Instrukcja obsługi

SECUREDOC v 2.0

Wersja 1.2

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 lub zewnętrznym.

Wykorzystywany zestaw kryptograficznych funkcji skrótu: SHA-256

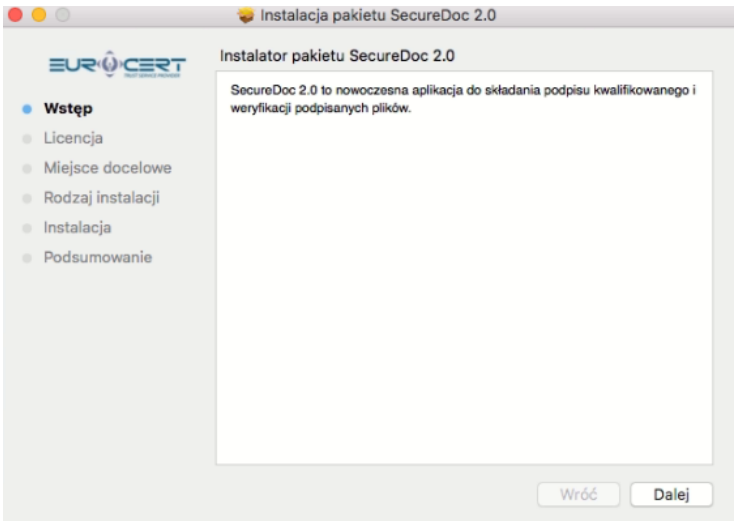
2. Minimalne wymagania systemowe

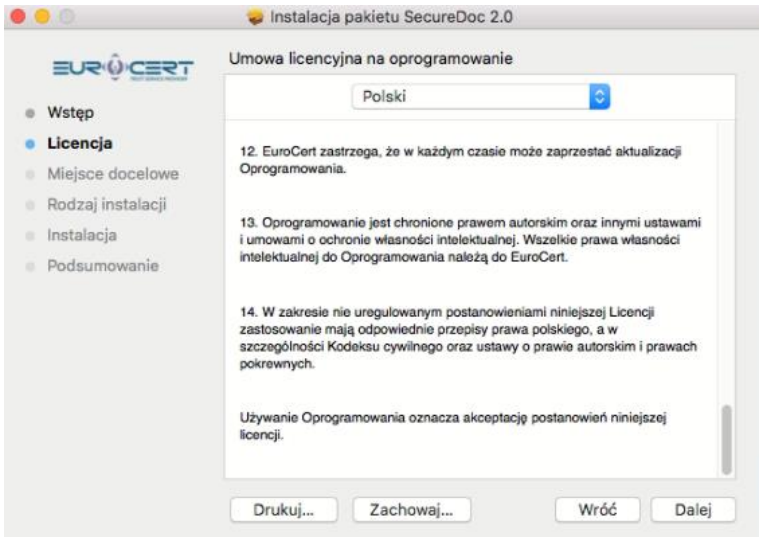
- system operacyjny Mac OS High Sierra i nowsze,
- oprogramowanie do zarządzania kartą - Charismathics Smart Security Interface,
- połączenie internetowe (niezbędne przy korzystania z funkcji weryfikacji).

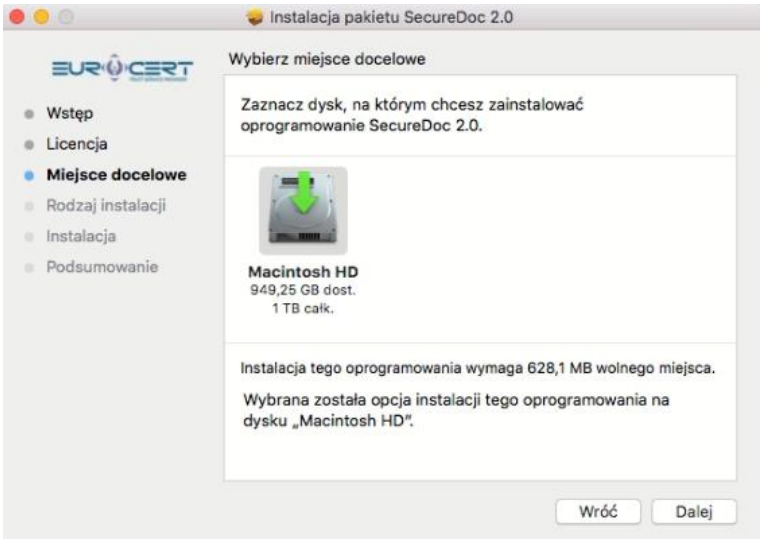
3. Instalacja aplikacji

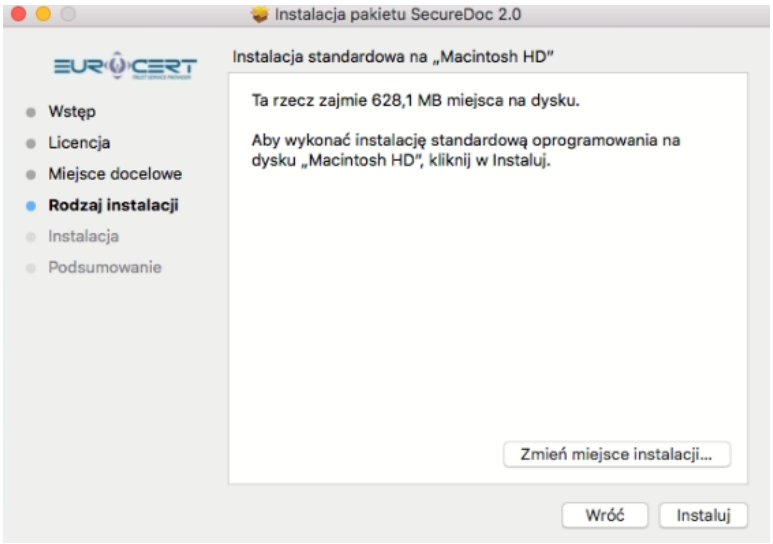
W celu rozpoczęcia instalacji aplikacji wejdź na stronę https://eurocert.pl/index.php/oprogramowanie i pobierz „*SecureDoc 2 - aplikacja do składania i weryfikacji podpisu kwalifikowanego*".

