



# **Instrukcja przeniesienia certyfikatu kwalifikowanego z karty kryptograficznej na kartę wirtualną SimplySign**

**Wersja 2.2**



## Spis treści

1. Wstęp.....	3
2. Wymagania.....	3
3. Aktywacja usługi SimplySign.....	3
3.1 iOS.....	3
3.2 Android.....	12
4. Złożenie wniosku o przeniesienie certyfikatu .....	19

## 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

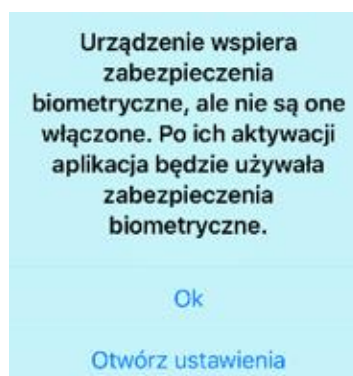
Aplikację **SimplySign** można pobrać z App Store (urządzenia z systemem iOS) oraz ze sklepu Google Play (urządzenia z systemem Android).

### 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.

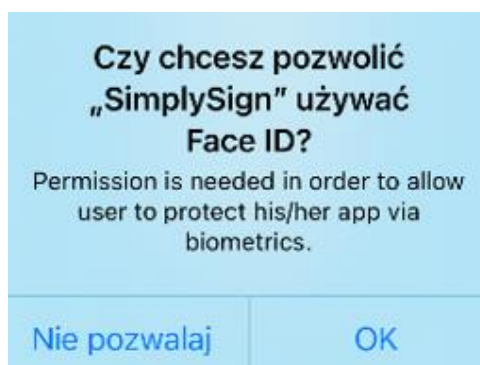
Zabezpieczenia biometryczne działają wg poniższej logiki:

- 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.

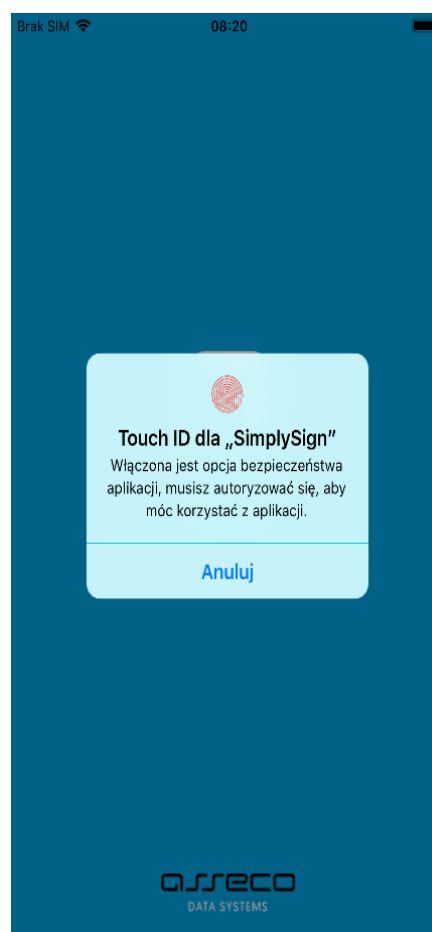


Po wybraniu **OK** aplikacja przejdzie do uwierzytelnienia.

Face ID:



Touch ID:



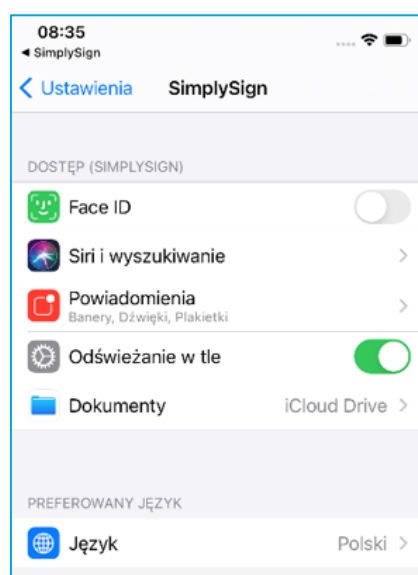
Jeżeli użytkownik wybierze opcję **Nie pozwalaj** (dla Face ID):



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**.



07:58

<

**Podaj adres e-mail**

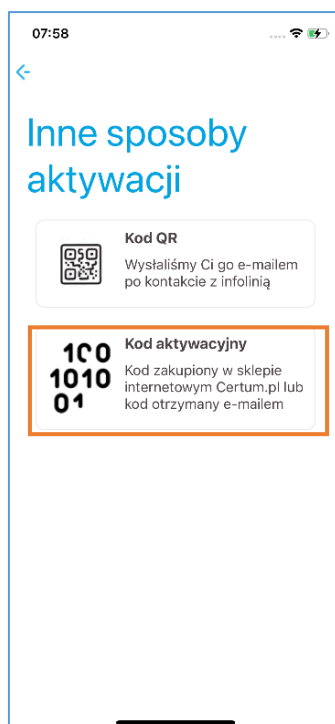
Powinien być to adres użyty podczas składania wniosku o certyfikat

