



WARMIŃSKI BANK SPÓŁDZIELCZY

## Instrukcja używania aplikacji e-podpis (SCSA)

### Wstęp

W bankowości elektronicznej dla Klientów Korporacyjnych wprowadzona została metoda uwierzytelniania i autoryzacji z użyciem karty mikroprocesorowej przez aplikację e-Podpis (SCSA). Aplikacja e-Podpis (SCSA) zastępuje wykorzystanie apletów Java opartych o technologię NPAPI. Pozwala na podpisywanie dyspozycji przy korzystaniu z większości przeglądarek internetowych: Internet Explorer, Edge, Mozilla FireFox, Chrome. Zmianie uległ proces uwierzytelniania i autoryzacji polegający na dodaniu aplikacji e-Podpis (SCSA).

### Oprogramowanie

Dla korzystania z aplikacji e-Podpis (SCSA) należy zainstalować Java lub **JAVA Web Start Client** (plik do pobrania ze strony Banku) umożliwiające komunikację systemu z czytnikami kart mikroprocesorowych zapewniające funkcjonalność autoryzacji z pominięciem apletu Java. Oprogramowanie wymaga zainstalowanej Javy na komputerze użytkownika, które można pobrać ze strony producenta firmy Oracle. Oprogramowanie jest przydatne/niezbędne do uruchomienia aplikacji Asseco e-Podpis z **pliku launch.jnlp** (plik do pobrania ze strony Banku lub ze strony <https://scsa.cui.pl/webstart>).

Jeżeli na komputerze zainstalowane jest środowisko JAVA firmy Oracle, to program Java Web Start jest zainstalowany domyślnie i nie są już wymagane żadne czynności dodatkowe.

Biorąc pod uwagę, że licencja środowiska JAVA firmy Oracle stała się płatna powyżej wersji (java 1.8\_202), zaleca się instalację oprogramowanie JAVA Web Start Client, zawierające darmowe otwarte środowisko Java (Open JDK) oraz komponent IcedTea do obsługi technologii JAVA Web Start.

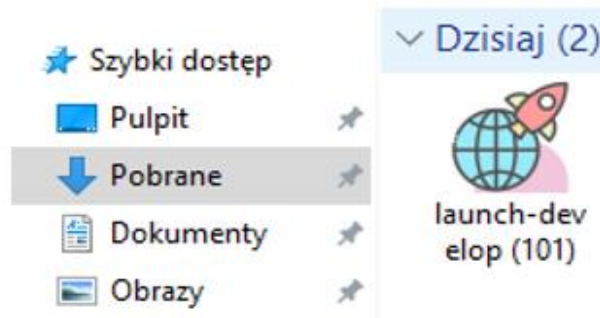
Z metody uwierzytelniania e-Podpis, można korzystać:

- poprzez jednorazowe zainstalowanie aplikacji na komputerze i późniejsze uruchamianie jej ze skrótu na pulpicie
- każdorazowe uruchamianie aplikacji z pozycji bankowości elektronicznej (klawisz [Uruchom aplikację SCSA]). Aplikacja e-Podpis SCSA wymaga zainstalowanej wersji Javy (min. 1.8\_144) lub JAVA Web Start Client.

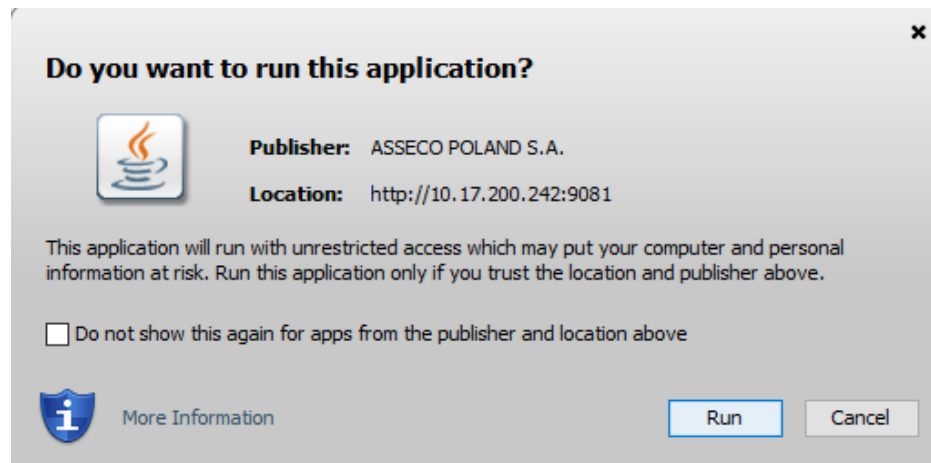
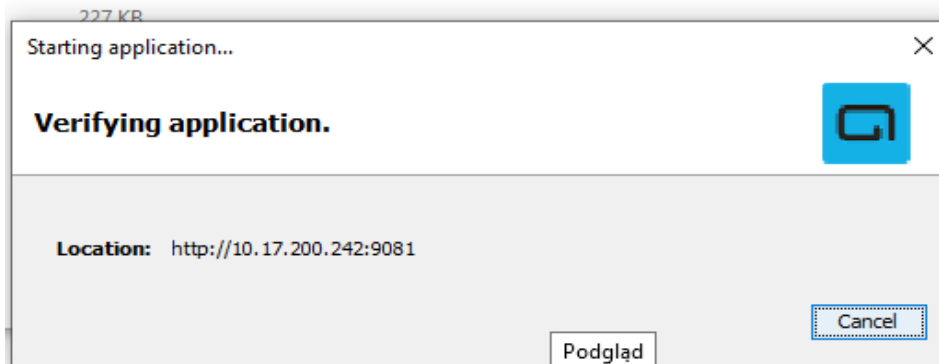
## Zmiana metody logowania i autoryzacji z apletu Java na e-Podpis- czynności do wykonania przed migracją, ale po wykonanej przez Bank zmianie metody logowania i autoryzacji

Dla klientów, którzy używają obecnie autoryzacji lub logowania do aplikacji z wykorzystaniem karty mikroprocesorowej apletu java **zmiana na nową metodę wymaga weryfikacji poprawności działania aplikacji e-podpis**. W tym celu należy:

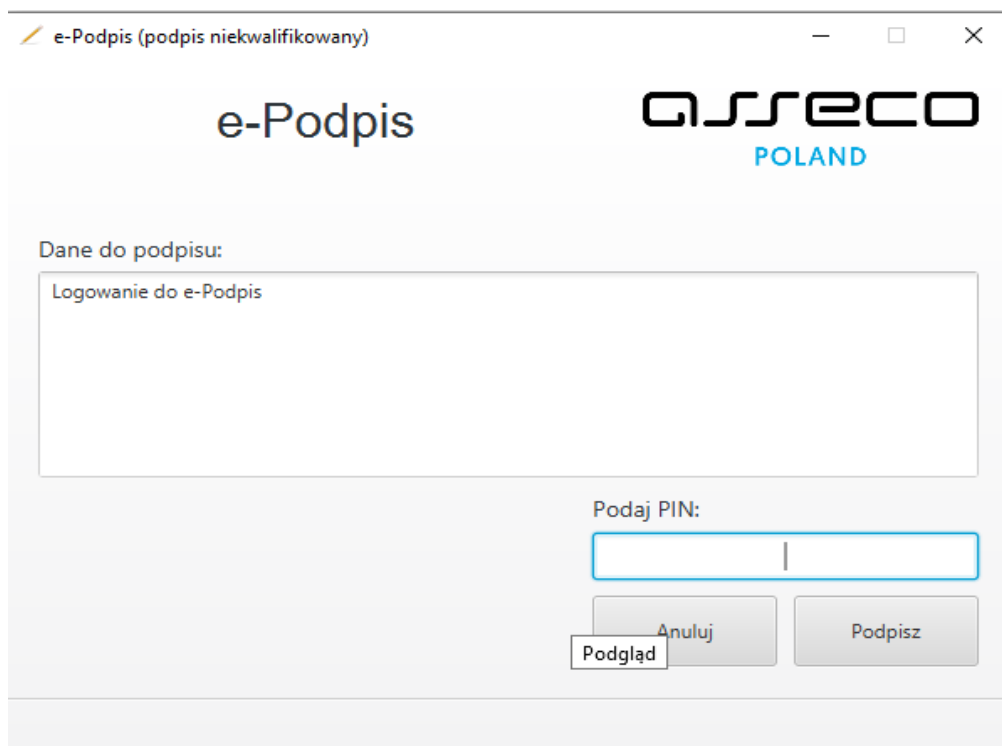
- wywołać pobranie aplikacji „**launch.jnlp**” ze strony Banku lub z linku <https://scsa.cui.pl/webstart>



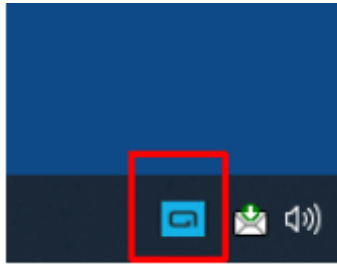
- uruchamiać aplikacje e-Podpis przechodząc przez poszczególne kroki jej wywołania,



- zalogować się do e-Podpisu używając obecnej kart mikroprocesorowej i PIN.



Zalogowanie do e-Podpisu jest sygnalizowane niebieską ikonką w zasobniku systemowym (na zrzucie ekranu oznaczona czerwonym kwadratem).



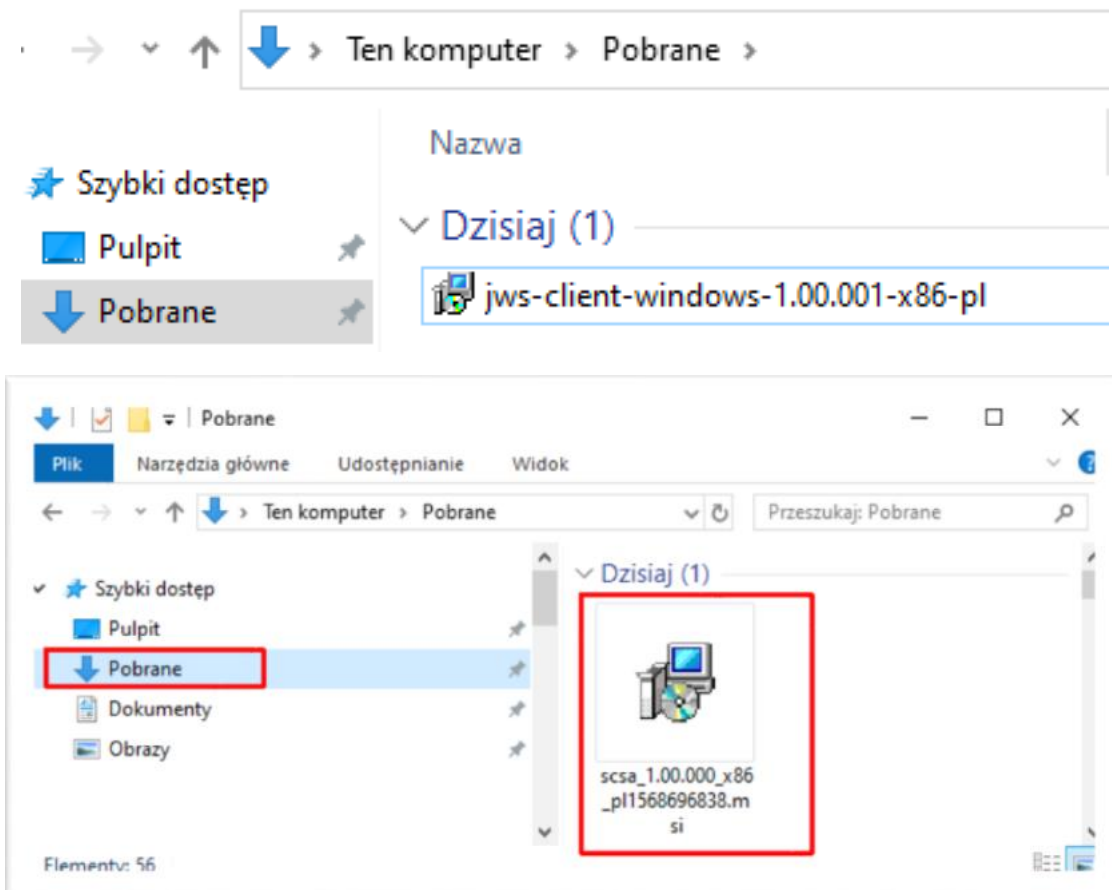
W przypadku braku możliwości zalogowania się do aplikacji e-Podpis lub nie pojawienia się e-Podpisu należy pobrać i wysłać logi do banku w celu dalszej diagnostyki:

- logi aplikacji e-Podpis – po pobraniu aplikacji zostaje utworzona struktura (katalog), w którym znajdują się pliki konfiguracyjne oraz logi z działania aplikacji (np. c:\Users\imie.nazwisko\.scsa\cui\).