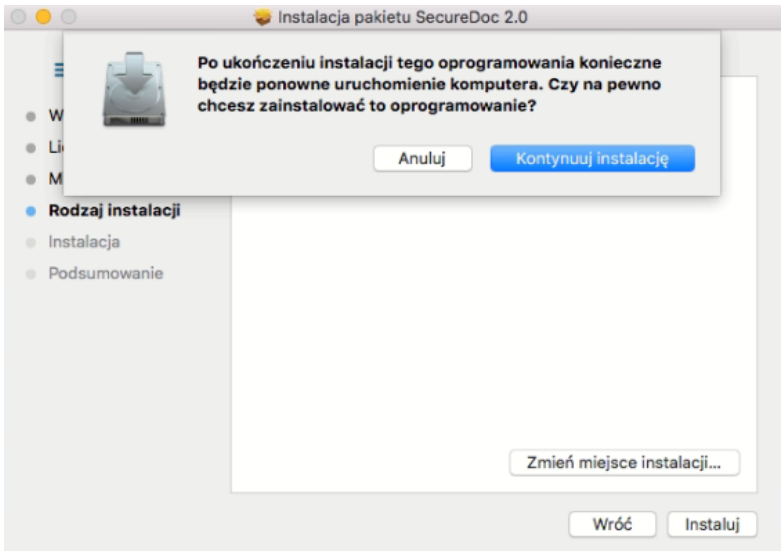
Po uruchomieniu pobranego instalatora podążaj zgodnie z poniższymi oknami dialogowymi:

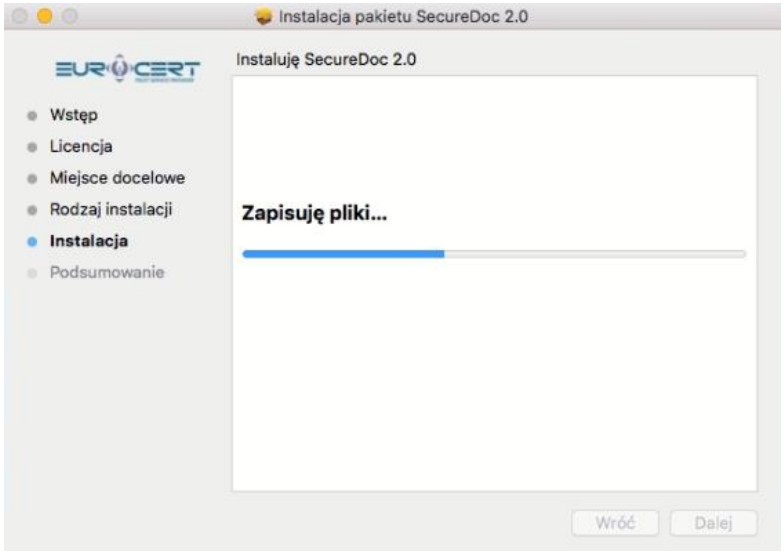


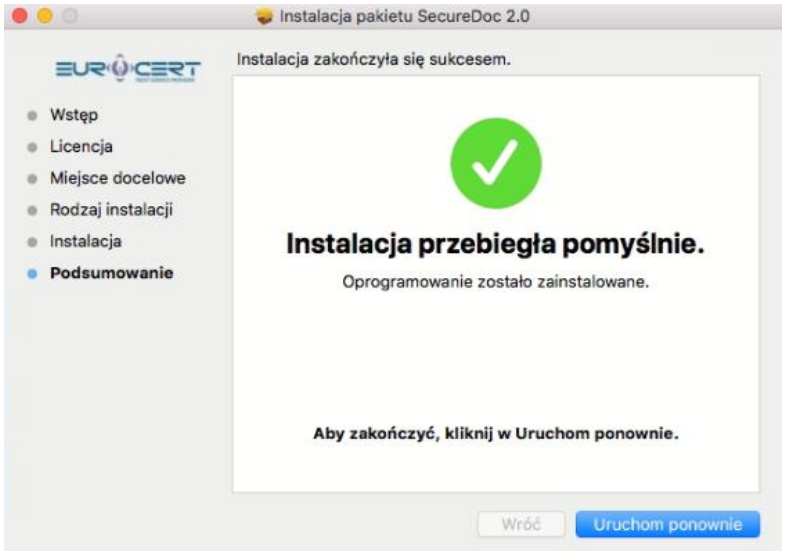

Instalacja pakietu SecureDoc 2.0
Umowa licencyjna na oprogramowanie
Polski
Wstęp
Licencja
Miejsce docelowe
Rodzaj instalacji
Instalacja
Podsumowanie
12. EuroCert zastrzega, że w każdym czasie może zaprzestać aktualizacji Oprogramowania.
13. Oprogramowanie jest chronione prawem autorskim oraz innymi ustawami i umowami o ochronie własności intelektualnej. Wszelkie prawa własności intelektualnej do Oprogramowania należą do EuroCert.
14. W zakresie nie uregulowanym postanowieniami niniejszej Licencji zastosowanie mają odpowiednie przepisy prawa polskiego, a w szczególności Kodeksu cywilnego oraz ustawy o prawie autorskim i prawach pokrewnych.
Używanie Oprogramowania oznacza akceptację postanowień niniejszej licencji.
Drukuj...
Zachowaj...
Wróć
Dalej


Instalacja pakietu SecureDoc 2.0
Wybierz miejsce docelowe
Wstęp
Licencja
Miejsce docelowe
Rodzaj instalacji
Instalacja
Podsumowanie
Zaznacz dysk, na którym chcesz zainstalować oprogramowanie SecureDoc 2.0.
Macintosh HD
949,25 GB dost.
1 TB całk.
Instalacja tego oprogramowania wymaga 628,1 MB wolnego miejsca.
Wybrana została opcja instalacji tego oprogramowania na dysku „Macintosh HD".
Wróć
Dalej


