kryptograficznego. Większa wartość skrótu zapewnia większe bezpieczeństwo.

4.1.4 Rodzaj zobowiązania

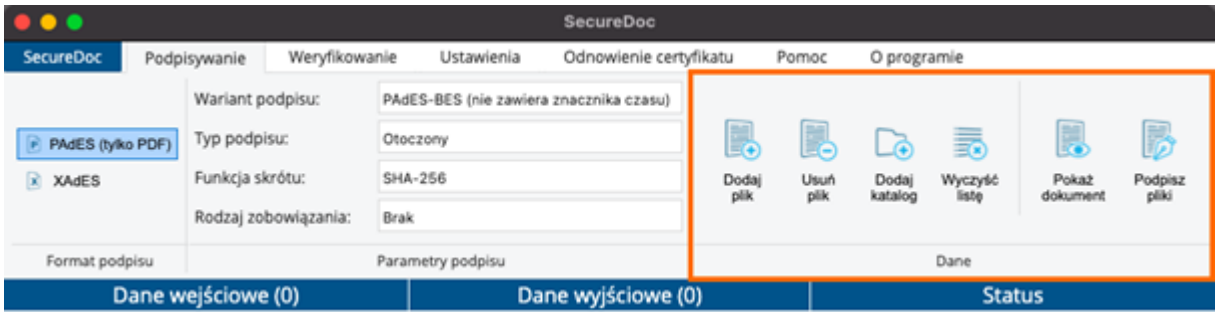


Dane pole jest opcjonalne i zawiera w sobie informacje dodatkowe odnośnie powodu lub celu złożenia podpisu.

Do wyboru dostępnych jest 6 rodzajów zobowiązań:

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

4.2 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 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 wybrany, czyli podświetlony plik), lub „Wyczyść listę” – aby usunąć wszystkie pliki z listy.

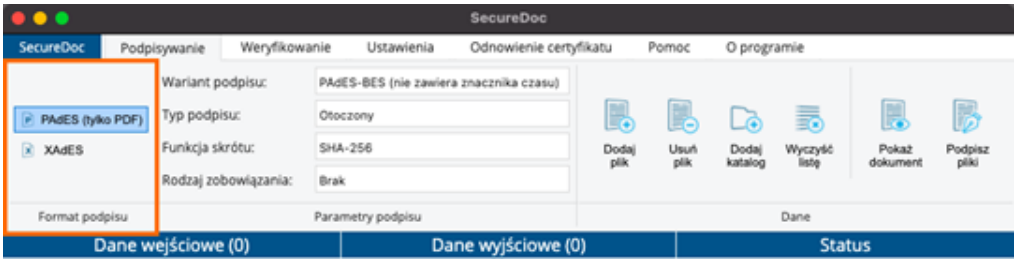
Wciśnięcie przycisku „Pokaż dokument” spowoduje wyświetlenie treści wybranego dokumentu w nowym oknie.

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

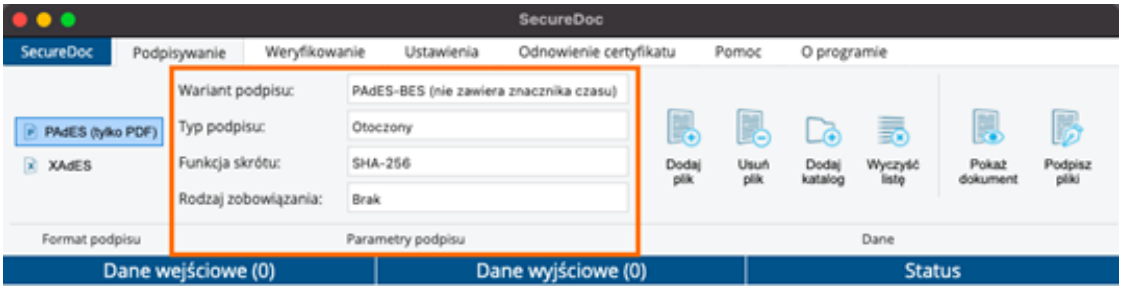
4.3 Proces złożenia podpisu elektronicznego