E-mail

Dalej

Inne sposoby aktywacji

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



07:58

<

**Inne sposoby aktywacji**

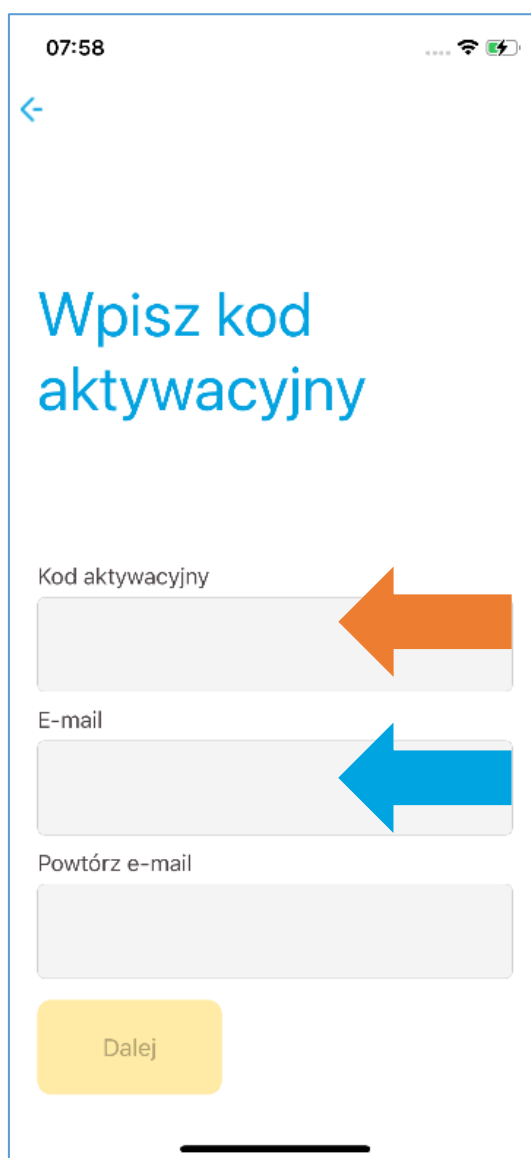
**Kod QR**  
Wysłaliśmy Ci go e-mailem po kontakcie z infolinią

**Kod aktywacyjny**  
1C0  
1010  
01  
Kod zakupiony w sklepie internetowym Certum.pl lub kod otrzymany e-mailem

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.



07:58

<

## Wpisz kod aktywacyjny

Kod aktywacyjny

E-mail

Powtórz e-mail

Dalej

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



Dostępne są dwa tryby:

- Podpisywanie i Generuj token – umożliwia podpisywanie dokumentów i jednocześnie 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.

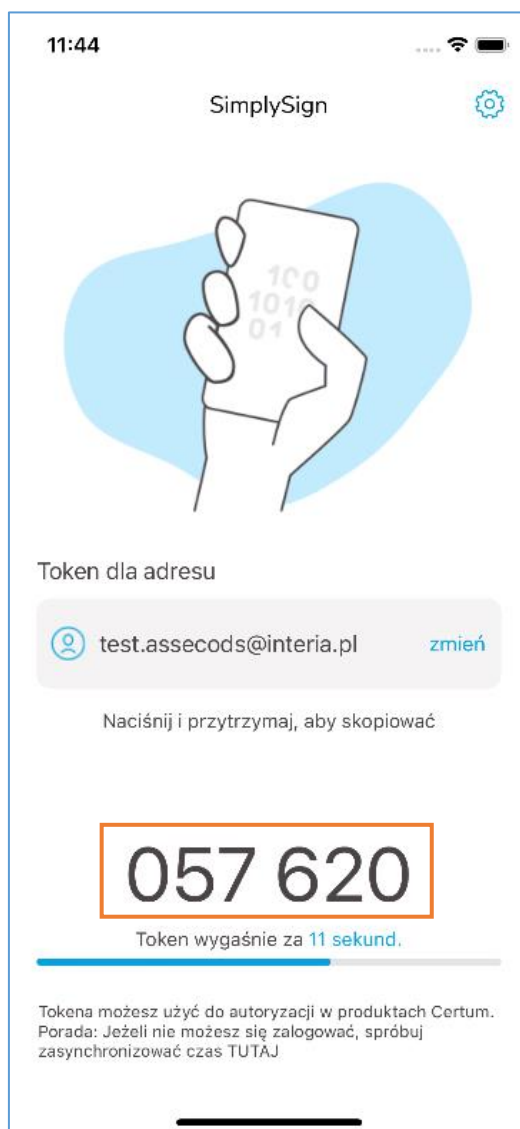


Po naciśnięciu przycisku **Zacznij podpisywać dokumenty** aplikacja przejdzie do ekranu startowego:



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

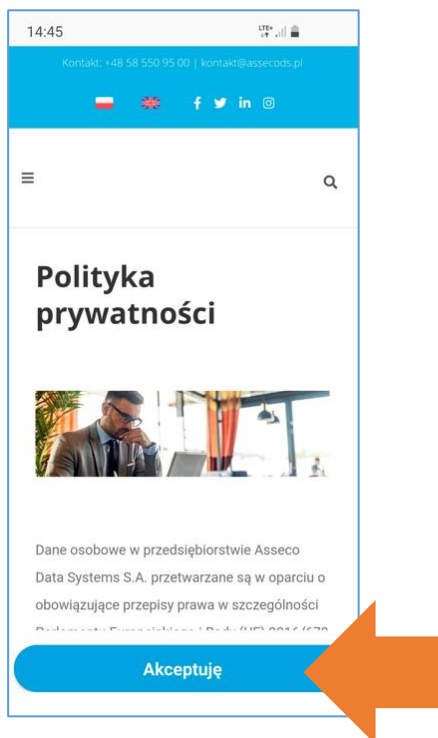
Nowy token generuje się co 30 sekund:



Po aktywacji aplikacji należy przejść do punktu 4 niniejszej instrukcji.

### 3.2 Android

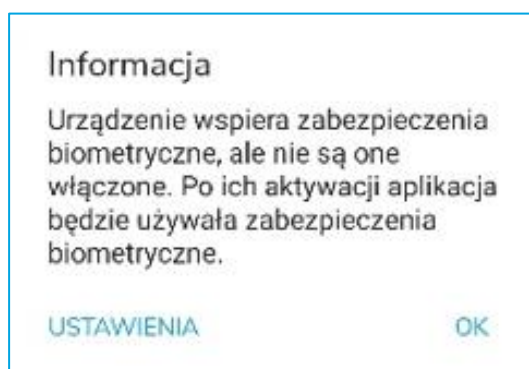
Przy pierwszym uruchomieniu aplikacji wymagane jest zapoznanie się z polityką prywatności i zaakceptowanie jej treści.