Instalacja pakietu SecureDoc 2.0
Instalacja standardowa na „Macintosh HD"
Wstęp
Licencja
Miejsce docelowe
Rodzaj instalacji
Instalacja
Podsumowanie
Ta rzecz zajmie 628,1 MB miejsca na dysku.
Aby wykonać instalację standardową oprogramowania na dysku „Macintosh HD", kliknij w Instaluj.
Zmień miejsce instalacji...
Wróć
Instaluj


Instalacja pakietu SecureDoc 2.0
Po ukończeniu instalacji tego oprogramowania konieczne będzie ponowne uruchomienie komputera. Czy na pewno chcesz zainstalować to oprogramowanie?
Anuluj
Kontynuuj instalację
Rodzaj instalacji
Instalacja
Podsumowanie
Zmień miejsce instalacji...
Wróć
Instaluj


Instalacja pakietu SecureDoc 2.0
Instaluję SecureDoc 2.0
Wstęp
Licencja
Miejsce docelowe
Rodzaj instalacji
Instalacja
Podsumowanie
Zapisuję pliki...
Wróć
Dalej

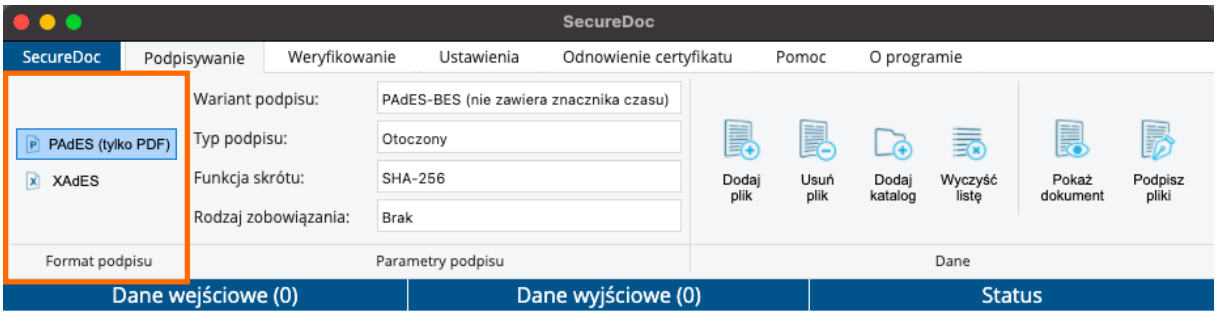

Instalacja pakietu SecureDoc 2.0
Instalacja zakończyła się sukcesem.
Wstęp
Licencja
Miejsce docelowe
Rodzaj instalacji
Instalacja
Podsumowanie
Instalacja przebiegła pomyślnie.
Oprogramowanie zostało zainstalowane.
Aby zakończyć, kliknij w Uruchom ponownie.
Wróć
Uruchom ponownie

Po zakończeniu tego etapu aplikacja jest gotowa do użytku.

4. Podpisywanie

Wkładka „Podpisywanie” jest wyznaczona do wystawienia podpisów elektronicznych.

W sekcji „Format podpisu” znajdują się dwa dostępne formaty dla plików podpisywanych:
PAdES oraz XAdES

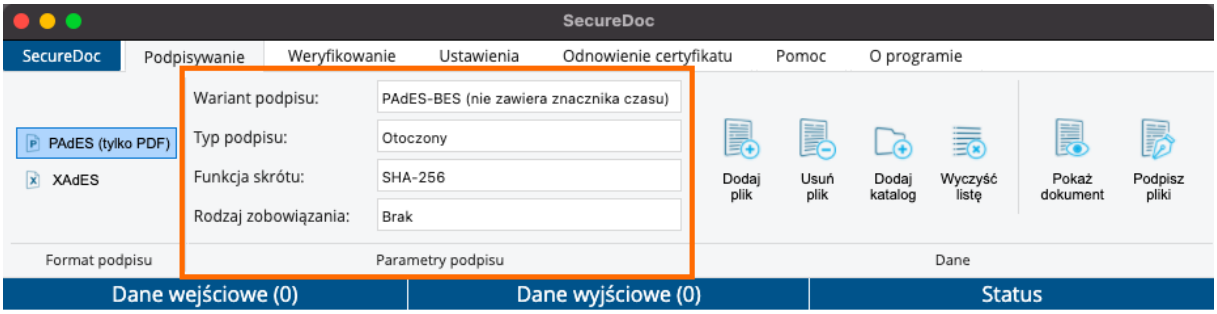


Format PAdES jest dedykowany i wyłączny dla plików PDF oraz jest opcją zalecaną przy podpisywaniu plików w formacie PDF.

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

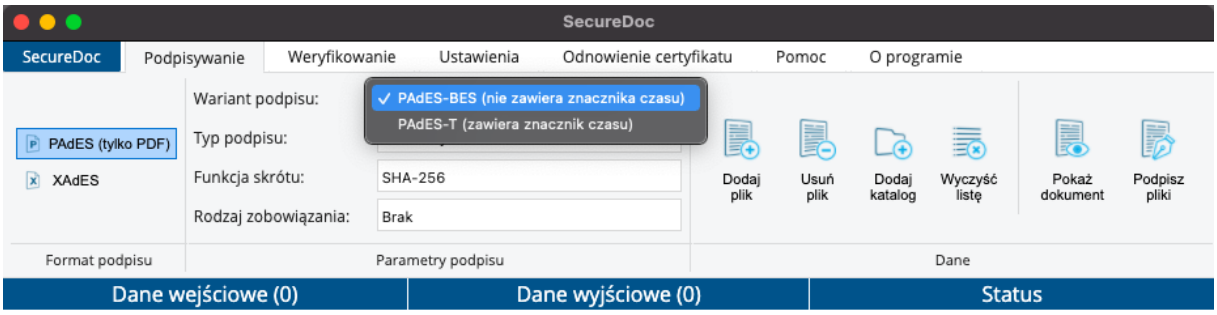
4.1 Sekcja „Parametry podpisu”

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



4.1.1 Wariant podpisu

W zależności od wybranego formatu podpisu możliwe są następujące opcje wyboru z danej listy – PAdES-BES / PAdES-T lub XAdES-BES / XAdES-T



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

Z kolei format -T mówi o tym, że podpis zostanie wystawiony ze znacznikiem czasu.