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. Określamy rodzaj podpisu jakim chcemy podpisać dokument (sekcja „Format podpisu”)



2. Wybieramy żądane opcje podpisu w sekcji „Parametry podpisu"

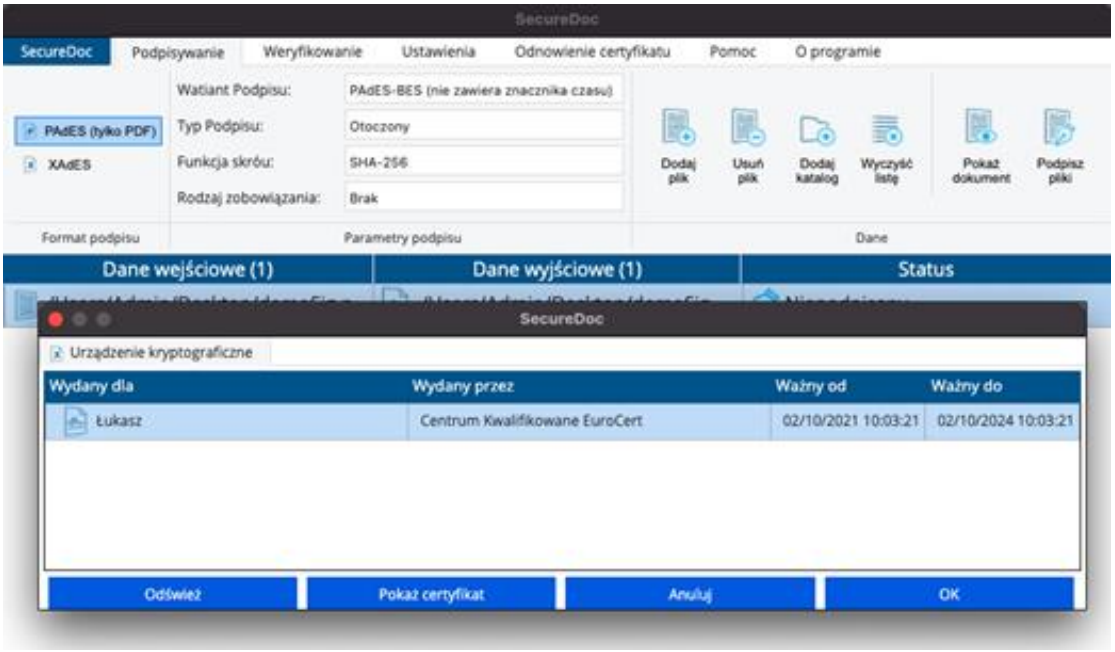


3. Dodajemy pliki, które chcemy podpisać za pomocą przycisku „Dodaj plik” lub przeciągając je z folderu do okna aplikacji SecureDoc (drag&drop).

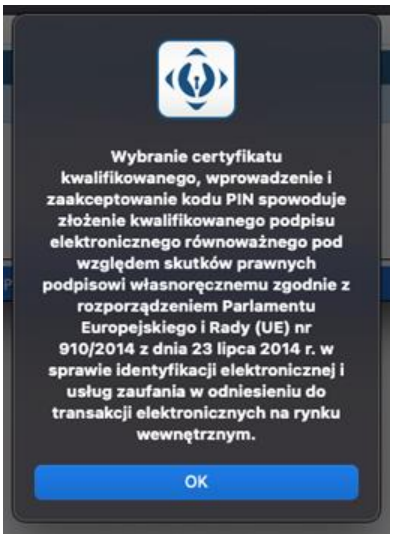
4. Klikamy „Podpisz pliki”. Warto zwrócić uwagę na to, że wszystkie dokumenty z listy wybranych do podpisania zostaną podpisane z takimi samymi ustawieniami parametrów podpisu.