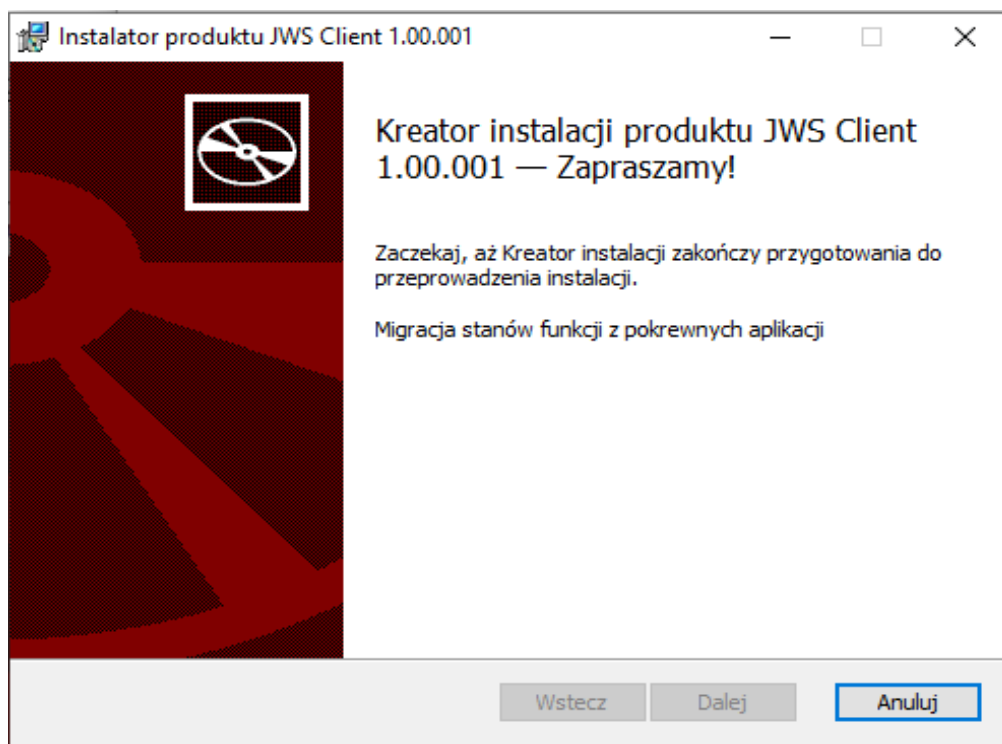
## Instalacja oprogramowanie Java (Open JDK) oraz komponentu IcedTea

W celu zainstalowania aplikacji JAVA Web Start Client należy:

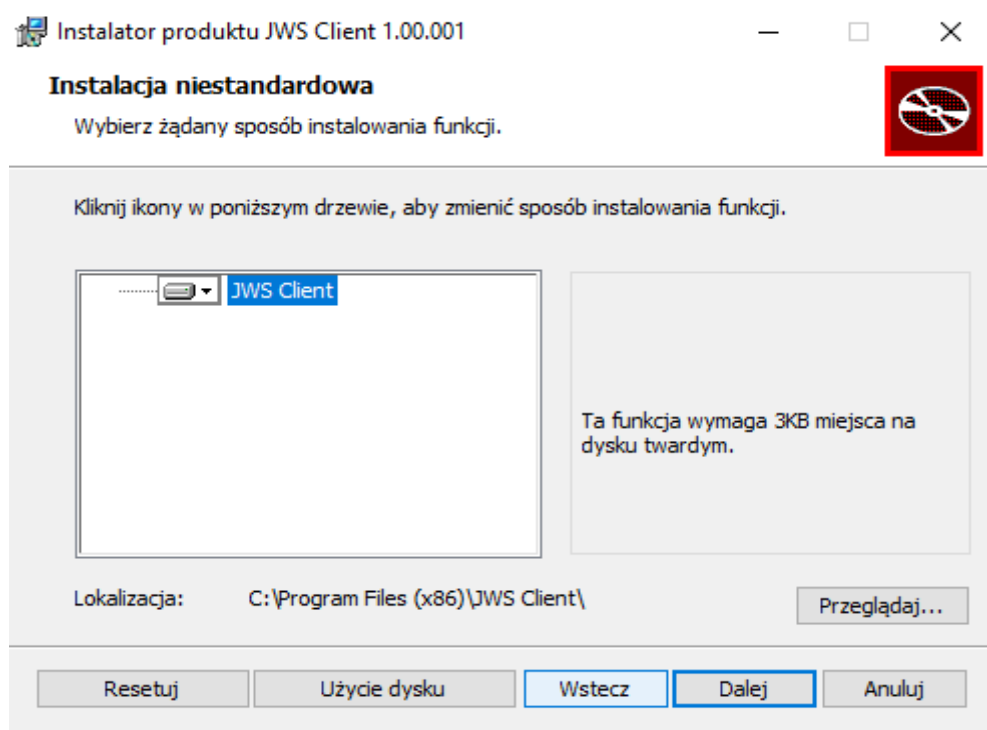
Plik dostarczony przez Bank (jws-client-windows-1.00.001-x86-pl.msi) lub starszy (jws-client-windows-1.00.000-x86-pl.msi) – oprogramowanie JAVA Web Start Client, zawierające otwarte środowisko Java (Open JDK) oraz komponent IcedTea do obsługi technologii JAVA Web Start.



Uruchomić pobrany plik MSI (domyślnie jest zapisywany w folderze „Pobrane”).