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:



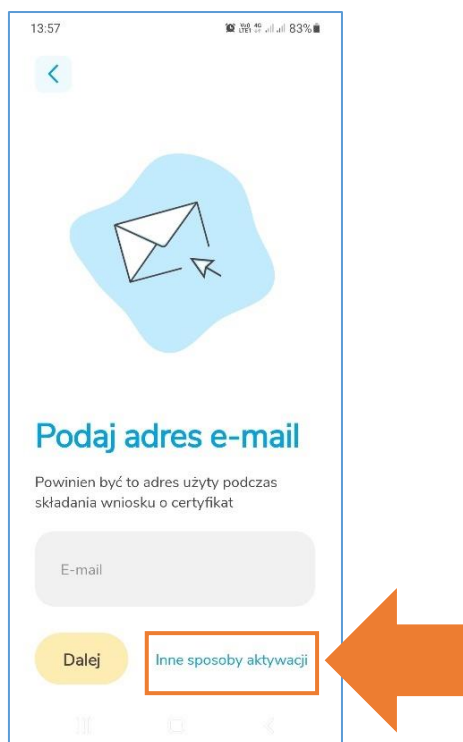
- B. W przypadku, gdy na urządzeniu włączone są zabezpieczenia biometryczne to przy uruchomieniu aplikacji pojawi się uwierzytelnianie wybranym zabezpieczeniem.



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.

13:57 83%

<

## Wpisz kod aktywacyjny

Kod aktywacyjny

E-mail

Powtórz e-mail

Dalej

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

Dostępne są dwa tryby:

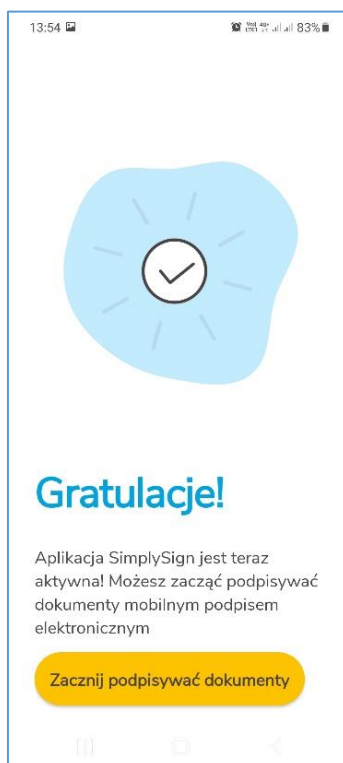
- Podpisywanie i Generuj token – umożliwia podpisywanie dokumentów i jednocześnie generowanie tokenów;
- Generuj token – umożliwia tylko generowanie tokena – wtedy podpisywanie trzeba będzie robić na innym urządzeniu.



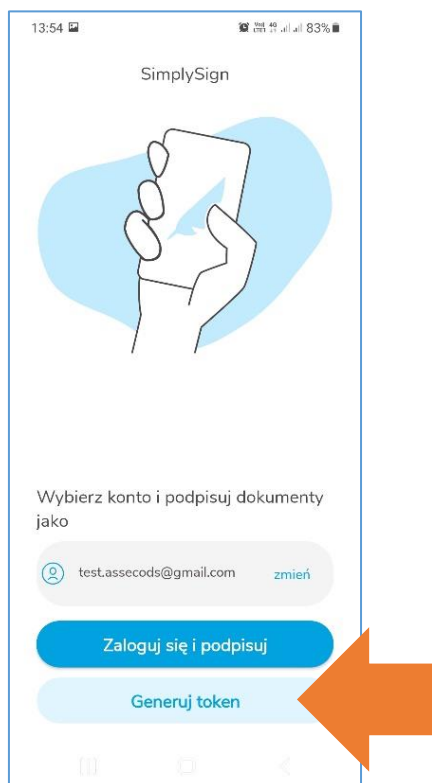
Po wybraniu trybu należy nacisnąć przycisk **Zakończ aktywację**.



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 punktu 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**.

**Certum**  
by ASSECO

English

Certyfikaty kwalifikowane > Odnowienie certyfikatu > Krok 1 z 5 - Logowanie

Wniosek o certyfikat kwalifikowany

Dokumenty formalne do umowy

Odnowienie certyfikatu

Instalacja certyfikatu

Powiadomienia e-mail

Wymiana karty kryptograficznej

Wsparcie techniczne

Wiedza

Odnowienie certyfikatu kwalifikowanego

1. Odnowienie certyfikatu kwalifikowanego dla: klasycznego e-podpisu / mobilnego e-podpisu w SimplySign (Instrukcja)

W celu rozpoczęcia aktywacji odnowienia certyfikatu kwalifikowanego należy pobrać i uruchomić aplikację Certum oraz aplikację JAVA, które wymagane są do odnowienia Twojego certyfikatu. Postępuj zgodnie z poniższą instrukcją:

1. Jeśli używasz usługi:

- a. Klasyczny e-podpis (fizyczna karta i czytnik) - umieść kartę kryptograficzną w czytniku kart.
- b. Mobilny e-podpis (usługa phmowa) - uruchom aplikację SimplySign Desktop i zaloguj się do usługi.

2. Sprawdź [www.certum.pl](http://www.certum.pl), czy posiadasz lub zainstalowałeś aplikację Sun Java Runtime Environment w aktualnie dostępnej wersji. Najnowszą wersję można pobrać ze strony: <http://java.com/pl>

**Pobierz aplikację Certum**

3. Poczekać aż automatycznie uruchomi się aplikacja Certum

4. Dokonać wyboru certyfikatu kwalifikowanego, który chcesz odnowić i kliknąć przycisk "OK" - automatycznie zostaną uzupełnione pola "Numer serijny certyfikatu" i "Numer karty"

5. Uzupełnić pozostałe wymagane pola: "Data urodzenia", "Miejsce urodzenia" oraz "Kod z obrazka" i kliknąć przycisk "Okaj"

Numer serijny certyfikatu\*

Numer karty\*

Data urodzenia\*

Miejsce urodzenia\*

Kod z obrazka\*

34v4qd

\* - pole wymagane

Na podstawie art. 38 ust. 1 pkt 1 ustawy z dnia 30 maja 2014 r. (Dz.U. z 2014 r. o prawach konsumenta) informujemy, że po udostępnieniu Klientowi przez Spółkę certyfikatu kwalifikowanego lub jego odnowienia, Klient traci prawo do odstąpienia od umowy zawartej na odległość.