5. Po wciśnięciu „Podpisz pliki” pojawi się okno wyboru certyfikatu. Z listy wybieramy

certyfikat z użyciem którego chcemy podpisać wybrane pliki i klikamy „OK”. W danej zakładce dostępne są certyfikaty, które znajdują się na aktualnie podłączonym urządzeniu oraz certyfikaty podpisu chmurowego ECSigner.

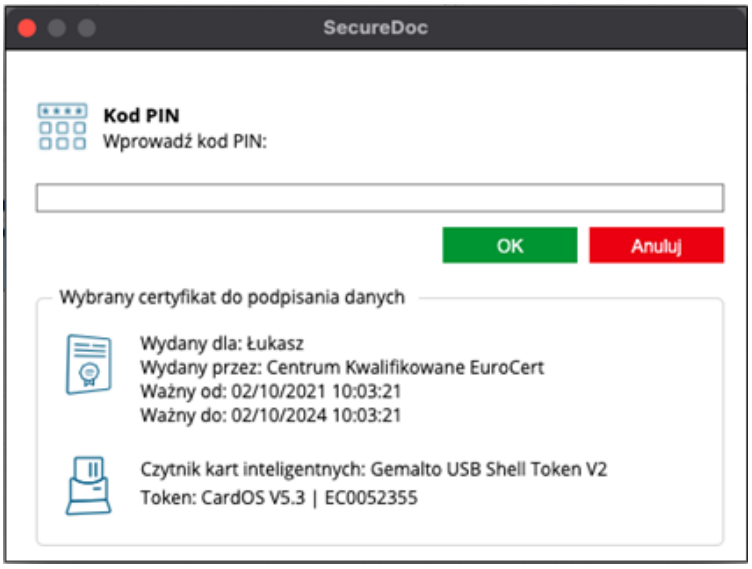


6. Po wybraniu certyfikatu i kliknięciu „OK” pojawi się komunikat informacyjny odnośnie składanego podpisu. Po zapoznaniu się z komunikatem klikamy „OK”.

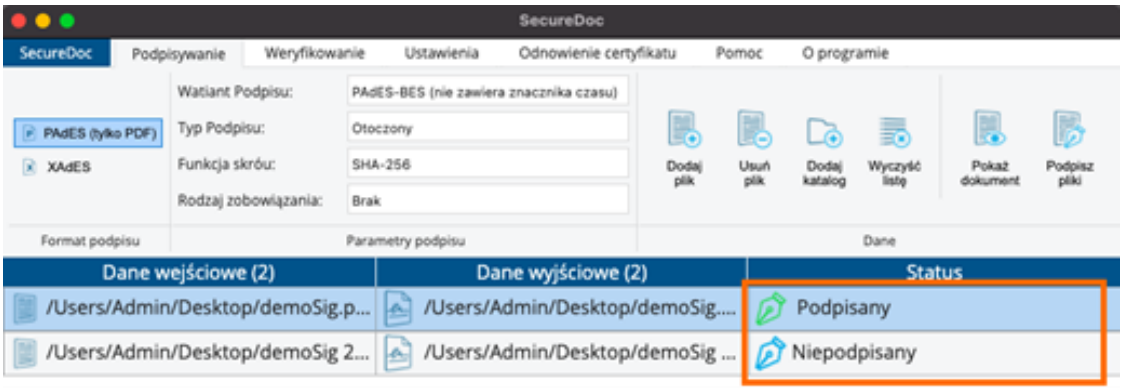


7. Przy podpisie karcianym wprowadzamy kod PIN i klikamy „OK”. Jeśli wpisany kod PIN jest prawidłowy, dojdzie do złożenia podpisu.

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



8. Sprawdzamy status dokumentu. Jeśli dokument został prawidłowo podpisany, w oknie statusu przy podpisanych plikach pojawi się status „Podpisany”, jeśli wystąpił błąd pojawi się status „Niepodpisany”.