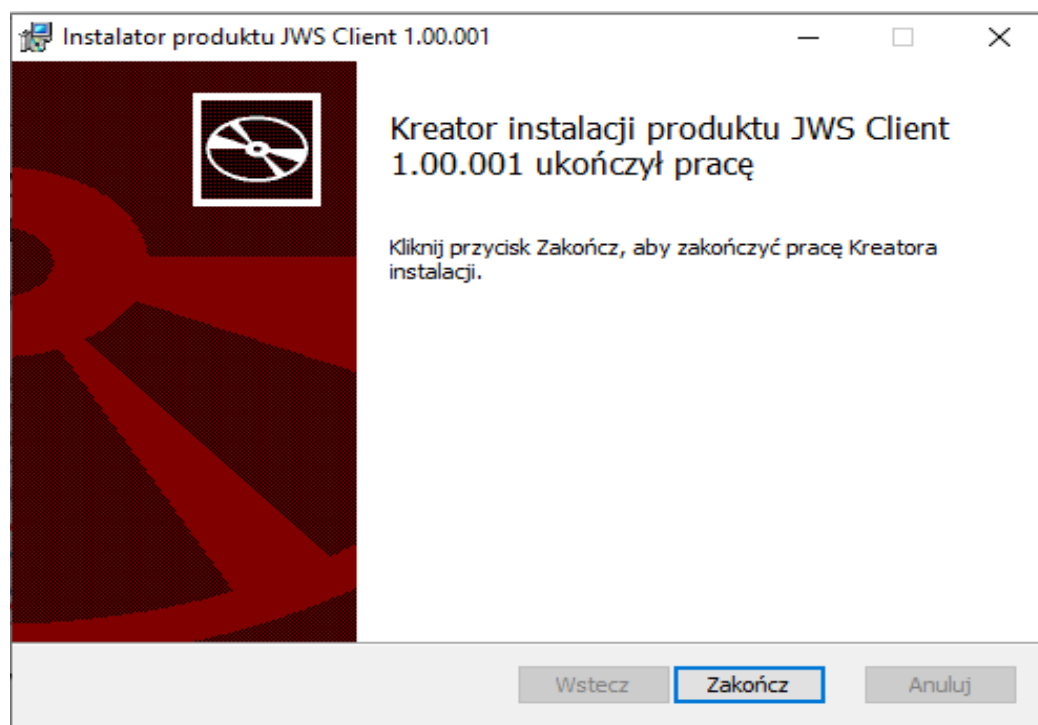
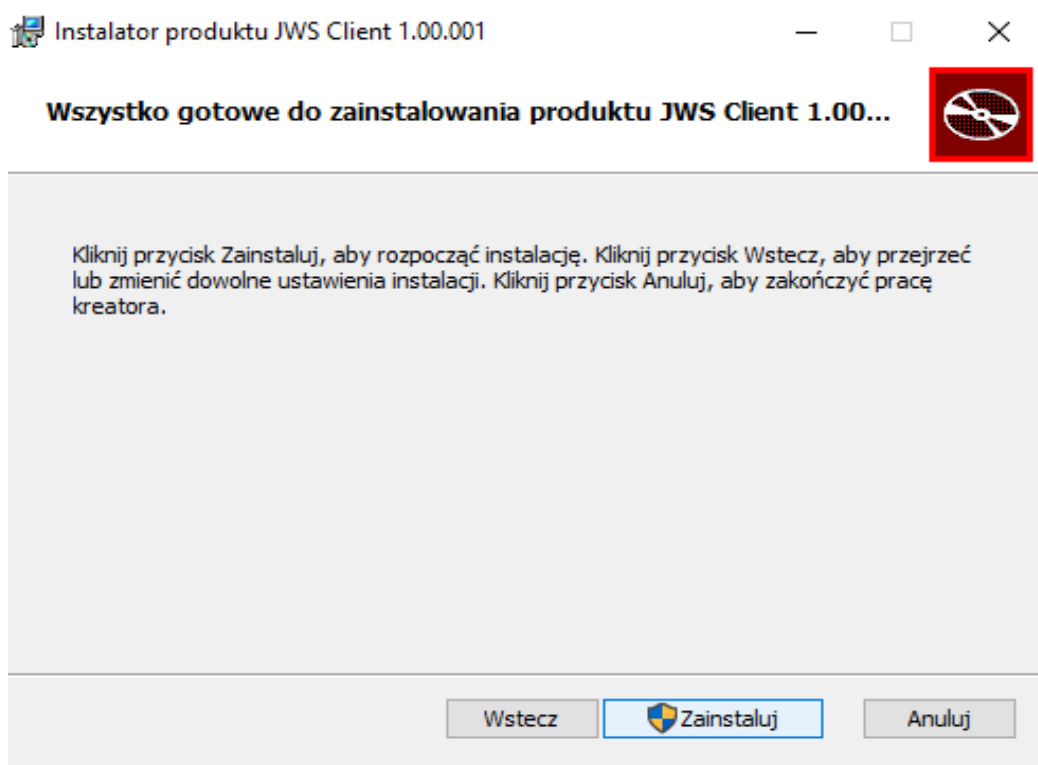


W kolejnym oknie (Instalacja niestandardowa) nic nie zmieniać i nacisnąć „Dalej”.

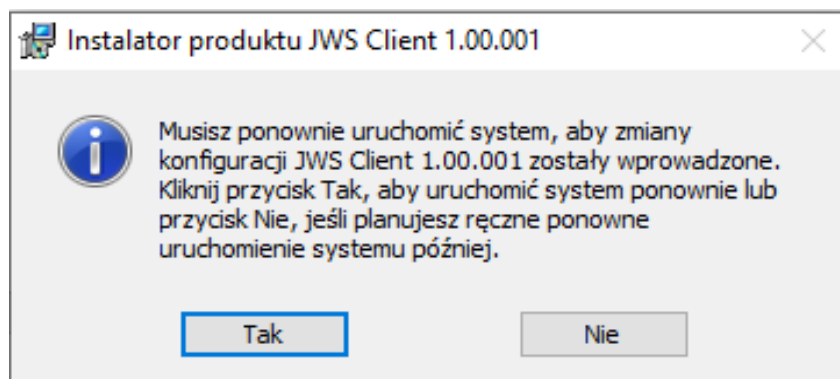


W następnym oknie, informującym, że wszystko jest gotowe do instalacji – nacisnąć „Zainstaluj”.

W oknie z informacją o zakończeniu instalacji nacisnąć „Zakończ”.



Wyświetlony zostanie komunikat o konieczności ponownego uruchomienia komputera – zatwierdzić przyciskiem „Tak”.



Po ponownym uruchomieniu komputera system jest gotowy do pracy.

## Pobieranie i zapis na dysku aplikacji e-Podpis (SCSA)

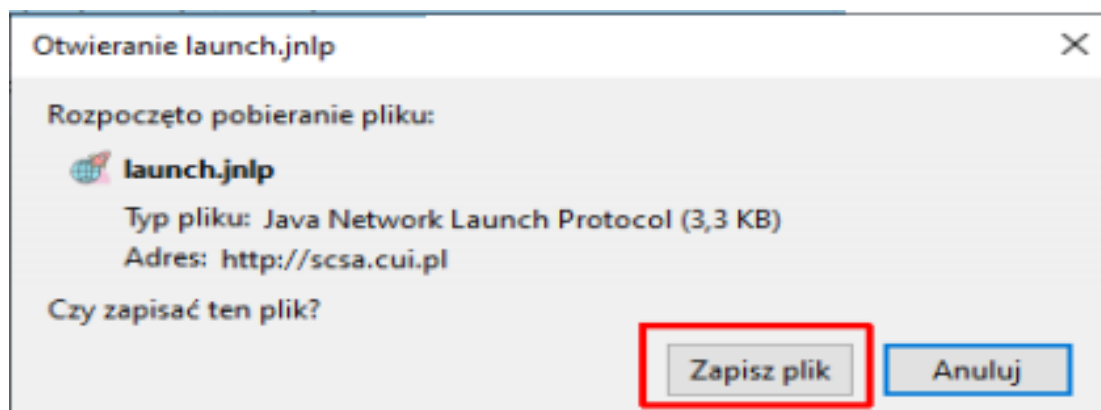
Aplikacje e-Podpis SCSA można pobrać z bankowości elektronicznej poprzez przycisk do uruchomienia (na formatce przelewu), lub z linku <https://scsa.cui.pl/webstart> lub ze strony Banku:

- Launch.jnlp - aplikacja Asseco e-Podpis dla użytkowników korporacyjnych korzystających z bankowości internetowej, potrzebna m.in. do odblokowania kodu PIN karty mikroprocesorowej.