**Certyfikaty Kwalifikowane od 18 czerwca 2018 roku**

Informujemy, iż od dnia **18 czerwca 2018 roku** certyfikaty kwalifikowane będą wydawane tylko w nowej strukturze SHA-2, zgodnie z rozporządzeniem eIDAS.

Wszystkie certyfikaty kwalifikowane wydane do 1 lipca 2018 roku w strukturze SHA-1 nie tracą swojej ważności po tej dacie, zachowując swoją ważność zgodnie z datą wskazaną w certyfikacie.

Dokumenty podpisane przed 1 lipca 2018 roku nie tracą swojej ważności po tej dacie.

Urzędy administracji publicznej mają obowiązek dostosowania i świadczenia usług w swoich systemach informacyjnych zgodnie z rozporządzeniem eIDAS. Zmiany nadzorowane są również przez Ministerstwo Cyfryzacji.

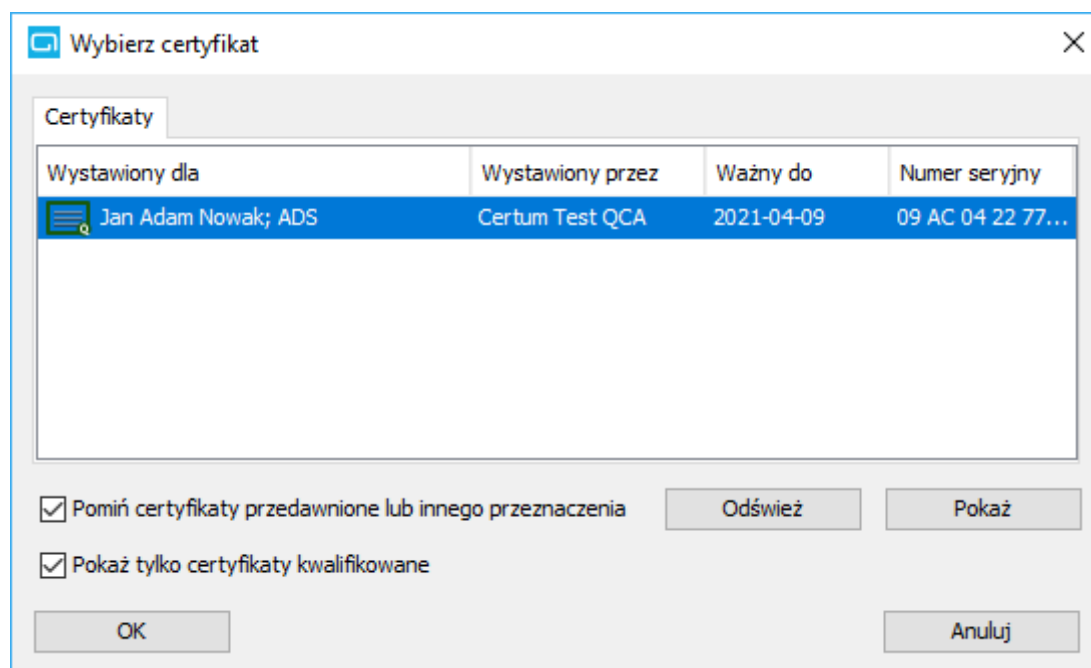
[Dowiedz się więcej >](#)

SHA-2 w instytucjach publicznych oraz prywatnych - [Dowiedz się więcej >](#)

[Dalej](#)



© 2018 Assoco Data Systems

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**.

Certyfikaty kwalifikowane > Odnowienie certyfikatu > Krok 1 z 5 - Logowanie

Wniosek o certyfikat kwalifikowany  
Dokumenty formalne do umowy  
Odnowienie certyfikatu  
Instalacja certyfikatu  
Powiadomienia e-mail  
Wymiana karty kryptograficznej  
Wsparcie techniczne  
Wiedza

### Odnowienie certyfikatu kwalifikowanego

**Odnowienie certyfikatu kwalifikowanego dla: klasycznego e-podpisu / mobilnego e-podpisu w SimplySign (instrukcja)**

W celu rozpoczęcia aktywacji odnowienia certyfikatu kwalifikowanego należy pobrać i uruchomić aplikację Certum oraz aplikację JAVA, które wymagane są do odnowienia Twojego certyfikatu. Postępuj zgodnie z poniższą instrukcją:

- Jeżeli używasz usługi:
  - Klasyczny e-podpis (fizyczna karta i czytnik) > umieść kartę kryptograficzną w czytniku kart.
  - Mobilny e-podpis (usługa chmurowa) > uruchom aplikację SimplySign Desktop i zaloguj się do usługi.
- Sprawdź ([sprawdź czy masz aplikację JAVA](#)), czy posiadasz lub zainstaluj aplikację **Sun Java Runtime Environment** w aktualnie dostępnej wersji. Najnowszą wersję można pobrać ze strony: <http://java.com/pl/>
- Pobierz Aplikację Certum wymaganą do odnowienia twojego certyfikatu

**Pobierz aplikację Certum**

- Uruchom pobrany plik: **aplikacja\_Certum.exe**
- Poczekaj aż automatycznie uruchomi się **aplikacja Certum**
- Dokonaj wyboru certyfikatu kwalifikowanego, który chcesz odnowić i wciśnij przycisk "OK" - automatycznie zostaną uzupełnione pola "Numer seryjny certyfikatu" i "Numer karty"
- Uzupełnij pozostałe wymagane pola: "Data urodzenia", "Miejsce urodzenia" oraz "Kod z obrazka" i wciśnij przycisk "Dalej"

Numer seryjny certyfikatu	12856210881978118666591691245078718927
Numer karty	4607119249675496
Data urodzenia	1982-07-31
Miejsce urodzenia	Szczecin
Kod z obrazka	qrkv7m

\* - pole wymagane

Na podstawie art. 38 ust. 1 pkt 1 ustawy z dnia 30 maja 2014 r. (Dz.U. z 2004 r. o prawach konsumenta) informujemy, że po udostępnieniu Klientowi przez Spółkę certyfikatu kwalifikowanego lub jego odnowienia, Klient traci prawo do odstąpienia od umowy zawartej na odległość.