4.4 Podpisywanie pliku PDF z reprezentacją graficzną

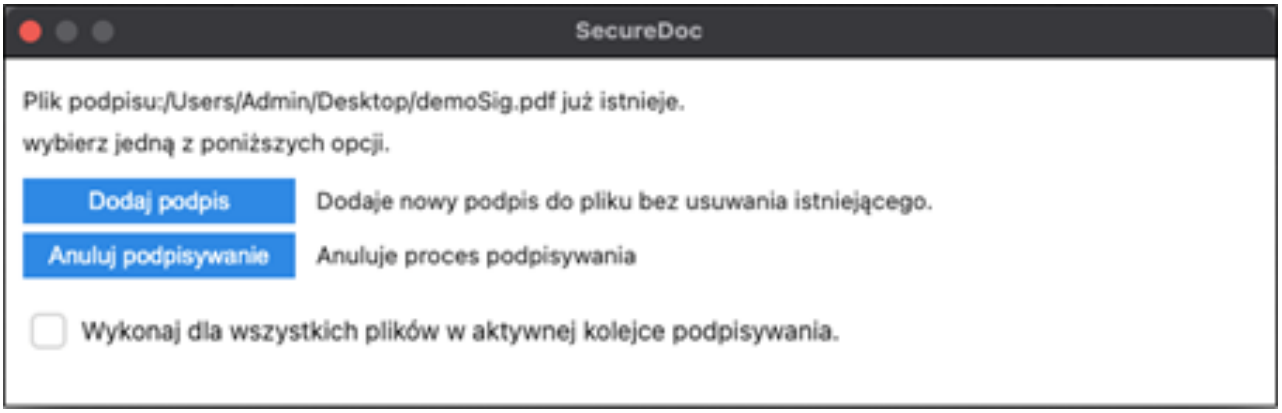
Przy zaznaczonej opcji „Wykonuj podpis graficzny, gdy tworzony jest podpis w formacie PAdES” w zakładce „Ustawienia”->”Ustawienia podpisywania”, proces podpisywania zawiera dodatkowe okno, z wyświetloną treścią dokumentu PDF, który podpisujemy. Należy kliknąć na ikonę pieczątki, a następnie wskazać konkretne miejsce w dokumencie, klikając lewym przyciskiem myszy.

Po kliknięciu przycisku „Podpisz” podpis zostanie złożony, a w zaznaczonym miejscu dodana zostanie graficzna reprezentacja podpisu. W danym procesie podpisywania, na dokumencie możliwe jest dodanie tylko jednego znaku graficznego.

W przypadku podpisywania większej ilości plików, można na pierwszym z nich umieścić znak graficzny, zaznaczając opcję „Zastosuj dla wszystkich plików w kolejce”, a następnie kliknąć „Podpisz”. W ten sposób każdy z dokumentów zostanie podpisany, ze znakiem graficznym w tym samym miejscu.

4.5 Dodawanie kolejnych podpisów do pliku

Jeżeli plik zawiera przynajmniej jeden podpis elektroniczny, przy próbie podpisania go wyświetli się poniższe okno. W celu złożenia kolejnego podpisu na dokumencie, wybieramy opcję „Dodaj podpis”.



5. Weryfikowanie

W danej zakładce mamy możliwość weryfikacji podpisanych plików oraz wyświetlenia raportu dla zweryfikowanych podpisów elektronicznych.

Działanie przycisków „Dodaj plik", „Usuń plik", „Dodaj katalog", „Wyczyść listę" oraz „Pokaż dokument" jest analogiczne do przycisków z zakładki „Podpisywanie".

