Instrukcja przeniesienia certyfikatu kwalifikowanego z karty kryptograficznej na kartę wirtualną SimplySign

Wersja 2.2

Spis treści

1. Wstęp

Niniejsza instrukcja przedstawia proces przeniesienia certyfikatu kwalifikowanego z karty kryptograficznej na kartę SimplySign.

Proces przebiega w dwóch etapach:

1. Aktywacja usługi SimplySign;
2. Złożenie wniosku o odnowienie/ przeniesienie.

2. Wymagania

Przed rozpoczęciem procedury wymagane jest aby Użytkownik:

1. Zainstalował i aktywował na urządzeniu mobilnym aplikację SimplySign;
2. Uzyskał kod aktywacyjny na przeniesienie.

3. Aktywacja usługi SimplySign

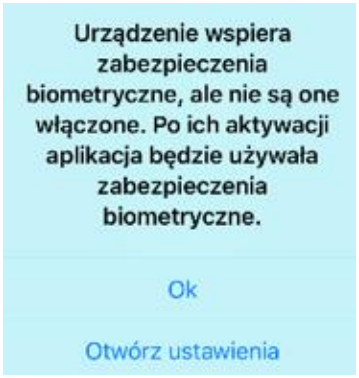
Aplikację **SimplySign** można pobrać z App Store (urządzenia z systemem iOS) oraz ze sklepu Google Play (urządzenia z systemem Android).

3.1 iOS

Aplikacja wspiera używanie zabezpieczeń biometrycznych ustawionych na urządzeniu. Jeżeli w systemie operacyjnym urządzenia ustawione są zabezpieczenia biometryczne w formie odcisku palca lub wizerunku twarzy, to przy uruchomieniu aplikacji wymuszone zostanie uwierzytelnienie się wybraną metodą zabezpieczeń.

Zabezpieczenia biometryczne działają wg poniższej logiki:

A. W przypadku, gdy urządzenie wspiera zabezpieczenia biometryczne, ale nie są one włączone to na starcie aplikacji pojawia się poniższy komunikat:

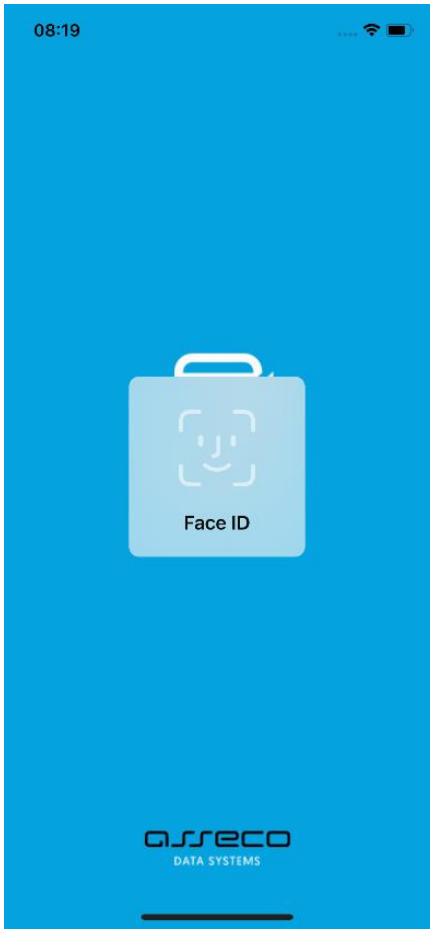


Naciśnięcie przycisku **Otwórz ustawienia** przenosi do Ustawień, w których można ustawić Touch ID/Face ID.

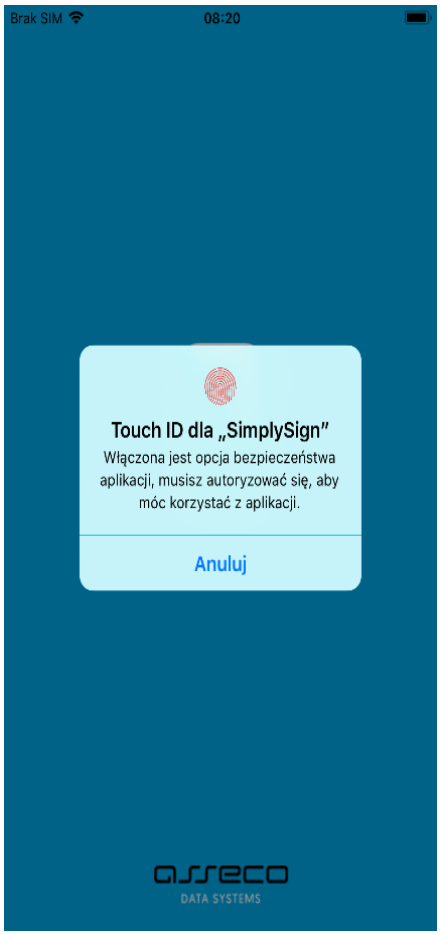
B. W przypadku, gdy urządzenie ma włączone Face ID, po pierwszym uruchomieniu aplikacji pojawia się poniższy komunikat. Przy włączonych zabezpieczeniach biometrycznych dla Touch ID nie ma takiego komunikatu, aplikacja przejdzie do uwierzytelnienia za pomocą odcisku palca.

Po wybraniu **OK** aplikacja przejdzie do uwierzytelnienia.

Face ID:



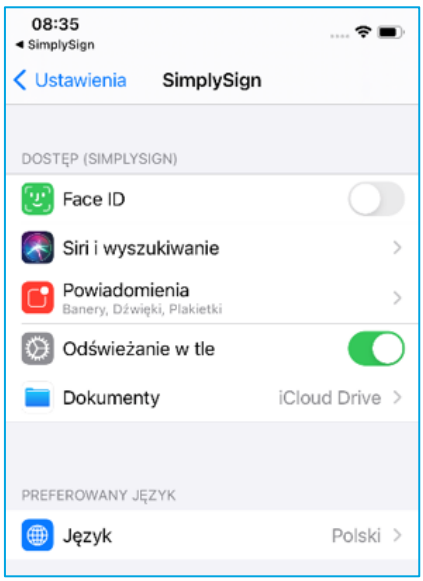
Touch ID:



Jeżeli użytkownik wybierze opcję **Nie pozwalaj** (dla Face ID):

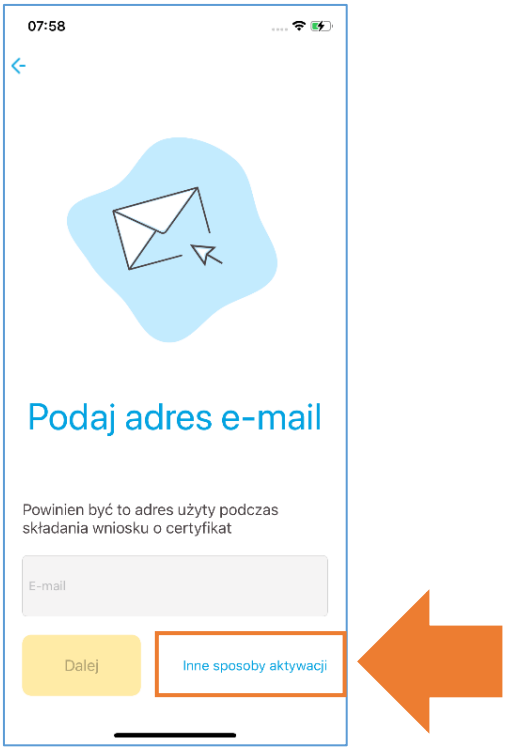
Wyświetlony zostanie poniższy komunikat, umożliwiający przejście do ustawień:

Naciśnięcie przycisku **Otwórz ustawienia** spowoduje przejście do Ustawień, w których należy zezwolić na Face ID dla aplikacji SimplySign. Dopóki nie ustawi się tego zezwolenia aplikacja nie pozwoli na pracę – cały czas będzie wyświetlała komunikat **„Aby skorzystać z FaceID musisz nadać aplikacji uprawnienia do korzystania z tej funkcji"**.