**Certyfikaty Kwalifikowane od 18 czerwca 2018 roku**

Informujemy, iż od dnia **18 czerwca 2018** roku certyfikaty kwalifikowane będą wydawane tylko w nowej strukturze SHA-2, zgodnej z rozporządzeniem eIDAS.




Wszystkie certyfikaty kwalifikowane wydane do 1 lipca 2018 roku w strukturze SHA-1 nie tracą swojej ważności po tej dacie, zachowując swoją ważność zgodnie z datą wskazaną w certyfikacie.

Dokumenty podpisane przed 1 lipca 2018 roku nie tracą swojej ważności po tej dacie.

Urzędy administracji publicznej mają obowiązek dostosowania i świadczenia usług w swoich systemach informatycznych zgodnie z rozporządzeniem eIDAS. Zmiany nadzorowane są również przez Ministerstwo Cyfryzacji. [Dowiedz się więcej >](#)

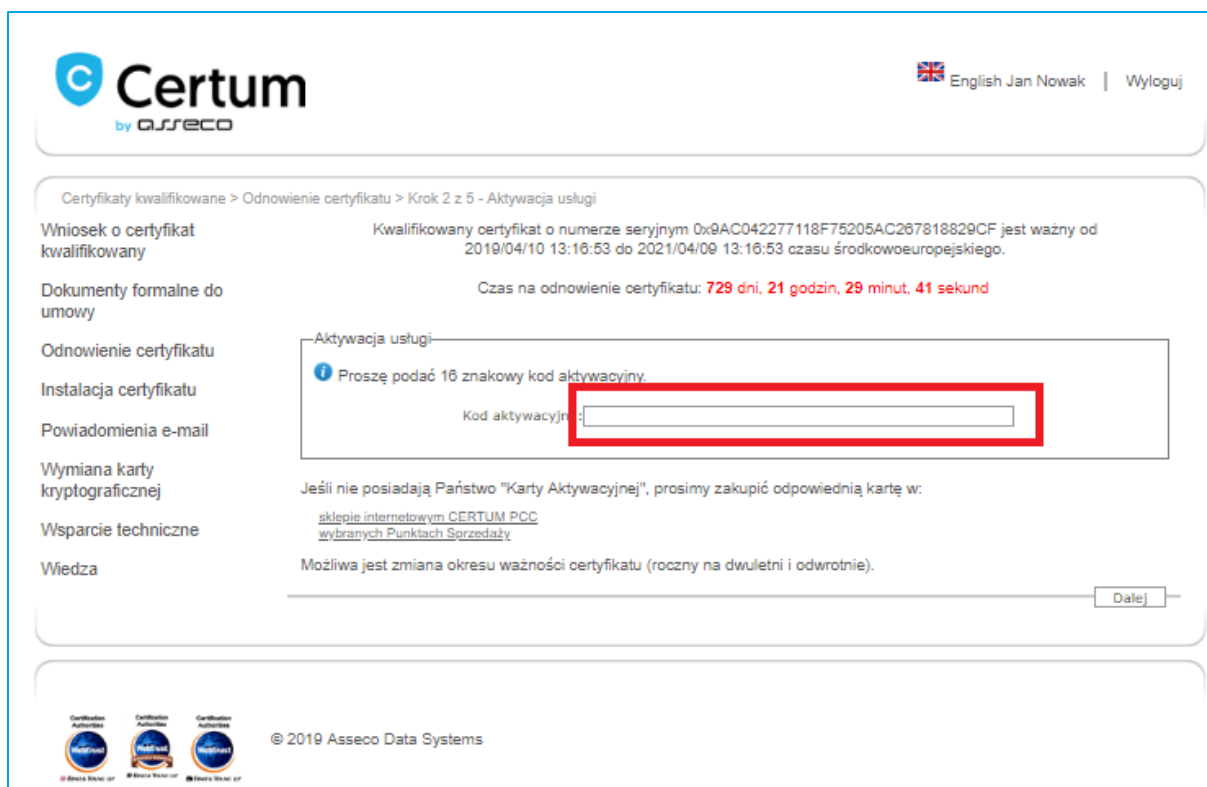
SHA-2 w instytucjach publicznych oraz prywatnych - [Dowiedz się więcej >](#)

**Dalej**

© 2019 Asseco Data Systems

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



Certyfikaty kwalifikowane > Odnowienie certyfikatu > Krok 2 z 5 - Aktywacja usługi

Wniosek o certyfikat kwalifikowany

Kwalifikowany certyfikat o numerze seryjnym 0x9AC042277118F75205AC267818829CF jest ważny od 2019/04/10 13:16:53 do 2021/04/09 13:16:53 czasu środkowoeuropejskiego.

Dokumenty formalne do umowy

Czas na odnowienie certyfikatu: **729 dni, 21 godzin, 29 minut, 41 sekund**

Odnowienie certyfikatu

Aktywacja usługi

Proszę podać 16 znakowy kod aktywacyjny.