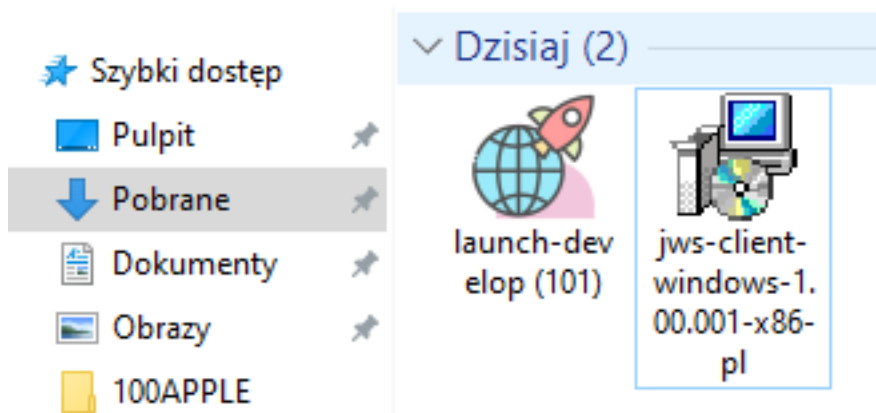
Instalacja skrótu na pulpicie wymaga uruchomienia pobranej aplikacji. Podczas instalacji, w zależności od posiadanej wersji Javy, pojawia się komunikat ostrzegający o otwarciu komponentu Javy



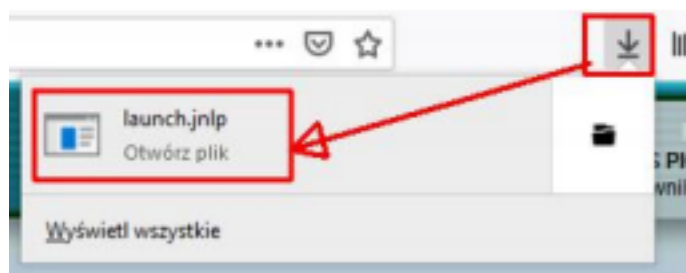
lub jest zapisywany (domyślnie w folderze „Pobrane”)



wówczas należy uruchomić pobrany plik z folderu „Pobrane”



lub jeśli jest taka możliwość to uruchomić go z poziomu przeglądarki.

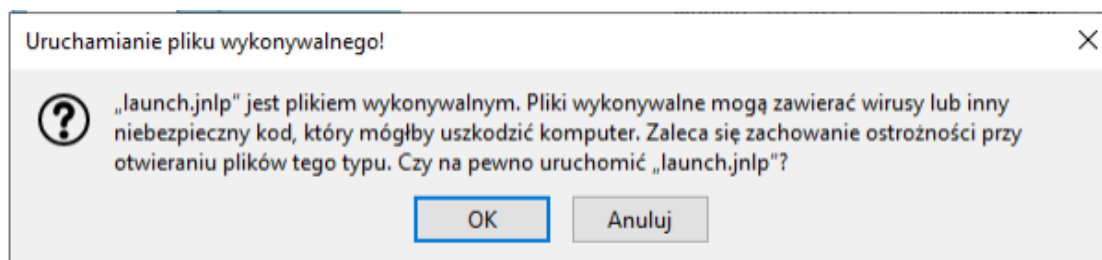
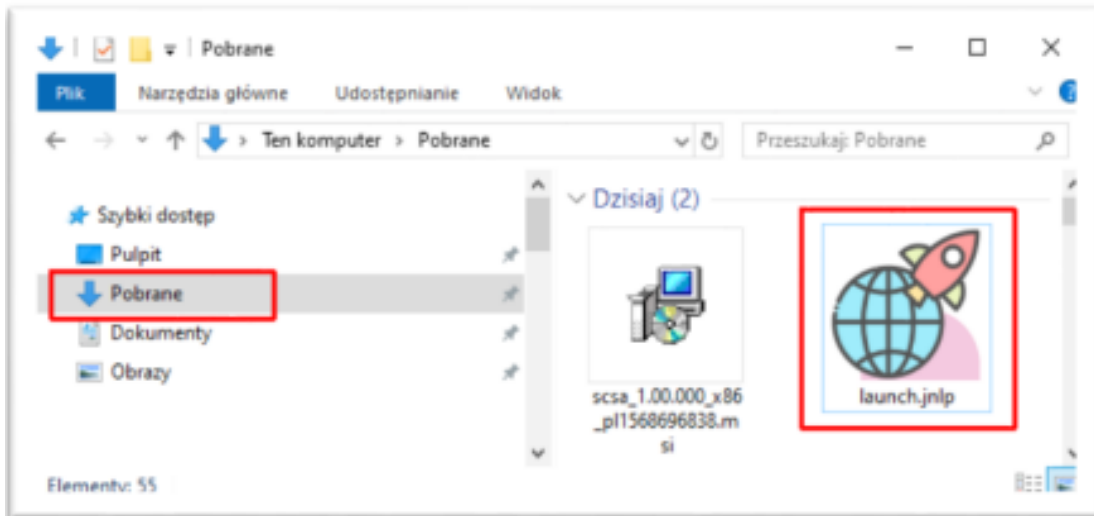


## Uruchomienie aplikacji e- Podpis z wykorzystaniem oprogramowania JWS Client lub Javy.

Dla wersji aplikacji jws-client-windows-1.00.001-x86-pl.msi po uruchomieniu launch-jnlp proces będzie przebiegał:

1. Po kliknięciu w ikonę pojawi się ostrzeżenie o uruchamianiu pliku wykonywalnego „**launch.jnlp**” – należy potwierdzić przyciskiem „OK”.