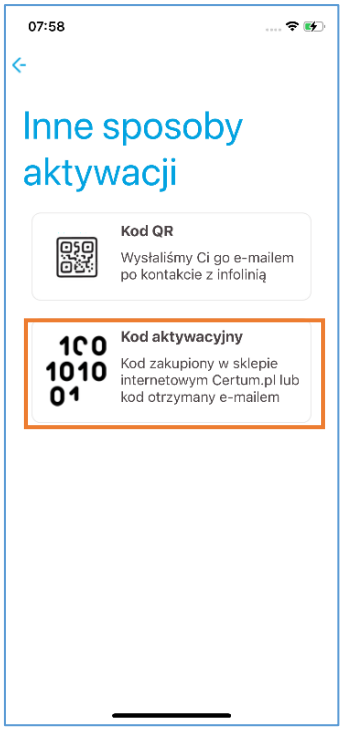


Po wyświetleniu ekranu startowego aplikacji, należy wybrać opcję **Aktywuj aplikację**.

W procesie przeniesienia certyfikatu z karty na chmurę należy przejść do **Innych sposobów aktywacji**.



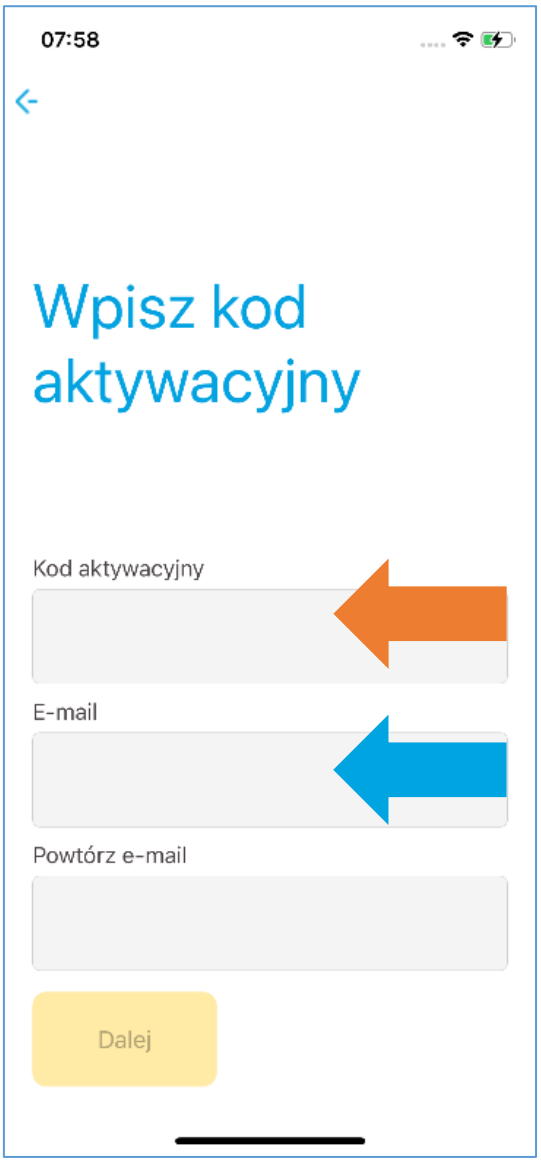
Następnie należy wybrać opcję **Kod aktywacyjny**. Wyświetlony zostanie ekran umożliwiający wprowadzenie kodu (użytkownik otrzymuje kod aktywacyjny po zakupie usługi przeniesienia).



Należy uzupełnić pola **Kod aktywacyjny**, **E-mail** i **Powtórz e-mail**. Po wprowadzeniu tych danych należy nacisnąć przycisk **Dalej**.

UWAGA!!!

Wprowadzony adres e-mail będzie jednocześnie identyfikatorem użytkownika. Zaleca się, aby był to **rzeczywisty** adres e-mail, do którego użytkownik ma dostęp - jest to związane z tym, że w przyszłości wiadomości e-mail (np. reset kodu PIN do wirtualnej karty) wysyłane z Systemu SimplySign do Użytkownika będą wysyłane na ten adres.



Jeśli dane są poprawne to aplikacja wyświetli ekran umożliwiający wybór trybu pracy.

Dostępne są dwa tryby:

- Podpisywanie i Generuj token – umożliwia podpisywanie dokumentów i jednoczesne generowanie tokenów;
- Generuj token – umożliwia tylko generowanie tokena – wtedy podpisywanie trzeba będzie robić na innym urządzeniu.

Po wybraniu trybu należy nacisnąć przycisk **Zakończ aktywację**.

Wyświetlony zostanie ekran z informacją, że aplikacja jest aktywna.

Po naciśnięciu przycisku **Zacznij podpisywać dokumenty** aplikacja przejdzie do ekranu startowego:

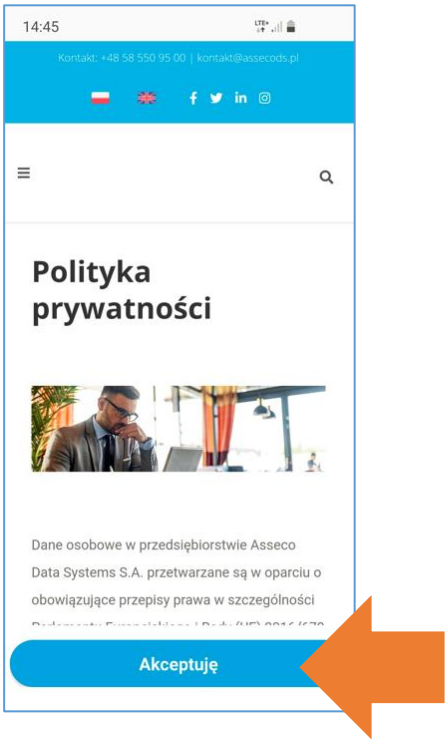
W trakcie procesu przeniesienia potrzebny będzie tzw. **token OTP**. Aby go wyświetlić należy nacisnąć przycisk **Generuj token**.

Nowy token generuje się co 30 sekund:

Po aktywacji aplikacji należy przejść do punktu 4 niniejszej instrukcji.