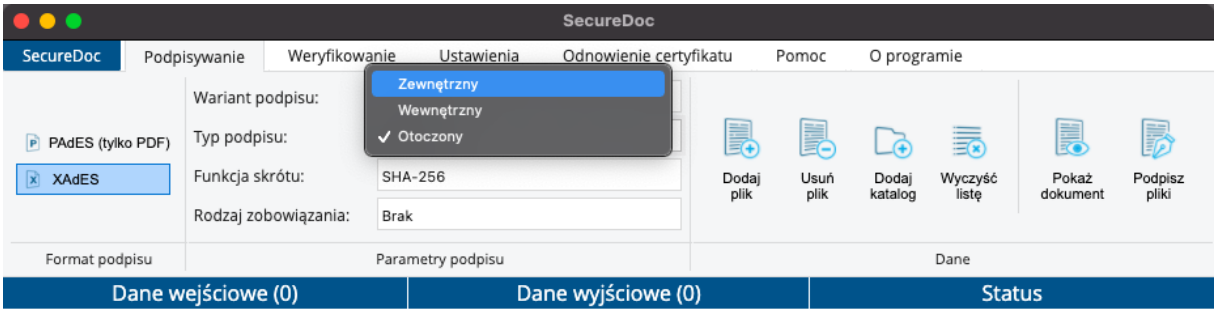
Usługa kwalifikowanego znakowania czasem („znacznik czasu" wspomniany wyżej) jest usługą dodatkową i umożliwia dokładne określenie daty i czasu czynności realizowanych w środowisku elektronicznym.

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.

Także warto zwrócić uwagę że 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.

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

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

Ważne jest aby po złożeniu podpisu zewnętrznego plik podpisywany nie był zmieniany 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.

Plik podpisu zewnętrznego zapisywany jest w formacie XAdES.

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.

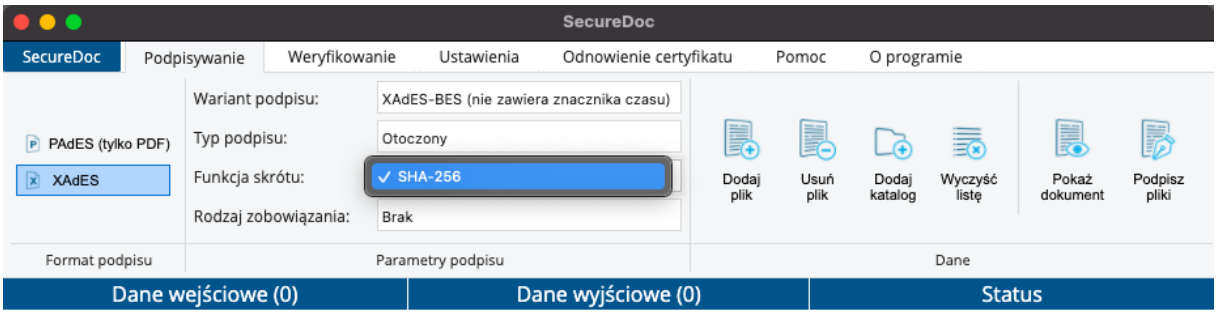
Czyli jeżeli np. podpisujemy plik *dokument.txt*, to plik podpisany podpisem wewnętrznym będzie wyglądał następująco – *dokument.txt.XAdES*

4.1.2.3 Otoczony

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

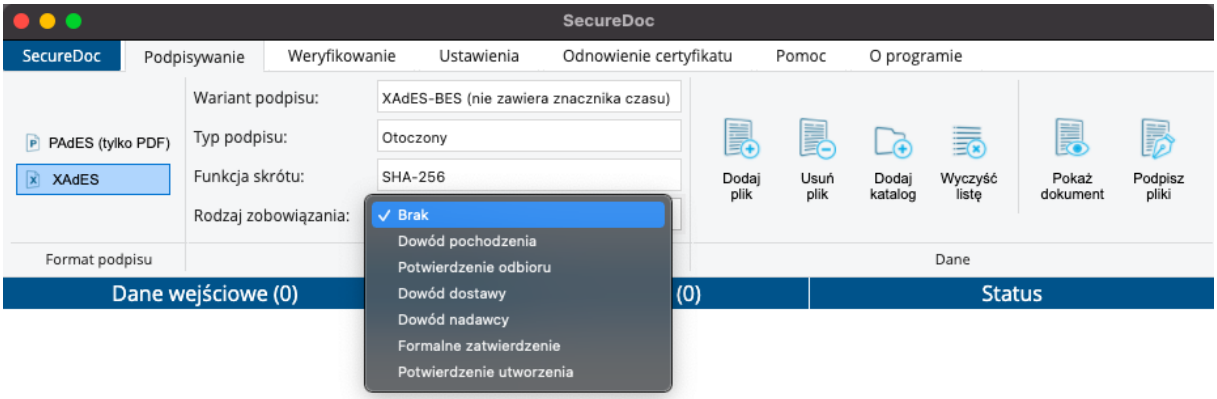
Czyli jeżeli chcemy podpisać plik XML tak, aby zawierał on podpis + treść dokumentu – należy wybrać typ podpisu „otoczony". Typ podpisu „otoczony" dotyczy jedynie plików w formacie XML.

4.1.3 Funkcja skrótu



- SHA-256 – jest typem zabezpieczenia kryptograficznego, większa wartość skrótu zapewnia większe bezpieczeństwo.