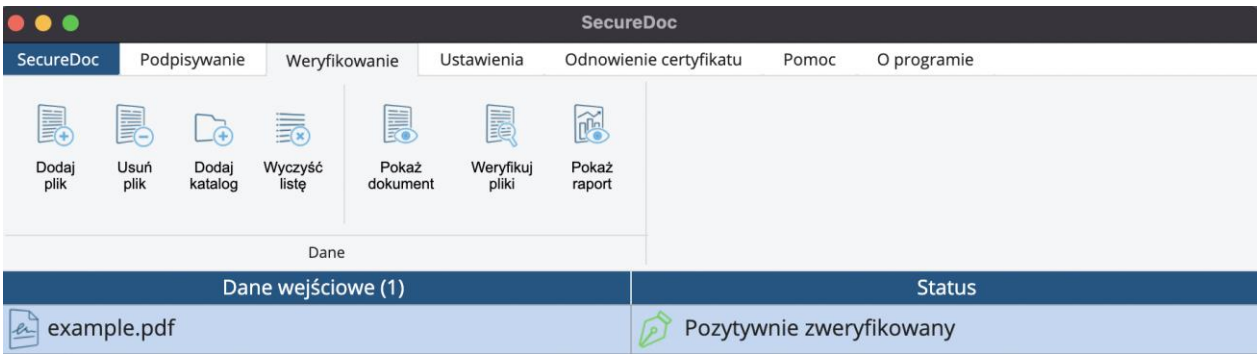
W zakładce „Weryfikowanie" do listy jednocześnie mogą zostać dodane pliki, które podpisano różnymi formatami/typami podpisu. Jeśli plik jest podpisany podpisem w formacie zewnętrznym, należy dodać do listy jedynie plik podpisu. Dodatkowo należy pamiętać aby zarówno plik podpisu jak i plik podpisywany znajdował się w tym samym miejscu/folderze. W innym przypadku aplikacja nie będzie mogła odwołać się do pliku źródłowego (podpisanego zewnętrznie). W sytuacji podpisu wewnętrznego wystarczy wskazać plik podpisany.

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. Oczekujemy na komunikat o statusie weryfikacji.



W zależności od wyniku weryfikacji możemy otrzymać status: „Poprawnie zweryfikowany” lub „Negatywnie zweryfikowany”.

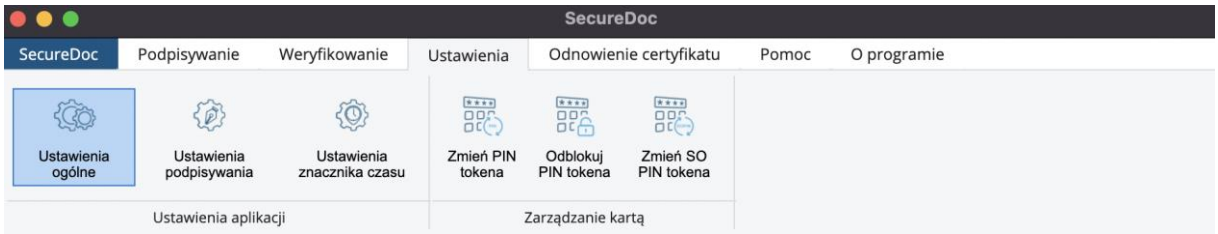
W celu otrzymania dokładniejszych informacji na temat wyniku weryfikacji, należy kliknąć „Pokaż raport”.

Możemy także wyświetlić podpisany dokument z listy klikając „Pokaż dokument”.

6. Ustawienia

6.1 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.

6.1.1.2 *Aktualizacje*

W momencie uruchomienia aplikacja SecureDoc 2.0 sprawdza dostępność aktualizacji i w sytuacji gdy używamy wersji starszej, aplikacja wyświetli komunikat o dostępnej aktualizacji. Aby zainstalować nową wersję, należy zaakceptować wyświetlony komunikat i przejść do instalacji.

W sekcji „Aktualizacje" jest dostępna informacja odnośnie zainstalowanej wersji aplikacji.

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, zaleca się przetestować połączenie, klikając na przycisk „Sprawdź połączenie z serwerem proxy".