3.2 Android

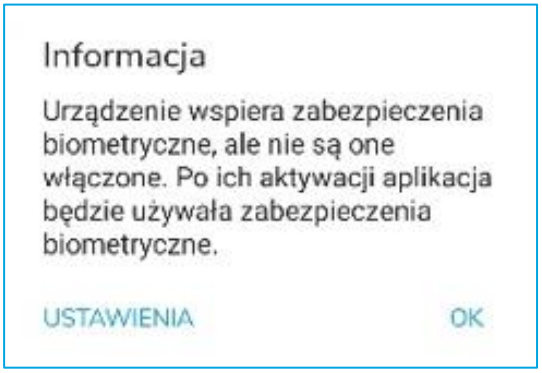
Przy pierwszym uruchomieniu aplikacji wymagane jest zapoznanie się z polityką prywatności i zaakceptowanie jej treści.



Aplikacja wspiera używanie zabezpieczeń biometrycznych ustawionych na urządzeniu. Jeżeli w systemie operacyjnym urządzenia ustawione są zabezpieczenia biometryczne w formie odcisku palca lub wizerunku twarzy, to przy uruchomieniu aplikacji wymuszone zostanie uwierzytelnienie się wybraną metodą zabezpieczeń.

Zabezpieczenia biometryczne działają wg poniższej logiki:

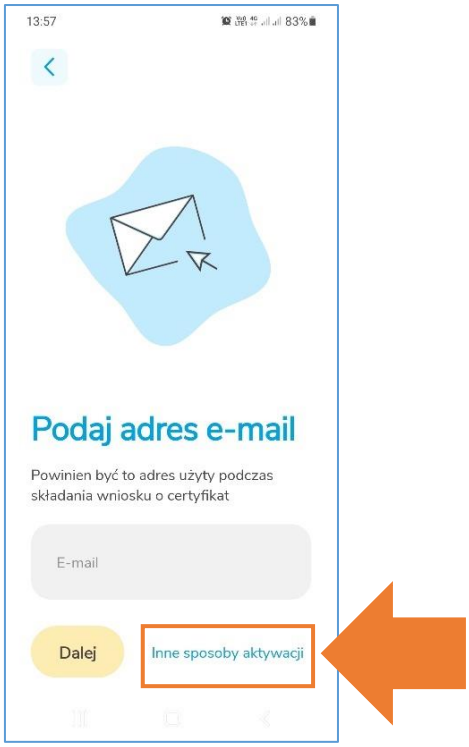
A. W przypadku, gdy urządzenie wspiera zabezpieczenia biometryczne ale nie są one włączone to na starcie aplikacji pojawia się poniższy komunikat:



B. W przypadku, gdy na urządzeniu włączone są zabezpieczenia biometryczne to przy uruchomieniu aplikacji pojawi się uwierzytelnianie wybranym zabezpieczeniem.

Po wyświetleniu ekranu startowego aplikacji, wybierz opcję **Aktywuj aplikację.**

W procesie przeniesienia certyfikatu z karty na chmurę należy przejść do **Innych sposobów aktywacji**.



Następnie należy wybrać opcję **Kod aktywacyjny**. Wyświetlony zostanie ekran umożliwiający wprowadzenie kodu (użytkownik otrzymuje kod aktywacyjny po zakupie usługi przeniesienia).

Następnie należy uzupełnić pola **Kod aktywacyjny**, **E-mail** i **Powtórz e-mail**. Po wprowadzeniu tych danych należy nacisnąć przycisk **Dalej**.

UWAGA!!!

Wprowadzony adres e-mail będzie jednocześnie identyfikatorem użytkownika. Zaleca się, aby był to **rzeczywisty** adres e-mail, do którego użytkownik ma dostęp - jest to związane z tym, że w przyszłości wiadomości e-mail (np. reset kodu PIN do wirtualnej karty) wysyłane z Systemu SimplySign do Użytkownika będą wysyłane na ten adres.

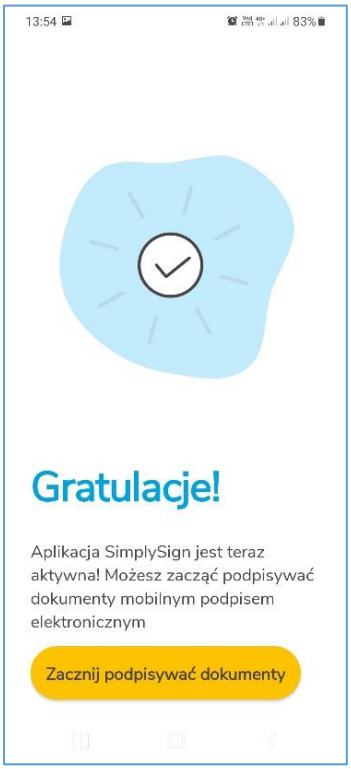
Jeśli dane są poprawne to aplikacja wyświetli ekran umożliwiający wybór trybu pracy.

Dostępne są dwa tryby:

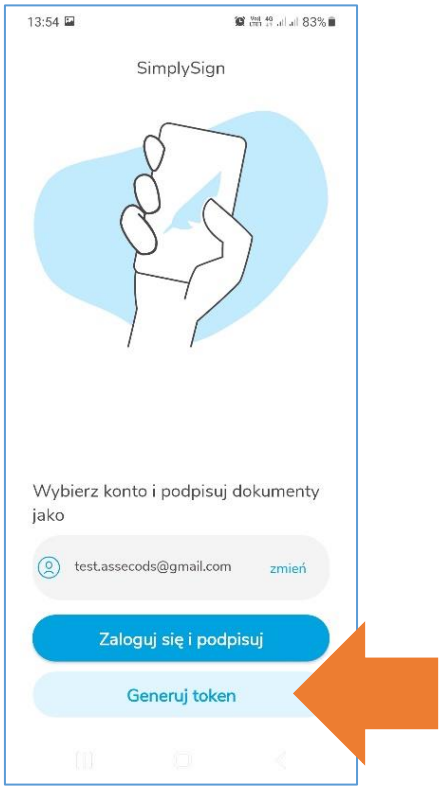
- Podpisywanie i Generuj token – umożliwia podpisywanie dokumentów i jednoczesne generowanie tokenów;
- Generuj token – umożliwia tylko generowanie tokena – wtedy podpisywanie trzeba będzie robić na innym urządzeniu.

Po wybraniu trybu należy nacisnąć przycisk **Zakończ aktywację**.

Wyświetlony zostanie ekran z informacją, że aplikacja jest aktywna.



Po naciśnięciu przycisku **Zacznij podpisywać dokumenty** aplikacja przejdzie do ekranu startowego:



W trakcie procesu odnowienia potrzebny będzie tzw. **token OTP**. Aby go wyświetlić należy nacisnąć przycisk **Generuj token**.