Kod aktywacyjny:

Jeśli nie posiadają Państwo "Karty Aktywacyjnej", prosimy zakupić odpowiednią kartę w: [sklepie internetowym CERTUM PCC](#) [wybranych Punktach Sprzedaży](#)

Wymiana karty kryptograficznej

Wsparcie techniczne

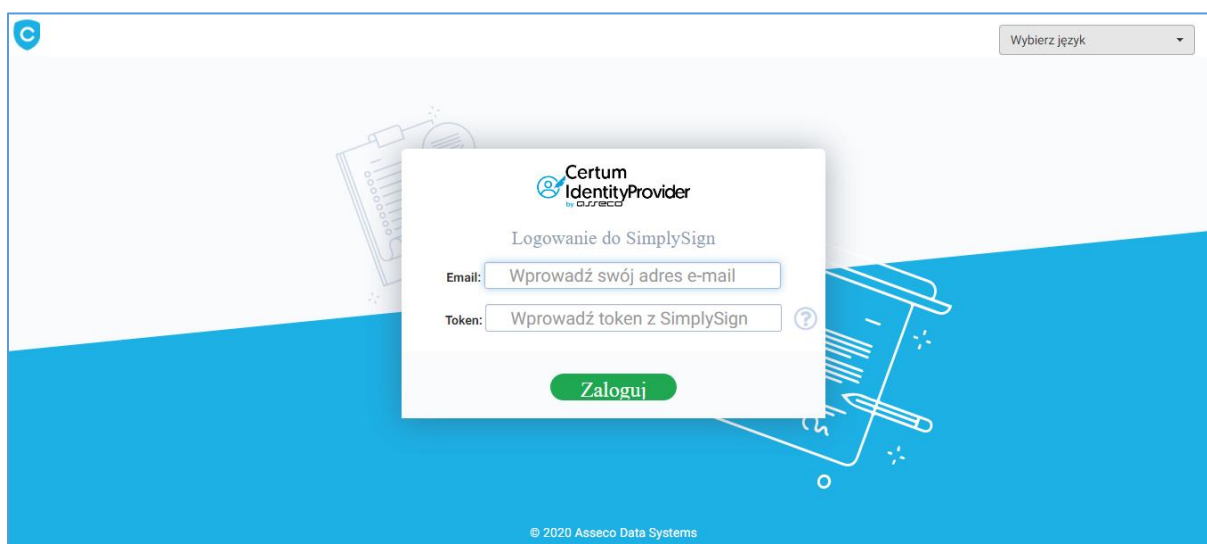
Wiedza

Możliwa jest zmiana okresu ważności certyfikatu (roczny na dwuletni i odwrotnie).

[Dalej](#)

© 2019 Asseco Data Systems

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



Certum IdentityProvider

Logowanie do SimplySign

Email:  Wprowadź swój adres e-mail

Token:  Wprowadź token z SimplySign

[Zaloguj](#)

© 2020 Asseco Data Systems

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.

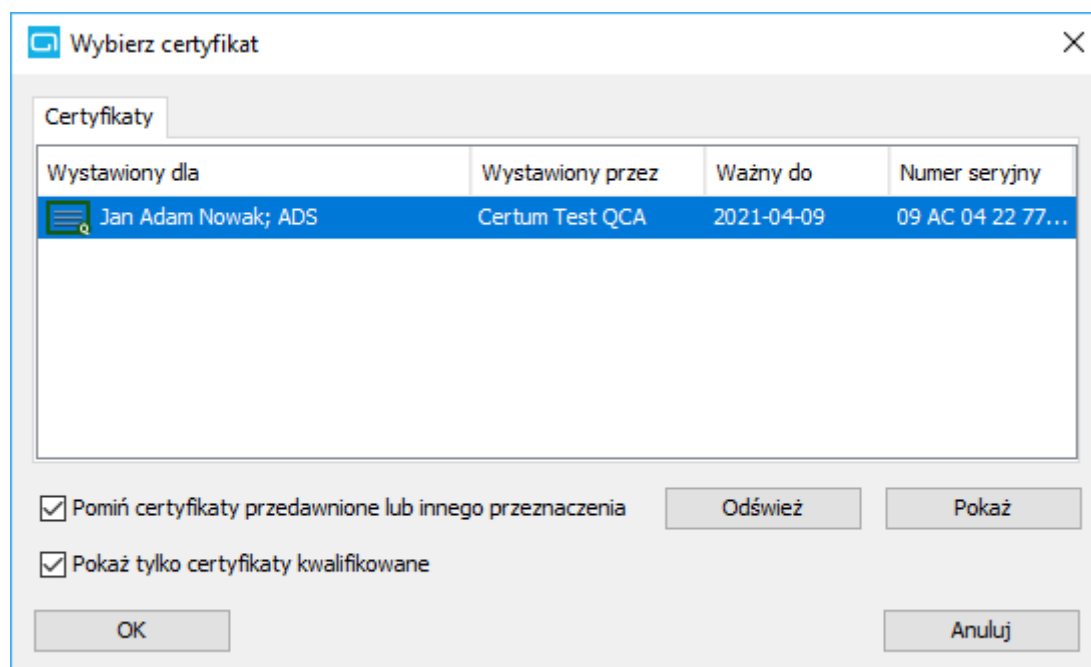
[illegible]

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

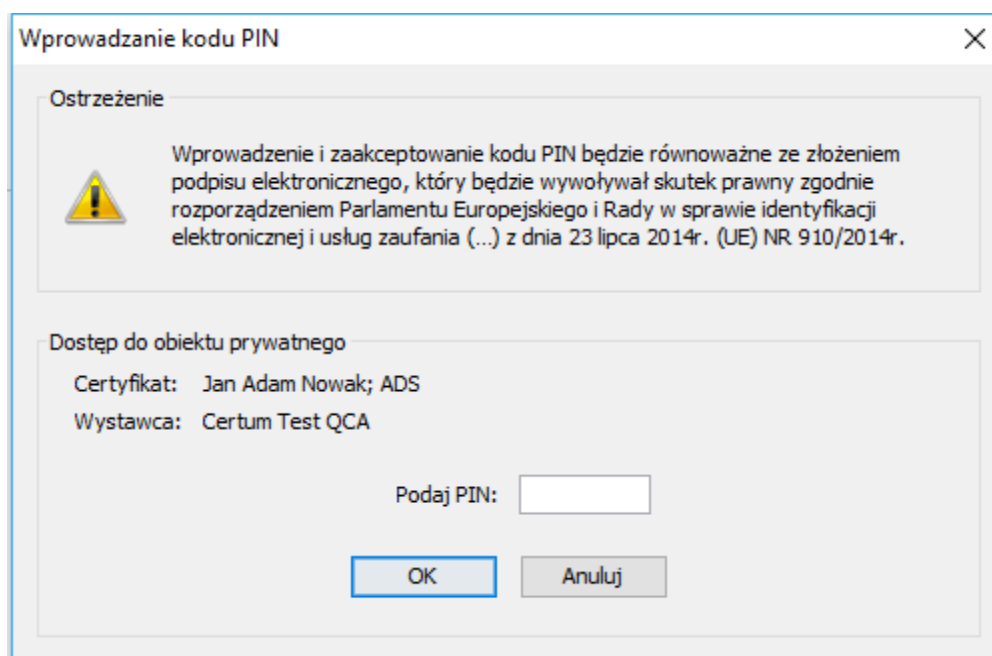
[illegible]

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.