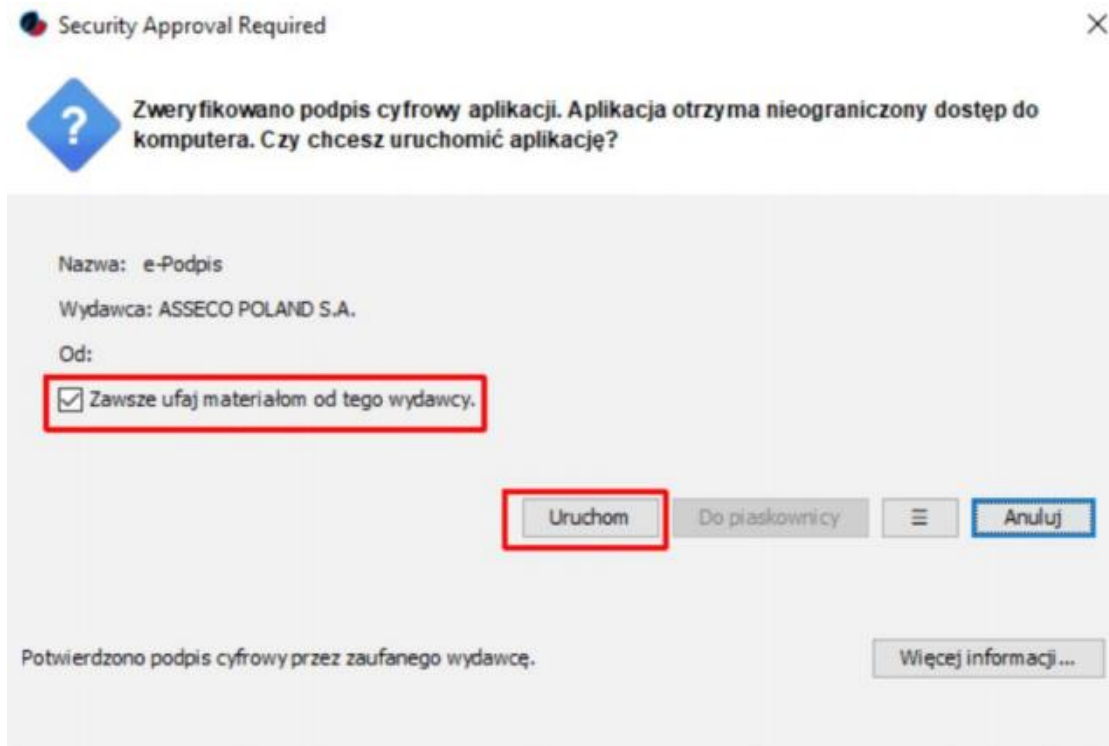


## 2. Uruchomiony zostaje e-Podpis przy pomocy JWS Client

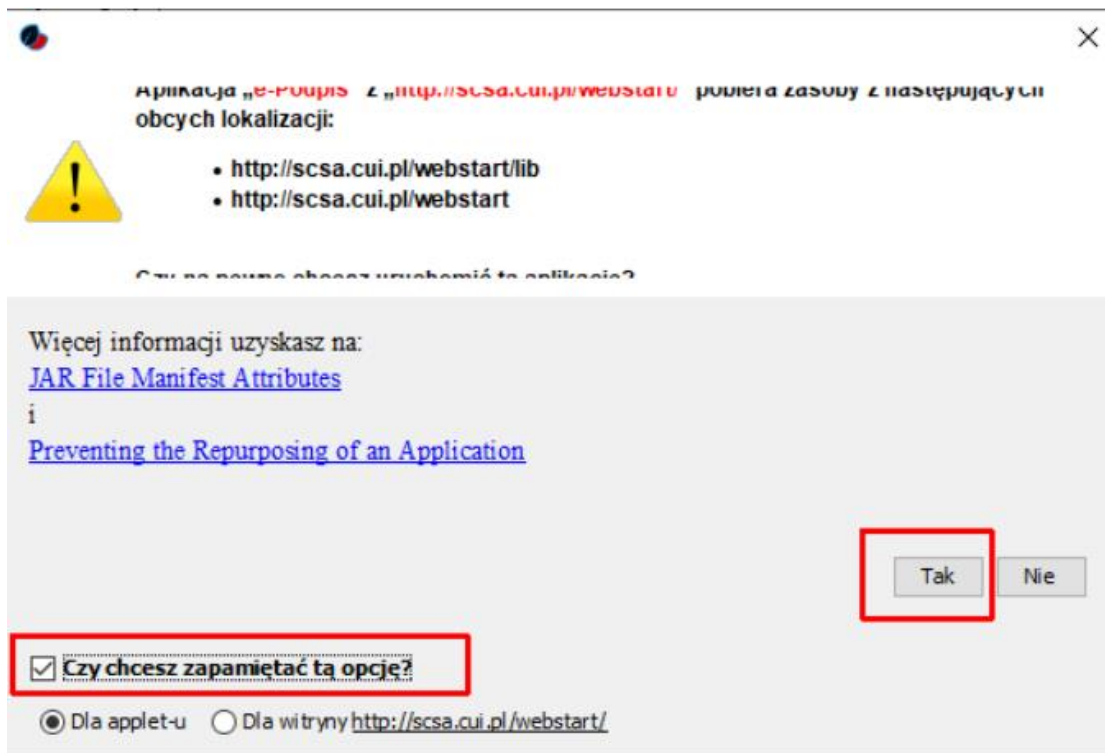


w wersji (jws-client-windows-1.00.001-x86-pl.msi) ekran nie jest prezentowany.

3. Wyświetlone zostanie okno zabezpieczeń „Security Approval Required”, w którym jest informacja „Nazwa: e-Podpis” i „Wydawca: ASSECO POLAND S.A.” – należy zaznaczyć „Zawsze ufaj materiałom od tego wydawcy” (czyli zapamiętanie danych jako zaufanych), a następnie nacisnąć przycisk „Uruchom”.



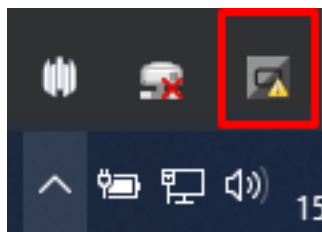
4. W kolejnym oknie wyświetlana jest informacja o pobieraniu przez e-Podpis danych z <https://scsa.cui.pl/webstart/lib> i <https://scsa.cui.pl/webstart> - należy zaznaczyć checkbox „Czy chcesz zapamiętać tę opcję” i następnie nacisnąć przycisk „Tak”.