Nowy token generuje się co 30 sekund:

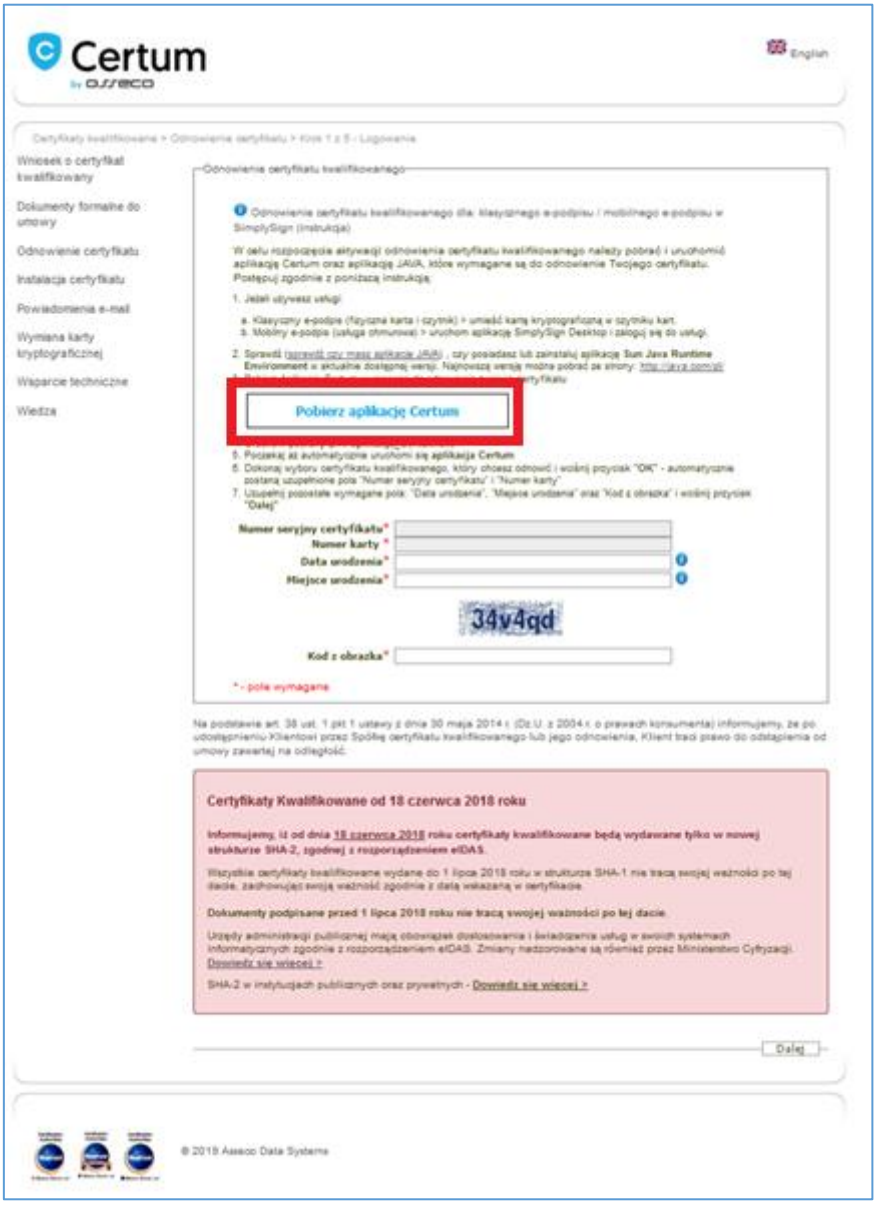
W celu rozpoczęcia procesu przeniesienia należy przejść do kolejnego punku zawartego w instrukcji.

4. Złożenie wniosku o przeniesienie certyfikatu

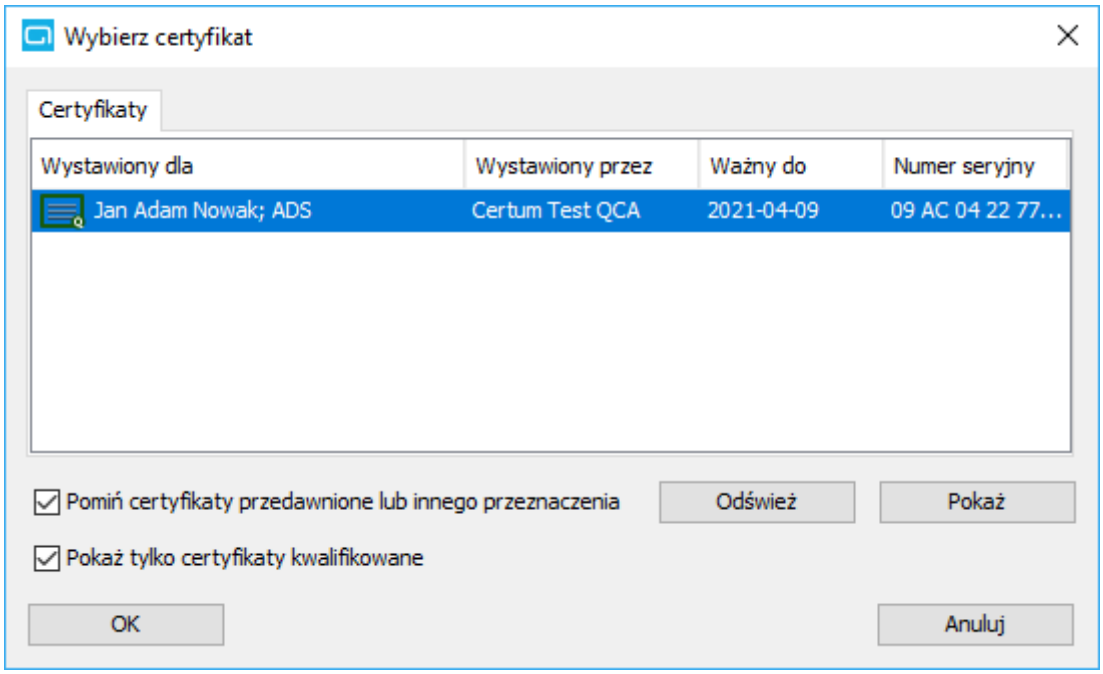
Należy umieścić kartę kryptograficzną w czytniku i uruchomić następującą stronę:

https://status.certum.pl/odnowienia/auth

i następnie uruchomić **aplikację Certum**.