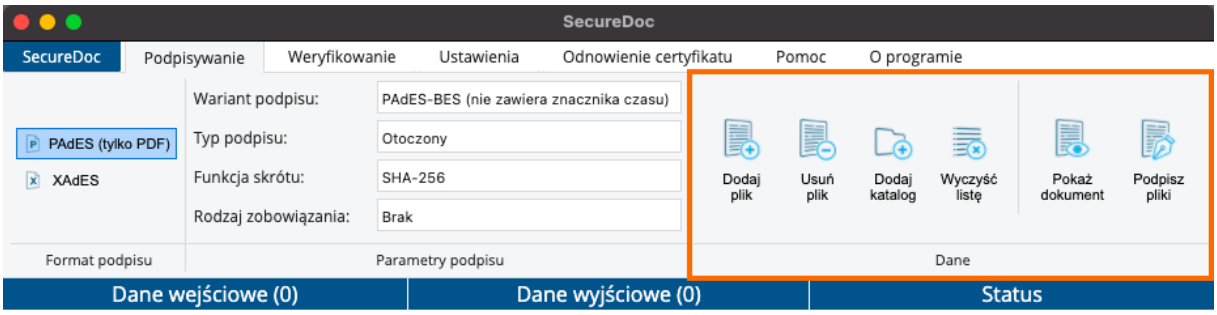
4.1.4 Rodzaj zobowiązania



Dane pole jest opcjonalne i zawiera w sobie informacje dodatkowe odnośnie powodu / celu złożenia podpisu. Wybór rodzaju zobowiązania nie jest wymagany aby złożyć podpis.
Do wyboru dostępne są 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.

"Dodaj katalog" - przy pomocy tej funkcji mamy możliwość dodania 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 dla podpisywania przy pomocy przycisków „Usuń plik" – w celu pojedynczego usuwania (usunięty zostanie wybrany, czyli podświetlony plik), lub „Wyczyść listę" – aby usunąć całą listę wybranych plików.

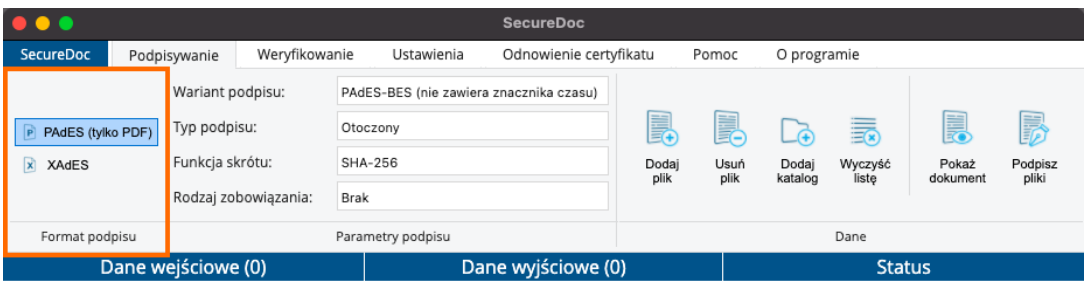
Wciśnięcie przycisku „Pokaż dokument" spowoduję wyświetlenie treści wybranego dokumentu w nowym oknie.

„Podpisz pliki" – po wciśnięciu danego przycisku zostaną podpisane wszystkie pliki z listy wybranych do podpisania plików.

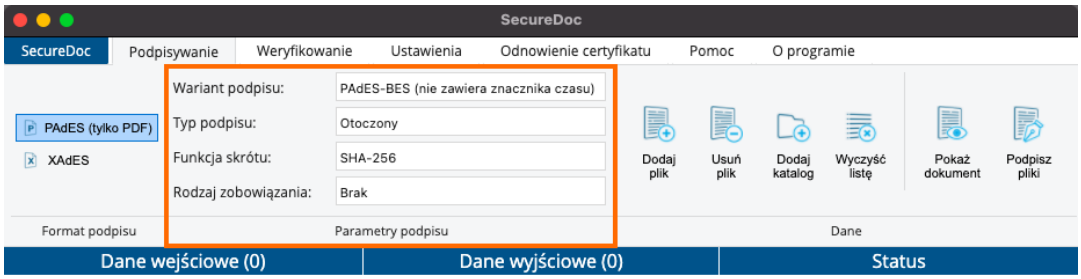
4.3 Proces złożenia podpisu elektronicznego:

Należy pamiętać że w celu podpisania pliku podpisem kwalifikowanym urządzenie z kartą kryptograficzną musi być podłączone do komputera.

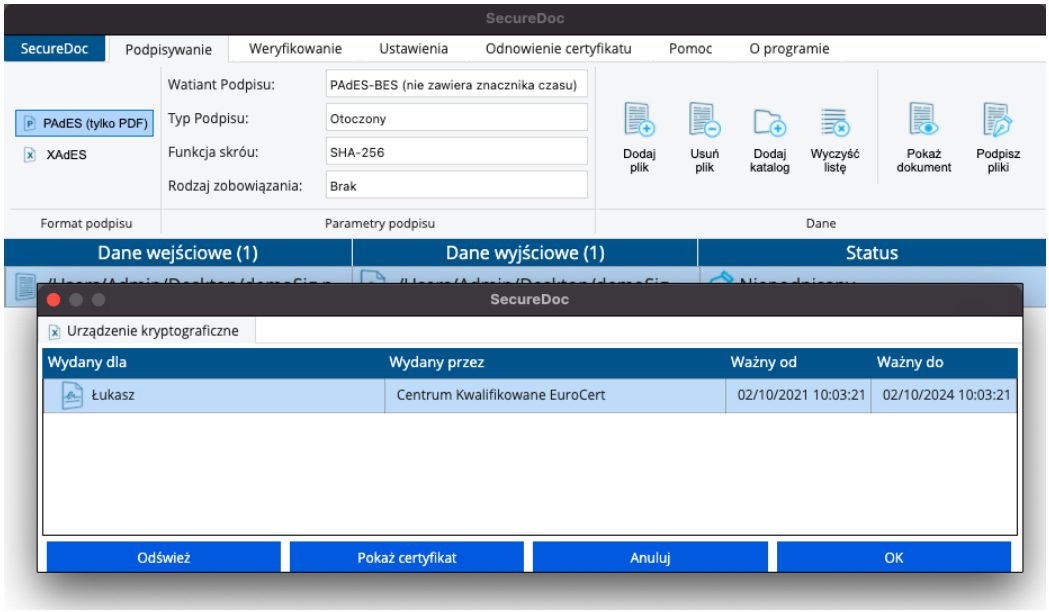
1. Określamy rodzaj podpisu jakim chcemy podpisać dokument (pole „Format podpisu")