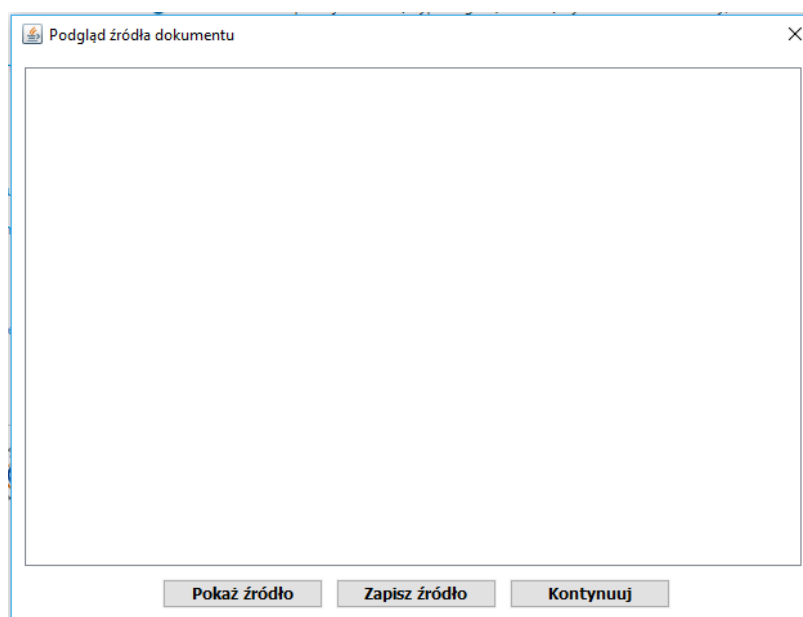




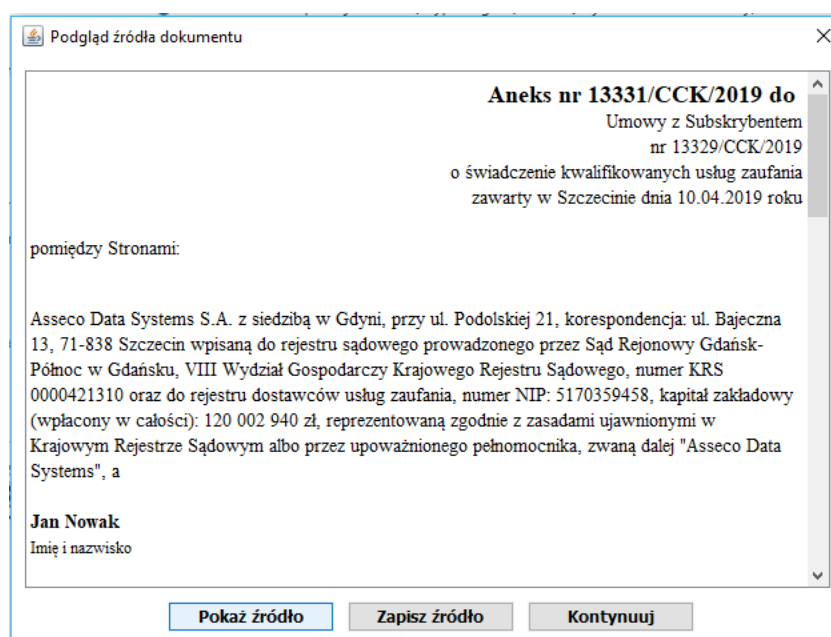
Należy wybrać certyfikat i nacisnąć przycisk **OK**. Wyświetlone zostanie okno, w którym należy wprowadzić **kod PIN** do karty.



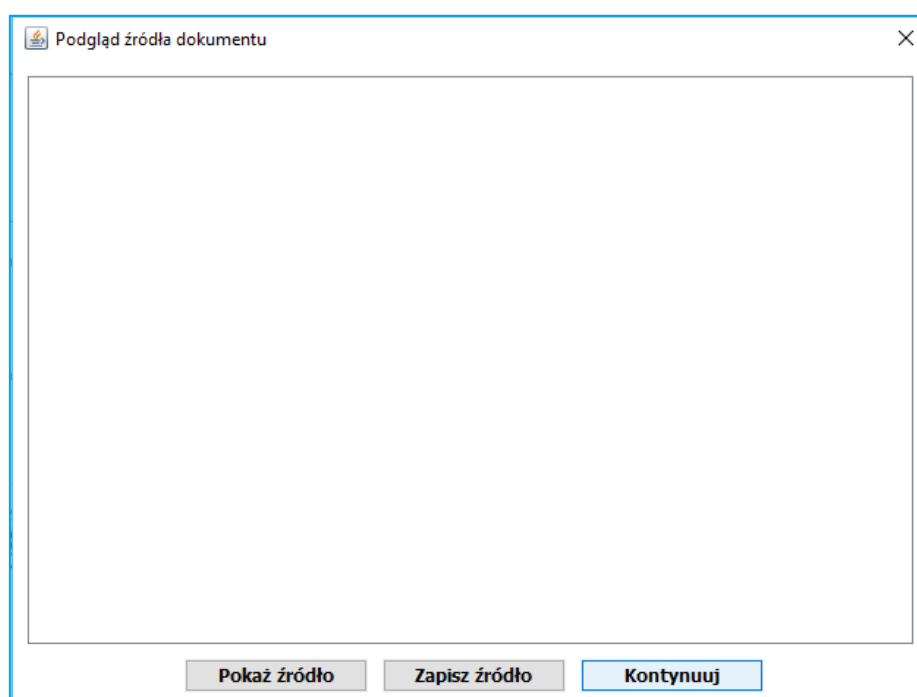
Po wprowadzeniu poprawnego kodu PIN do karty i jego zatwierdzeniu wyświetlone zostanie okno umożliwiające podgląd podpisywanego aneksu.