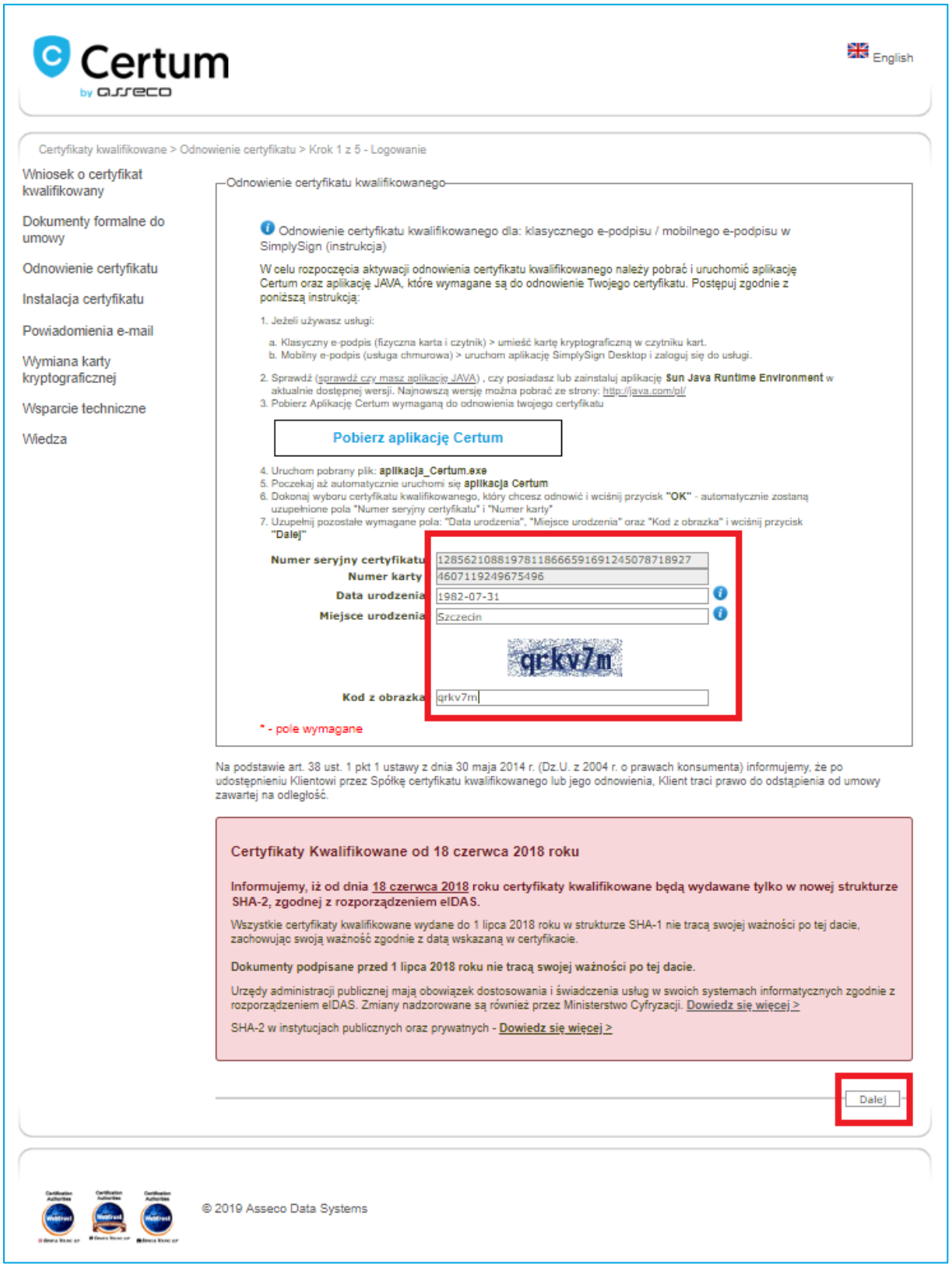


Po uruchomieniu aplikacji Certum wyświetlone zostanie okienko wyboru certyfikatu, który zostanie odnowiony/ przeniesiony.

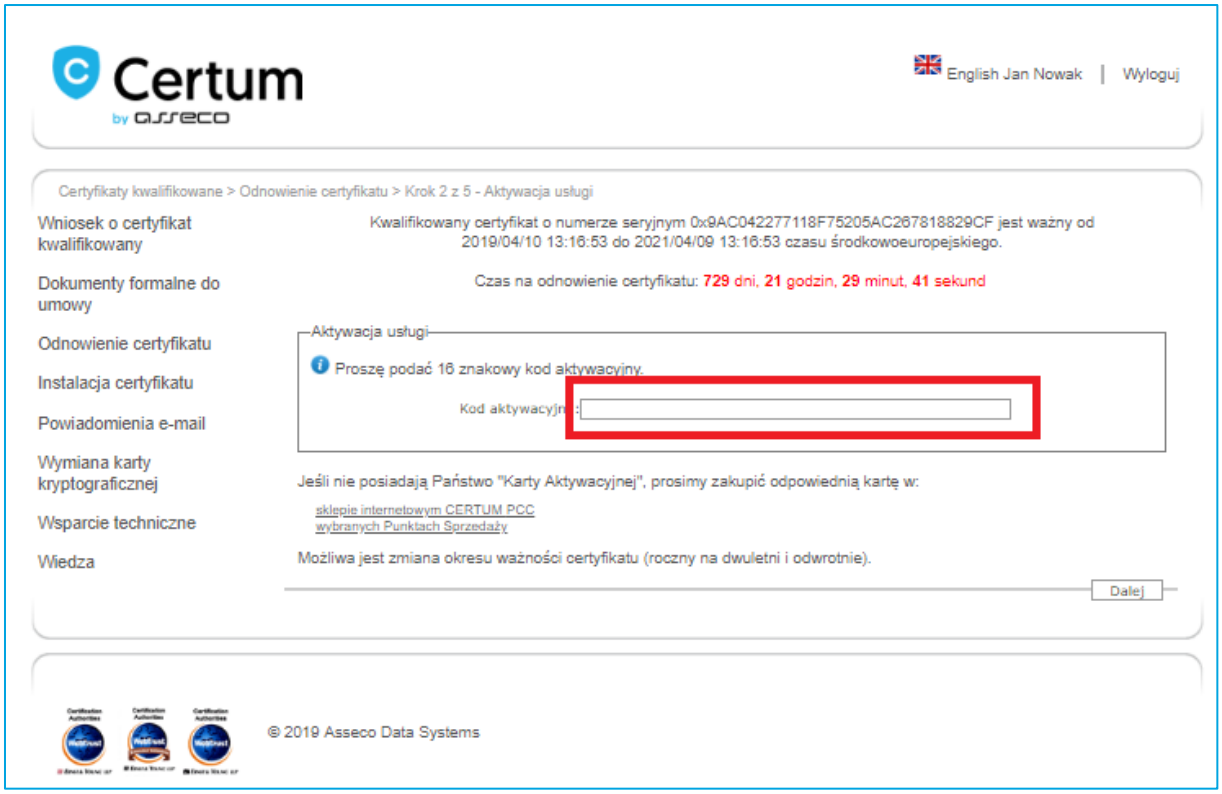


Należy wybrać certyfikat, który zostanie przeniesiony z karty na chmurę i nacisnąć przycisk **OK**.

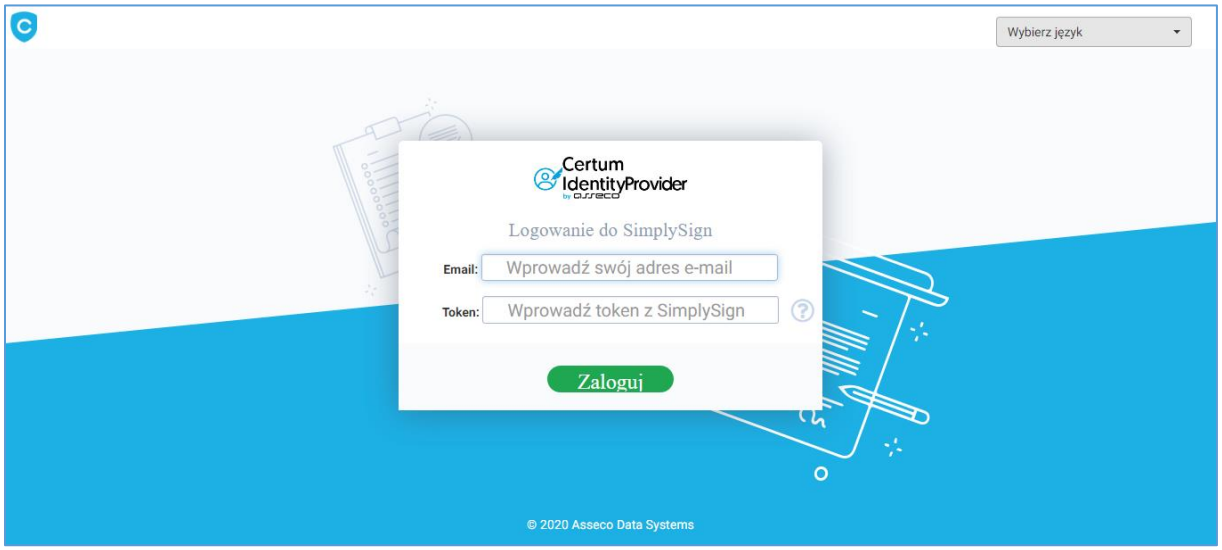
Do formularza automatycznie zostanie wprowadzony numer karty i numer wybranego certyfikatu. W formularzu należy wprowadzić **datę i miejsce urodzenia**, **kod zabezpieczający (kod z obrazka)** i nacisnąć przycisk **Dalej**.