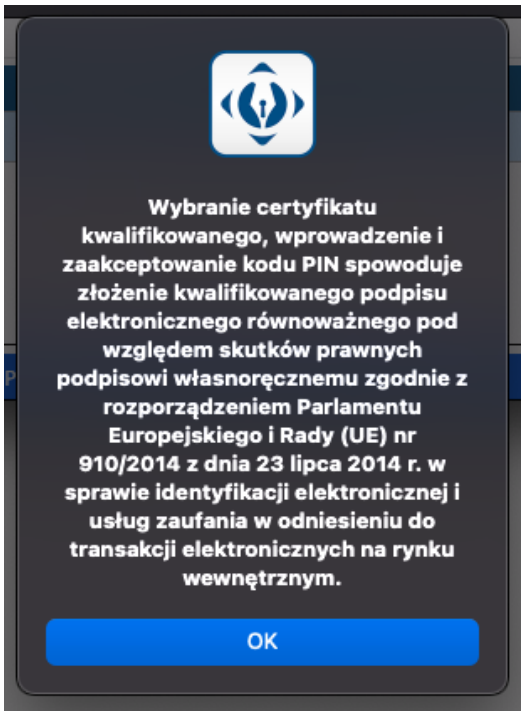
2. Wybieramy żądane opcje podpisu w polu „Parametry podpisu"



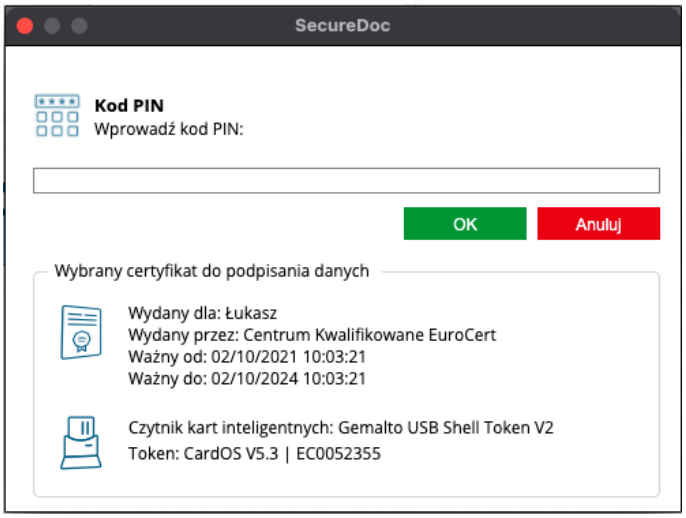
3. Dodajemy pliki, które chcemy podpisać
4. Klikamy „Podpisz pliki”. Warto zwrócić uwagę na to, że wszystkie dokumenty z listy wybranych do podpisania zostaną podpisane z takimi samymi ustawieniami parametrów podpisu.
5. Po wciśnięciu „Podpisz pliki” pojawi się okno wyboru certyfikatu. Z listy wybieramy certyfikat z użyciem którego chcemy podpisać wybrane pliki i klikamy „OK”. W danej zakładce dostępne są certyfikaty, które znajdują się na aktualnie podłączonym urządzeniu.



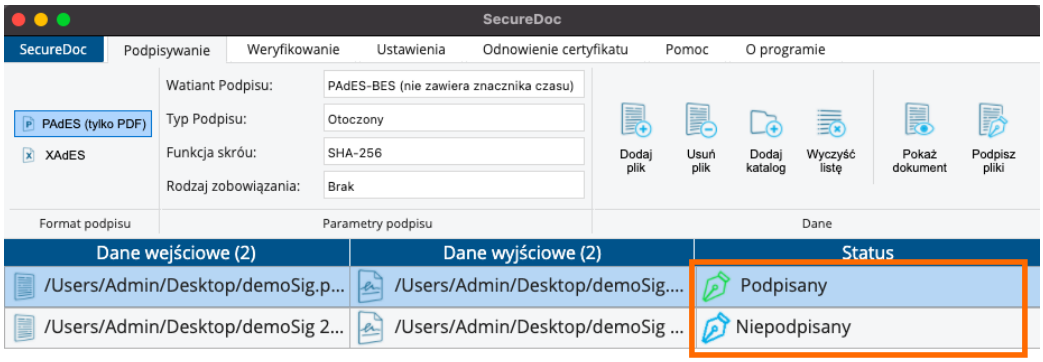
6. Po wybraniu certyfikatu i kliknięciu „OK” pojawi się komunikat informacyjny odnośnie składanego podpisu. Po zapoznaniu się z komunikatem klikamy „OK”



7. Wprowadzamy kod PIN i klikamy „OK”. Jeśli wpisany kod PIN jest prawidłowy, aplikacja rozpocznie proces podpisywania.

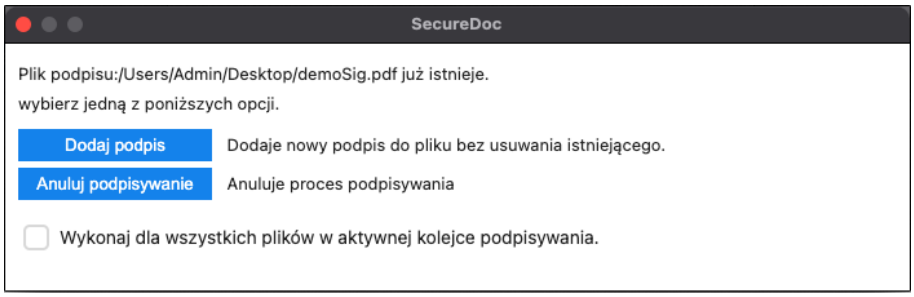


8. Sprawdzamy status podpisu. Jeśli dokument został prawidło podpisany, w oknie statusu przy podpisanych plikach pojawi się status „Podpisany”, jeśli wystąpił błąd otrzymasz status „Niepodpisany”.