6.1.2 Ustawienia podpisywania

W zakładce „Ustawienia podpisywania" można dostosować ustawienia domyślne podpisu, które będą automatycznie wybrane przy każdym uruchomieniu aplikacji. Nowo określone ustawienia formatu podpisu będą obowiązywać od momentu ponownego uruchomienia aplikacji.

Dostępne są następujące opcje ustawień domyślnych aplikacji (Każda z dostępnych opcji jest krótko wytłumaczona w SecureDoc v2.0):

- Domyślny format podpisu
- Domyślny wariant podpisu:
- Domyślny typ podpisu:
- Domyślna funkcja skrótu
- Domyślny rodzaj zobowiązania

6.1.2.1 *Dodatkowe opcje podpisywania*

W danej sekcji mamy możliwość konfiguracji następujących opcji:

„Nadpisz dokument PDF, gdy tworzony jest podpis w formacie PAdES" - odznaczenie 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.

Przy zaznaczonej opcji, podpisywany plik zostanie nadpisany, bez zmiany jego nazwy. Przy podpisywaniu nie tworzy się 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.

Odznaczenie tej opcji uniemożliwia dodanie reprezentacji graficznej podpisu na dokumencie PDF, skracając proces podpisywania.

„Nie koduj danych XML do Base64 w przypadku tworzenia podpisu w formacie XAdES w typie wewnętrznym - odznaczenie tej opcji spowoduje zapisanie podpisywanego pliku XML jako zakodowanego w Base64. Zaznaczenie 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 zaznaczonej opcji format dokumentu (.XML) nie zmieni się przy podpisie.

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

„Twórz podpis w formacie XAdES w typie otoczonym w wersji standardowej" – Podpis złożony w danej 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 znaczników czasu. Po otrzymaniu od EuroCert niezbędnych danych konfiguracyjnych, należy uzupełnić wymagane pola, a następnie kliknąć przycisk „Zapisz".

- Adres serwera znacznika czasu – spersonalizowany link dostępowy do serwera znaczników czasu
- Użytkownik – spersonalizowany login
- Hasło – spersonalizowane hasło (bez możliwości zmiany)

Użytkownik otrzymuje przedstawione dane konfiguracyjne po zakupie dodatkowej usługi znakowania czasem.

Przed podpisywaniem dokumentów zaleca się przetestować konfigurację znaczników czasu, klikając na przycisk „Sprawdź konfigurację znacznika".

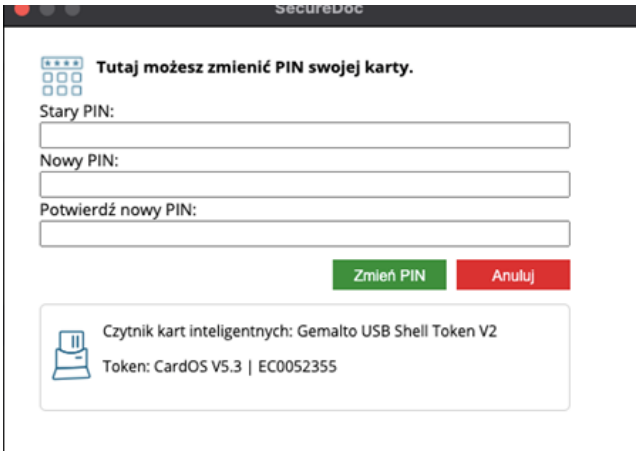
6.2 Zarządzanie kartą inteligentną

Uwaga! Trzykrotne wprowadzenie niepoprawnego kodu PIN skutkuje jego zablokowaniem.

W celu odblokowania kodu PIN, należy postępować zgodnie z zaleceniami punktu „Odblokowanie PIN-u".