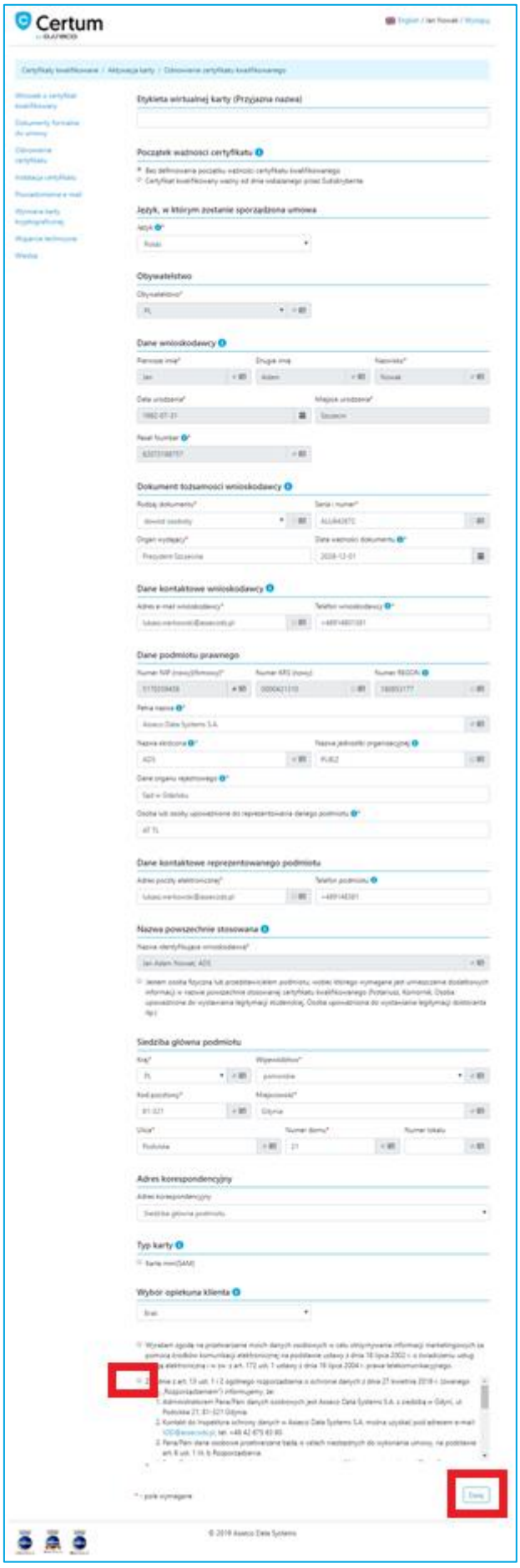
Wyświetlony zostanie formularz, w którym należy wprowadzić **kod aktywacyjny** i nacisnąć przycisk **Dalej**.



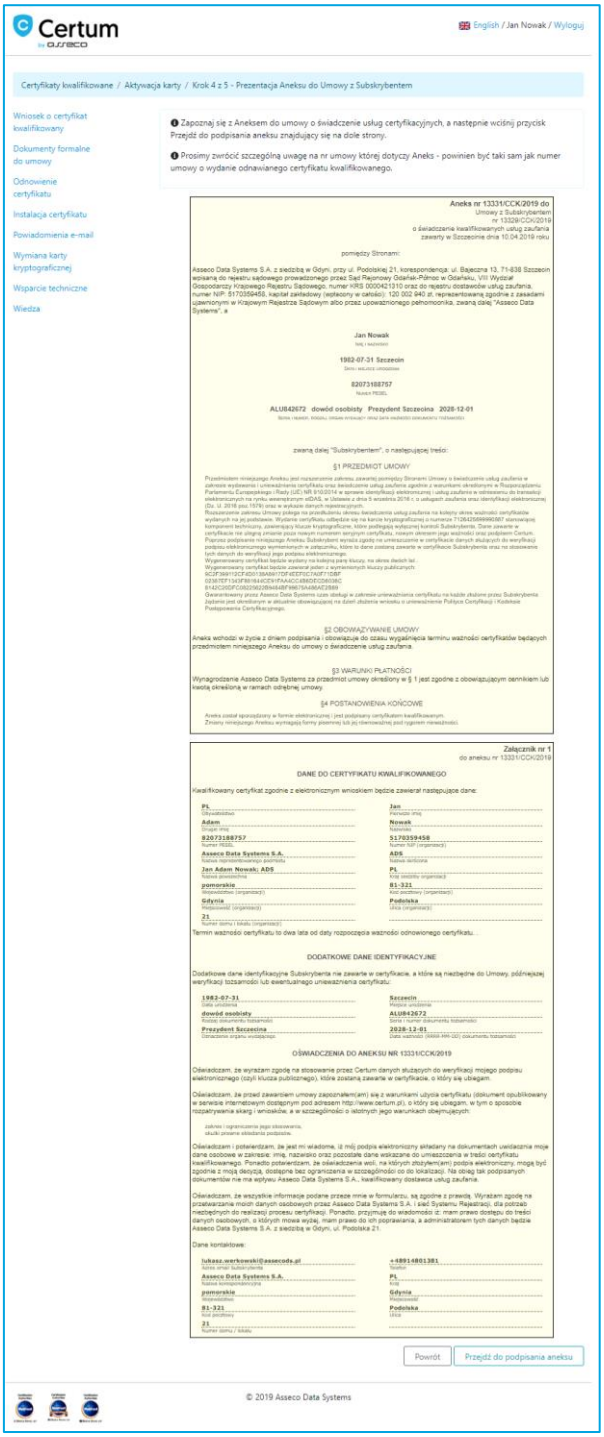
Wyświetlony zostanie formularz, w którym należy wprowadzić dane do logowania do konta **SimplySign**.