4.4 Dodawanie kolejnych podpisów do pliku

W celu dodania kolejnego podpisu do podpisanego pliku, w przypadku podpisu XAdES dodajemy plik który podpisaliśmy, lub plik podpisu w formacie XAdES i postępujemy w ten sam sposób jak z dodawaniem pierwszego podpisu. W momencie wyświetlenia okienka „Dodaj podpis" wybieramy opcję „Dodaj podpis".



5. Weryfikowanie

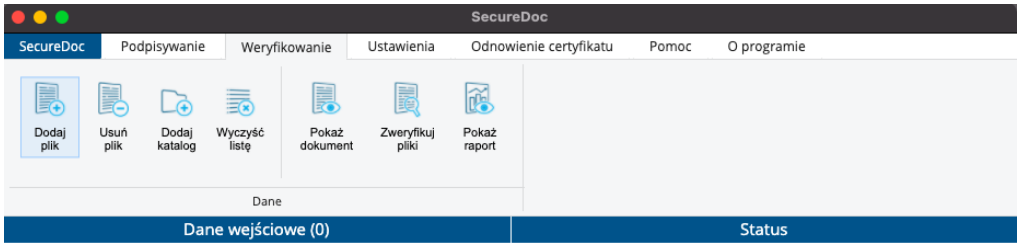
W danej wkładce mamy możliwość weryfikacji podpisanych plików oraz wyświetlenia raportu dla zweryfikowanych podpisów elektronicznych.

Funkcjonalność przycisków „Dodaj plik", „Usuń plik", „Dodaj katalog", „Wyczyść listę" oraz „Pokaż dokument" jest dokładnie taka sama jak funkcjonalność analogicznych przycisków z wkładki „Podpisywanie".

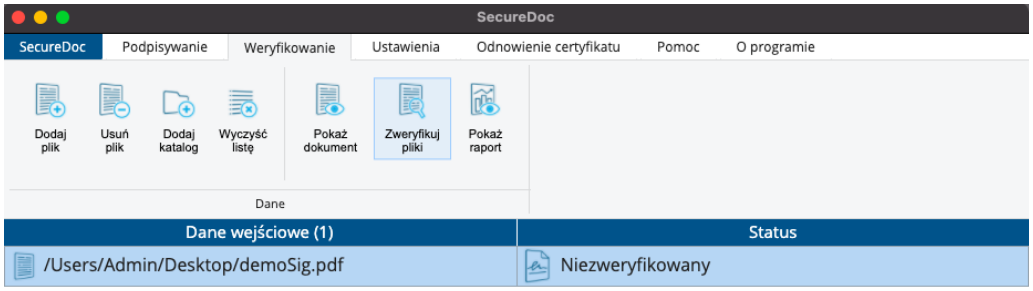
Warto wspomnieć, że do listy dla weryfikacji mogą zostać dodane jednocześnie pliki o różnym rodzaju podpisu. Jeśli plik jest podpisany podpisem w formacie zewnętrznym, należy dodać do listy jedynie plik podpisu. Dodatkowo należy pamiętać aby zarówno plik podpisu jak i plik podpisywany znajdował się w tym samym miejscu/folderze. W innym wypadku aplikacja nie będzie mogła odwołać się do pliku źródłowego (podpisanego zewnętrznie). W sytuacji podpisu wewnętrznego wystarczy wskazać plik podpisany.

5.1 Proces weryfikacji plików

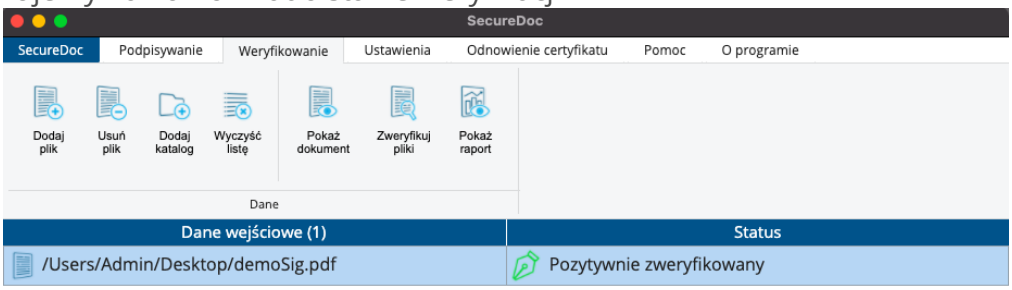
1. Dodajemy pliki, które chcemy zweryfikować



2. Klikamy „Zweryfikuj pliki" (Należy pamiętać aby w momencie weryfikowania pliku posiadać połączenie z Internetem)



3. Oczkujemy na komunikat o stanie weryfikacji



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

W celu otrzymania bardziej dokładnych informacji na temat wyniku weryfikacji należy kliknąć „Pokaż raport"

Możemy także podejrzeć podpisany dokument, który weryfikujemy klikając „Pokaż dokument"

6. Ustawienia:

6.1 Ustawienia aplikacji

6.1.1 Ustawienia ogólne

Język

W celu zmiany języka w ustawieniach ogólnych, w sekcji „Język” należy wybrać jeden z dostępnych języków z listy rozwijanej.

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.

Także w danej sekcji jest dostępna informacja odnośnie zainstalowanej wersji aplikacji.

Proxy

W sekcji Proxy jest dostępna możliwość skonfigurowania serwera proxy, który ma być wykorzystywany przez aplikację SecureDoc. Aby skonfigurować proxy należy zaznaczyć opcję „Włącz proxy” i podać wszystkie niezbędne informacje w dostępnych polach.