6.2.1 Zmiana PIN-u

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



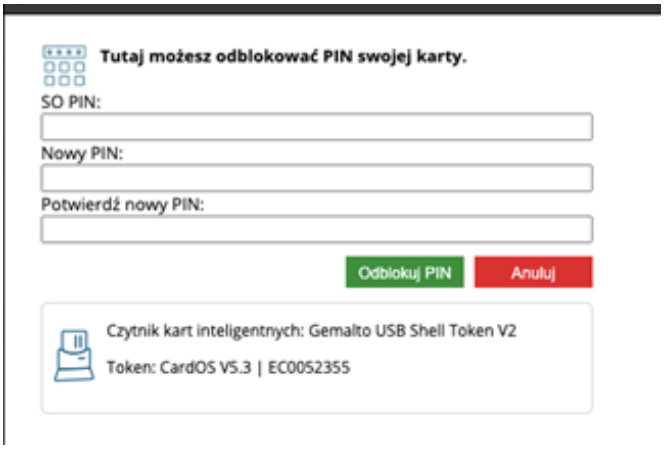
W polu „Stary PIN" należy wpisać obecny PIN. W kolejnych dwóch polach należy wpisać nowy PIN.

Minimalna długość PIN-u to 4 znaki a maksymalna 8 lub 10 znaków. Nowy PIN może składać się z dowolnych znaków: liczb, liter (małych, dużych), symboli oraz innych znaków.

6.2.2 Odblokowanie PIN-u

Trzykrotne wprowadzenie niepoprawnego PIN-u podczas składania podpisu elektronicznego lub próby zmiany PIN-u prowadzi do jego zablokowania.

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

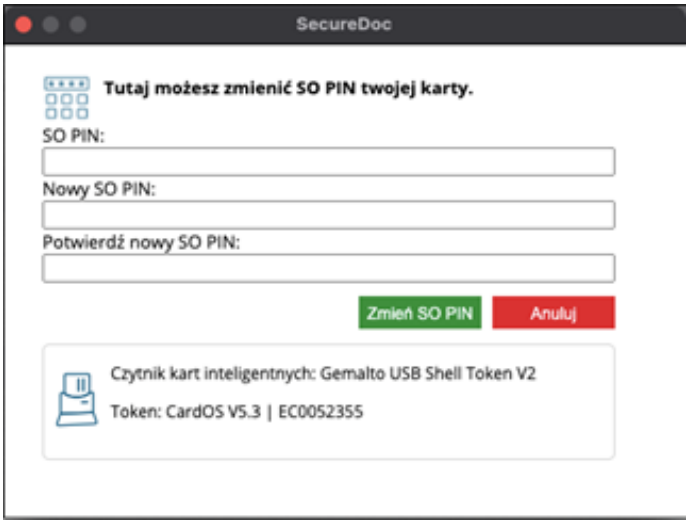


Najpierw należy wprowadzić SO PIN, a następnie dwukrotnie podać nowy PIN.

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 SOPIN 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

Kup odnowienie

Odnowienie online dla obecnych klientów można zakupić w sklepie internetowym EuroCert klikając na ten przycisk: sklep.eurocert.pl

Odnowienie certyfikatu

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

Po zakupie kodu odnawiającego należy przejść do programu SecureDoc do zakładki „Odnowienie certyfikatu” i kliknąć przycisk „Odnowienie certyfikatu”.

Pojawi się okno dla wprowadzenia kodu odnowienia. Następnie należy wypełnić wniosek i podpisać wygenerowaną umowę aktualnym podpisem kwalifikowanym.

Warto pamiętać, iż zakup produktu nie jest równoważny z przedłużeniem ważności podpisu kwalifikowanego. Ważność podpisu zostanie przedłużona dopiero w momencie zakończenia procedury przedstawionej w instrukcji.

Po otrzymaniu informacji o akceptacji wniosku przez EuroCert, należy wprowadzić ponownie kod odnowienia w aplikacji SecureDoc, co spowoduje aktywację odnowionego certyfikatu.

8. Pomoc

Dana zakładka zawiera dane kontaktowe do działu wsparcia technicznego oraz umożliwia pobranie aplikacji AnyDesk do połączeń zdalnych.

9. O programie

Zakładka zawiera treść licencji.