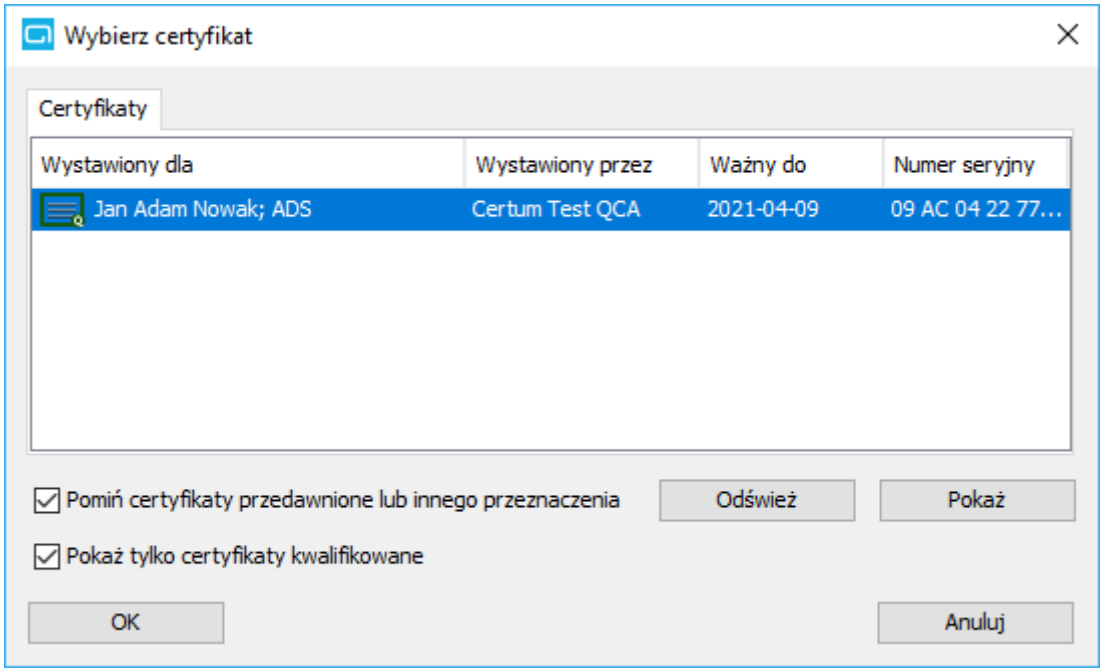
Dane do logowania należy uzyskać z **aplikacji SimplySign** na urządzeniu mobilnym (Opcja **Generuj token**). Po wprowadzeniu danych do logowania należy nacisnąć przycisk **Zaloguj**. Wyświetlony zostanie formularz z danymi, które umieszczone zostaną w przeniesionym certyfikacie.


Certum
Etykieta wirtualnej karty (Przyjazna nazwa)
Początek ważności certyfikatu
Język, w którym zostanie sporządzona umowa
Obywatelstwo
Dane wnioskodawcy
Dokument tożsamości wnioskodawcy
Dane kontaktowe wnioskodawcy
Dane podmiotu prawnego
Dane kontaktowe reprezentowanego podmiotu
Nazwa powszechnie stosowana
Siedziba główna podmiotu
Adres korespondencyjny
Typ karty
Wybór opiekuna klienta

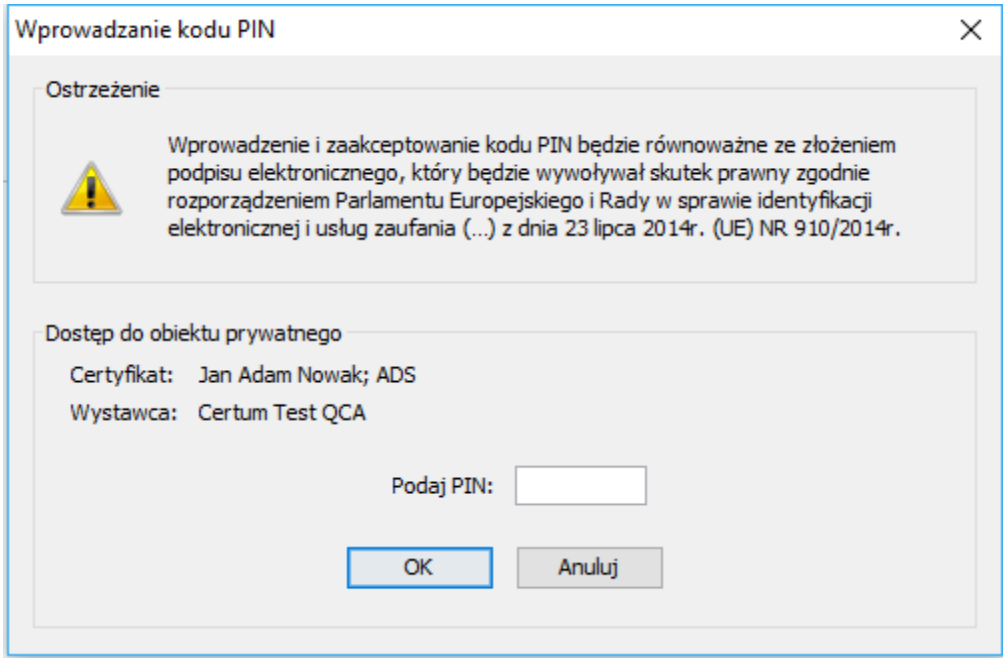
W formularzu z danymi należy **zaznaczyć zgodę na przetwarzanie danych** osobowych i nacisnąć przycisk **Dalej**. Wygenerowany zostanie aneks i załącznik do aneksu.



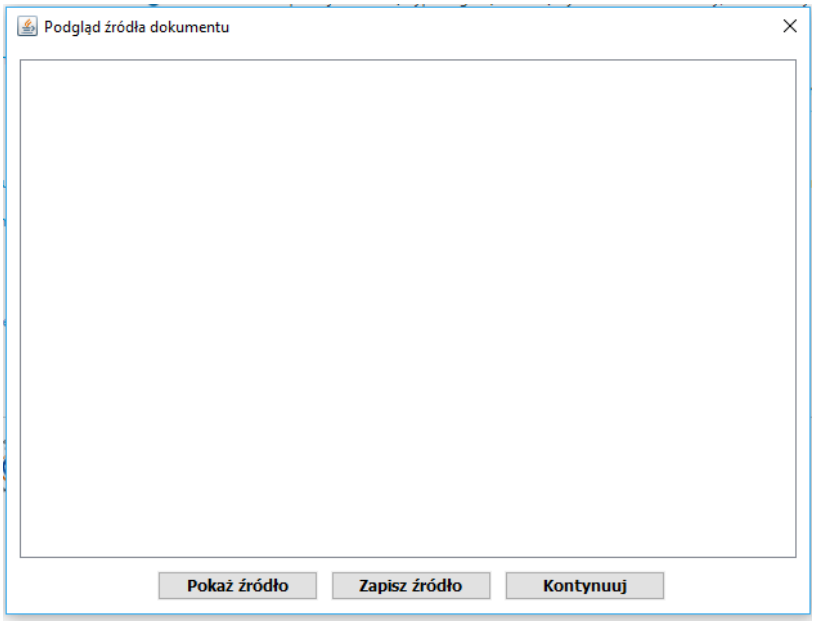
Należy nacisnąć przycisk **Przejdź do podpisania aneksu**. Rozpocznie się proces podpisywania wniosku o odnowienie i przeniesienie certyfikatu. Wyświetlone zostanie okno wyboru certyfikatu, którym zostanie podpisany aneks i załącznik do aneksu.