6.1.2 Ustawienia podpisywania

W zakładce Ustawienia podpisywania, można dostosować, jakie mają być ustawienia „domyślne” podpisu w momencie uruchomienia 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

Dodatkowe opcje podpisywania

W danej sekcji mamy możliwość konfiguracji następujących opcji:

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

Zaznaczona opcja, z kolej, spowoduję utworzenie podpisu w pliku źródłowym i nadpisanie jego, czyli edycja pliku podpisywanego zamiast zapisania pliku z podpisem w osobnym dokumencie.

„Nie koduj danych XML do Base64" - odznaczenie danej opcji spowoduję zapisanie podpisywanego pliku XML jako zakodowanego w Base64. Zaznaczenie z kolei pozwoli na normalne zapisywanie plików XML w standardowym kodowaniu UTF-8.

„Nadpisz plik XML, gdy używasz typu „Otoczonego" w formacie podpisu XAdES" - Jeżeli podpisywany jest plik XML i chcemy aby po podpisaniu został on zapisany w tym samym formacie – XML, należy **zaznaczyć** daną opcję.

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

„Utwórz podpis „Otoczony" w standardowej wersji" – Podpis złożony w danej konfiguracje blokuje dodanie kolejnych podpisów na tym samym dokumencie.

6.1.3 Ustawienia znacznika czasu

Aby mieć możliwość korzystania ze znaczników czasu należy odpowiednio skonfigurować dostęp do serwera znaczników czasu. Możemy do niej przystąpić w momencie gdy otrzymamy od EuroCert niezbędne dane konfiguracyjne:

- Adres serwera znaczników czasu – spersonalizowany link dostępowy do serwera znaczników czasu,
- Nazwa użytkownika – spersonalizowany login,
- Hasło – spersonalizowane hasło (bez możliwości zmiany).

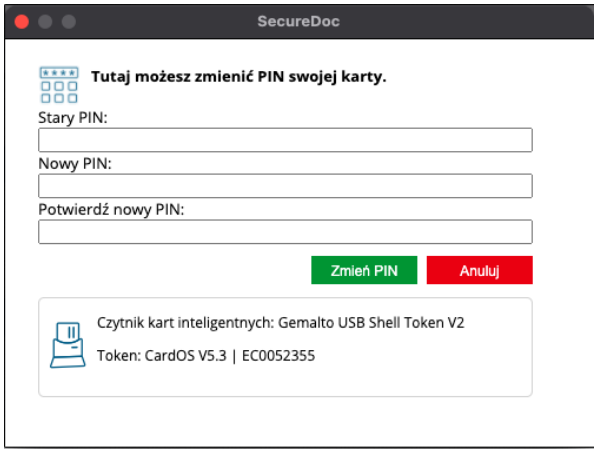
Użytkownik otrzymuje przedstawione dane konfiguracyjne w momencie gdy zakupi dodatkową usługę znakowania czasem.

6.2 Zarządzanie kartą inteligentną

Uwaga! Trzykrotne wprowadzenie niepoprawnego kodu PIN skutkuje jego zablokowaniem.
Aby odblokować 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:



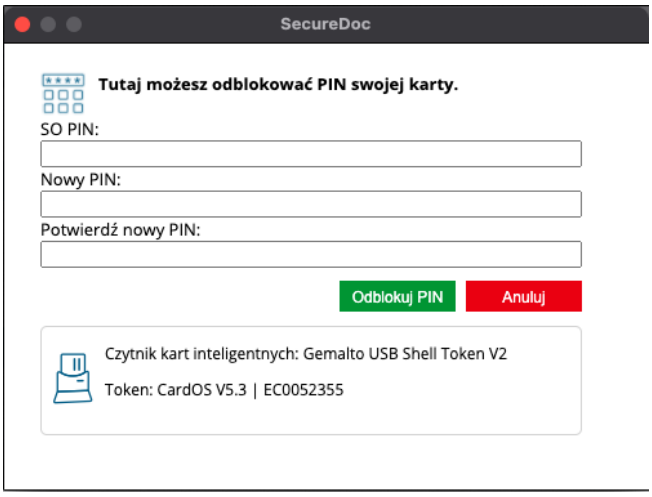
Następnie należy wprowadzić „Stary PIN” oraz dwukrotnie podać „Nowy PIN”.

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:

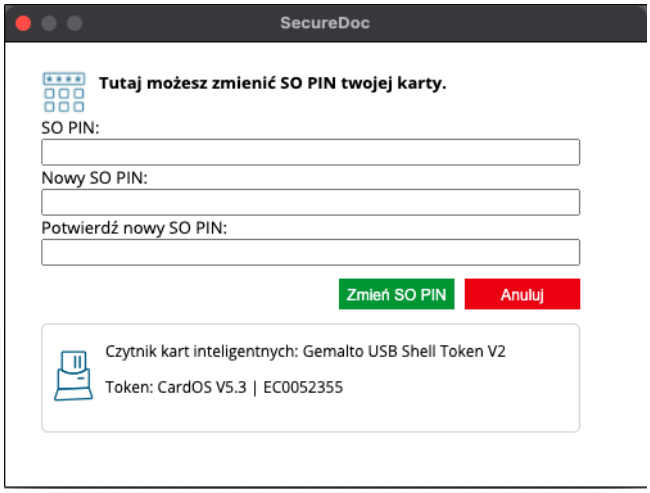


Następnie należy wprowadzić „SO PIN” oraz dwukrotnie podać „Nowy PIN”

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

6.2.3 Zmiana SO PIN

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



Następnie należy wprowadzić „SO PIN” oraz dwukrotnie podać „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.

Pozostałe informacje:

Podczas zmiany numerów 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

Po kliknięciu danego przycisku zostaniemy przeniesieni na stronę sklepu sklep.eurocert.pl w rozdział „Odnowienie online - dla obecnych klientów EuroCert”, gdzie można wybrać żądany certyfikat.

Odnowienie certyfikatu

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

Po zakupie kodu odnawiającego należy przejść do wkładki „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 przestawionej w instrukcji.

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

8. Pomoc

Dana zakładka zawiera dane kontaktowe do działu wsparcia technicznego oraz możliwość pobrania aplikacji AnyDesk do połączeń zdalnych

9. O programie

Zakładka zawiera treść licencji