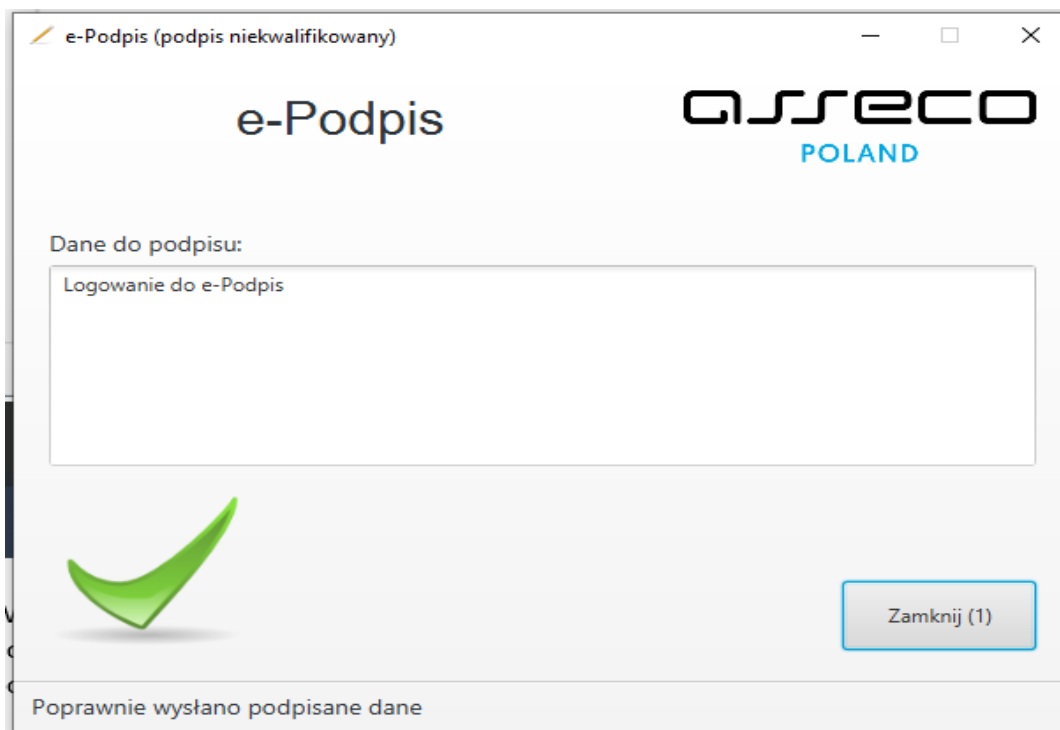
5. Opcje z punktu 3 i 4 powinny pojawić się tylko przy pierwszym uruchamianiu, jeśli zaznaczono „Zawsze ufaj materiałom od tego wydawcy” i „Czy chcesz zapamiętać tę opcję” tak jak opisano powyżej, to informacje zostaną zapamiętane.
6. Należy następnie włożyć kartę do czytnika i zalogować się do e-Podpisu wpisując PIN karty mikroprocesorowej.



7. Przed zalogowaniem do aplikacji SCSA jej ikona znajdująca się w zasobniku jest szara (na zrzucie ekranu oznaczona czerwonym kwadratem):

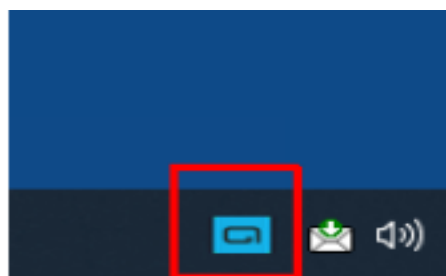


8. W oknie dialogowym „Dane do podpisu” pojawi się komunikat „Logowanie do e-Podpis”  
Prawidłowe podanie kodu PIN powoduje zalogowanie do bankowości elektronicznej i pojawienie się komunikatu „Poprawnie wysłano podpisane dane”.



9. Powyższe okno dialogowe można zamknąć po kliknięciu na klawisz „Zamknij” lub poczekać, aż zostanie zamknięte samoczynnie po upływie 3 sekund.

Zalogowanie do e-Podpisu jest sygnalizowane niebieską ikonką w zasobniku systemowym (na zrzucie ekranu oznaczona czerwonym kwadratem)

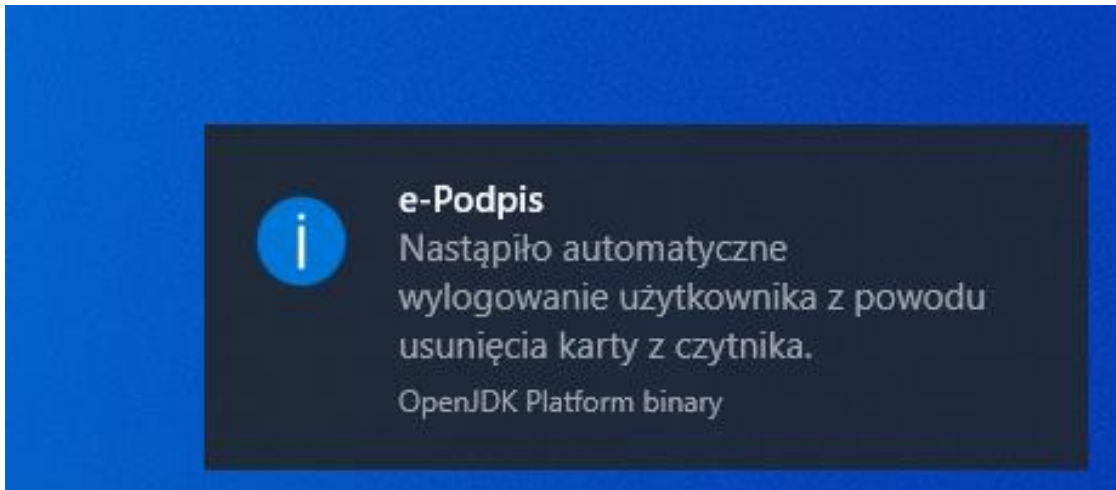


#### Warning

Ważne zalecenia bezpieczeństwa.

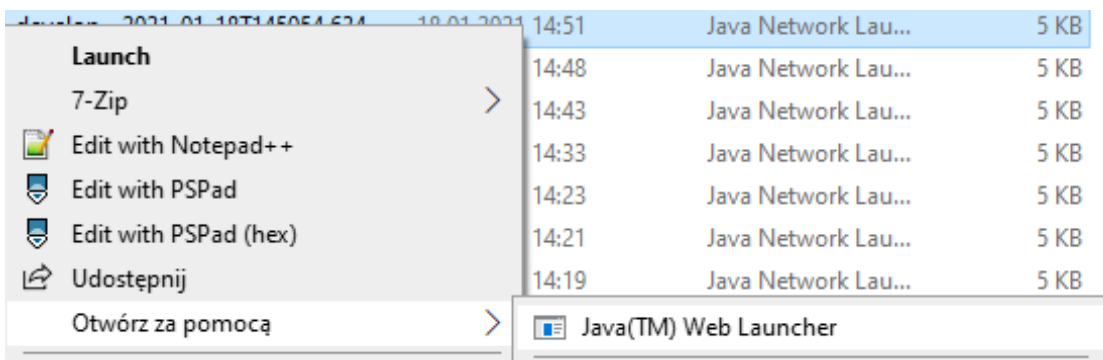
Kartę mikroprocesorową wkładamy do czytnika kart wyłącznie w momencie procesu logowania lub autoryzacji dyspozycji. Nie jest zalecane, aby karta mikroprocesorowa znajdowała się przez cały czas w czytniku.