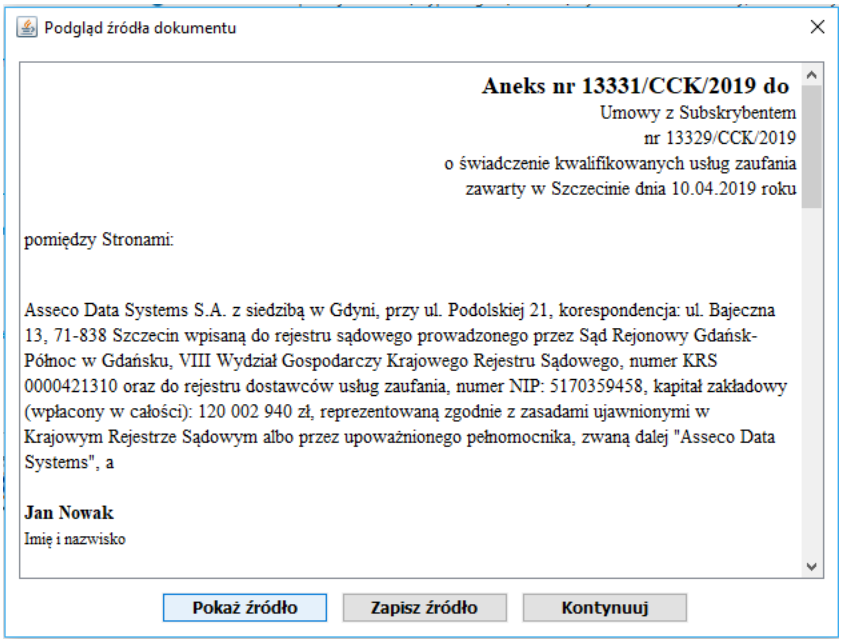
Należy wybrać certyfikat i nacisnąć przycisk **OK**. Wyświetlone zostanie okno, w którym należy wprowadzić **kod PIN** do karty.



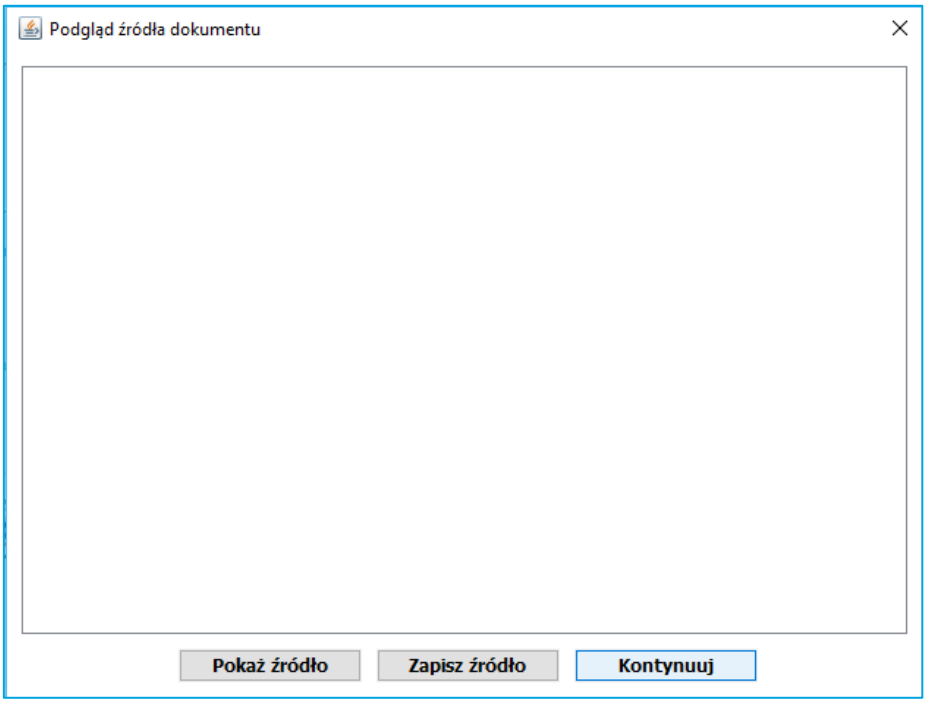
Po wprowadzeniu poprawnego kodu PIN do karty i jego zatwierdzeniu wyświetlone zostanie okno umożliwiające podgląd podpisywanego aneksu.



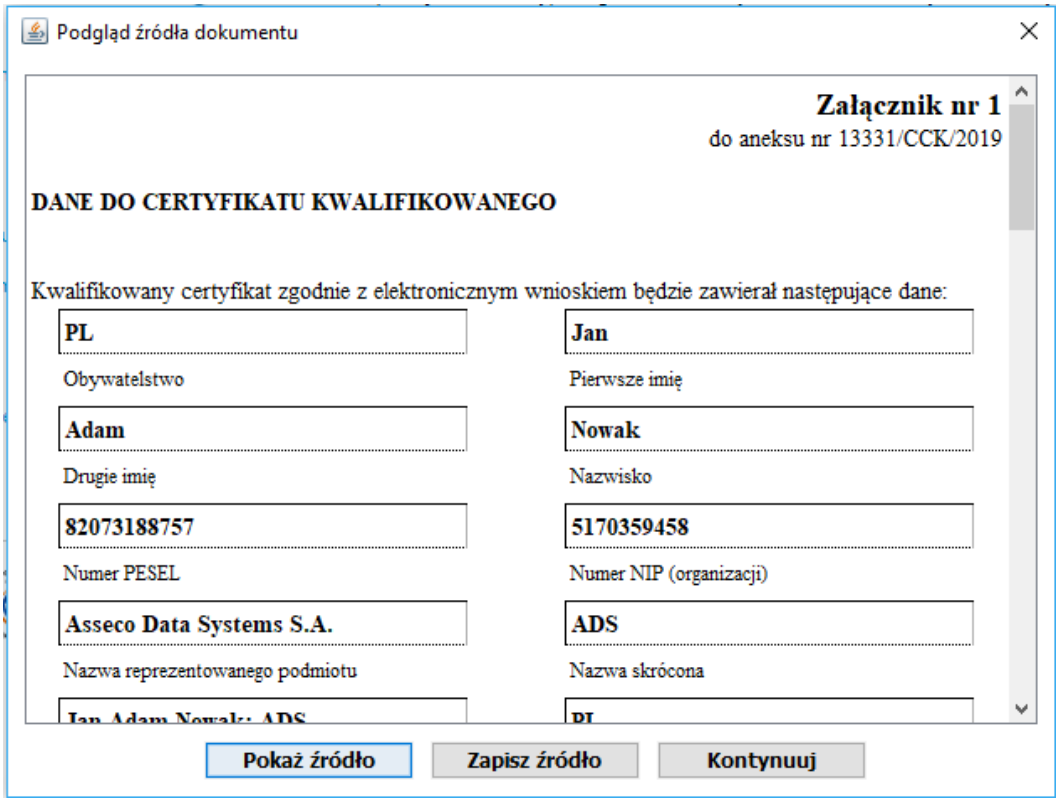
Należy nacisnąć przycisk **Pokaż źródło**. Wyświetlona zostanie treść podpisywanego aneksu.



Należy nacisnąć przycisk **Kontynuuj**. Wyświetlone zostanie okno umożliwiające podgląd podpisywanego załącznika



Należy nacisnąć przycisk **Pokaż źródło**. Wyświetlona zostanie treść podpisywanego załącznika.



Należy nacisnąć przycisk **Kontynuuj.** Wniosek o przeniesienie i odnowienie certyfikatu zostanie złożony. W tym momencie proces złożenia wniosku zostaje zakończony. Należy oczekiwać na kontakt ze strony Certum (informacja zostanie wysłana na adres email) i wydanie certyfikatu.