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



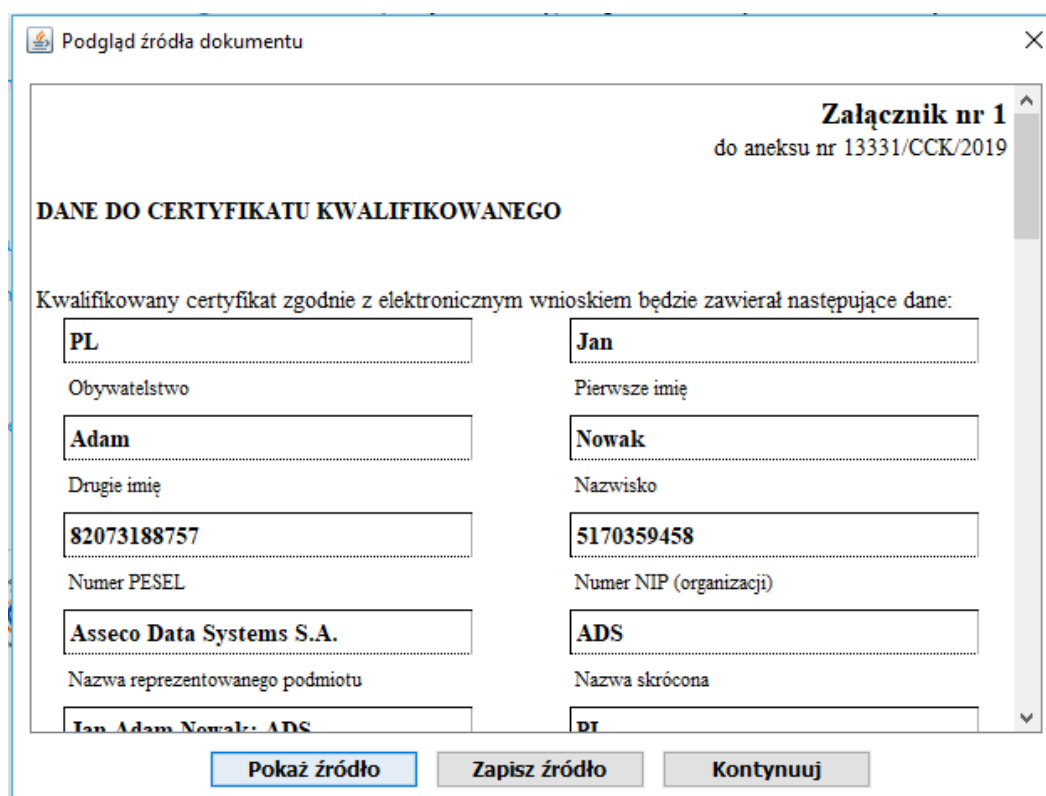
Należy nacisnąć przycisk **Kontynuuj**. Wyświetlone zostanie okno umożliwiające podgląd podpisywanego załącznika



Podgląd źródła dokumentu

Pokaż źródło Zapisz źródło Kontynuuj

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



Podgląd źródła dokumentu

**Załącznik nr 1**  
do aneksu nr 13331/CCK/2019


**DANE DO CERTYFIKATU KWALIFIKOWANEGO**


Kwalifikowany certyfikat zgodnie z elektronicznym wnioskiem będzie zawierał następujące dane:

PL	Jan
Obywatelstwo	Pierwsze imię
Adam	Nowak
Drugie imię	Nazwisko
82073188757	5170359458
Numer PESEL	Numer NIP (organizacji)
Asseco Data Systems S.A.	ADS
Nazwa reprezentowanego podmiotu	Nazwa skrócona
Jan Adam Nowak: ADS	pr

Pokaż źródło Zapisz źródło Kontynuuj

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.



 English / Jan Nowak / Wyloguj

[Certyfikaty kwalifikowane](#) / [Aktywacja karty](#) / [Podsumowanie](#)

[Wniosek o certyfikat kwalifikowany](#)  
[Dokumenty formalne do umowy](#)  
[Odnowienie certyfikatu](#)  
[Instalacja certyfikatu](#)  
[Powiadomienia e-mail](#)  
[Wymiana karty kryptograficznej](#)  
[Wsparcie techniczne](#)  
[Wiedza](#)

## Dziękujemy!

Proces składania wniosku o odnowienie certyfikatu kwalifikowanego został zakończony.




Najpóźniej w ciągu 7 dni roboczych od momentu wpłynięcia poprawnie podpisanych elektronicznie dokumentów do Certum, zostanie wydany odnowiony certyfikat kwalifikowany, który będzie można pobrać drogą elektroniczną na posiadaną kartę kryptograficzną. Informacja o wydaniu certyfikatu kwalifikowanego oraz instrukcja dalszego postępowania zostanie przekazana drogą elektroniczną.

W wiadomości zawarty będzie także adres, przez który będzie możliwość pobrania podpisanego obustronnie Aneksu do Umowy z Subskrybentem.

W przypadku jakichkolwiek pytań prosimy o kontakt z Operatorem naszej Infolinii.

Jesteśmy do Państwa dyspozycji w dniach roboczych, w godzinach 7.00 - 17.00 pod numerami telefonów:  
 0 801 540 340\* (dla połączeń z tel. stacjonarnych)  
 +48 91 4801 340\* (dla połączeń z tel. komórkowych)  
 e-mail: infolinia@certum.pl

\* - stawka za minutę połączenia zgodnie z cennikiem operatora

© 2019 Asseco Data Systems