Wyciągnięcie karty mikroprocesorowej z czytnika kart powoduje, wylogowanie z aplikacji e-Podpis, gdzie Użytkownik pozostaje w dalszym ciągu zalogowany do bankowości elektronicznej.



Ikona na pasku narzędzi zmienia się na kolor szary. Dodatkowo prezentowany jest komunikat: „Nastąpiło automatyczne wylogowanie użytkownika z powodu usunięcia karty z czytnika. Włożenie karty do czytnika, gdy aplikacja e-Podpis działa w tle, spowoduje automatyczne wywołanie okna do zalogowania się do aplikacji e-Podpis.

10. Uruchamianie aplikacji „**launch.jnlp**” za pomocą Java.



Po uruchomieniu aplikacji przy pomocy Java, system wyświetli okno, w którym będzie zaprezentowane okno do weryfikacji danych.



po poprawnej weryfikacji zaprezentuj się okno „Logowanie do e-Podpis”.

## Obsługa e-Podpisu

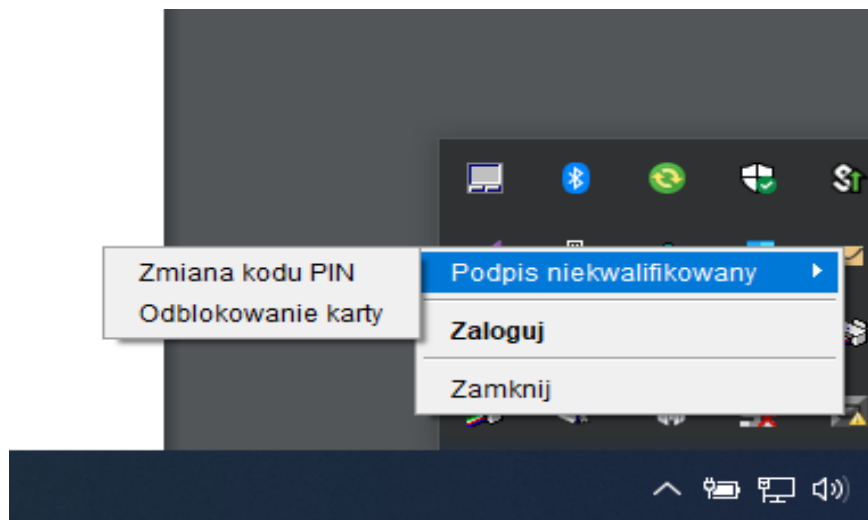
Jeśli aplikacja została już wcześniej uruchomiona to w zasobniku systemowym wyświetlana jest jej ikon, która umożliwia:

a) Podpis niekwalifikowany:

- zmianę kodu PIN karty,
- odblokowanie karty w przypadku jej zablokowania,

b) zalogowanie się,

c) zamknięcie aplikacji e-Podpis.



Użycie klawisza:

- **Zamknij** - powoduje zamknięcie aplikacji e-Podpis
- **Wyloguj/Zaloguj** - powoduje możliwość zalogowania/wylogowania do aplikacji e-Podpis. Automatyczne wylogowanie uzyskuje się również poprzez wyciągnięcie karty mikroprocesorowej z czytnika.
- **Zmiana kodu PIN** – umożliwia zmianę kodu PIN z poziomu aplikacji e-Podpis bez konieczności logowania się do bankowości elektronicznej

Zmiana kodu PIN

Stary kod PIN:

Nowy kod PIN:

Powtórz kod PIN:

Zmień

- **Odblokowanie karty** – umożliwia odblokowanie karty mikroprocesorowej po podaniu kodu PUK z poziomu aplikacji e-Podpis bez konieczności logowania się do bankowości elektronicznej

Odblokowanie karty

Kod PUK:

Nowy kod PIN:

Powtórz kod PIN:

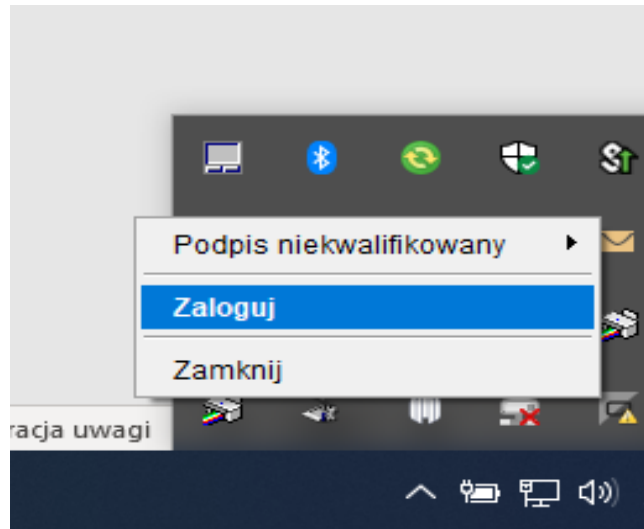
Odblokuj

**Note**

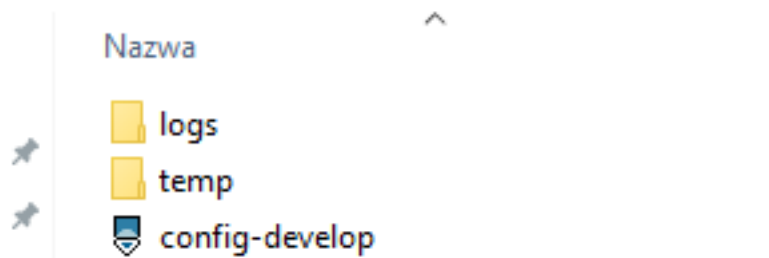
Aktywna aplikacja e-Podpis działa w tle niezależnie od posiadanej przeglądarki internetowej, na pasku narzędzi jest widoczna jako niebieska ikona banku (karta mikroprocesorowa znajduje się w czytniku kart).

- **Zalogowanie** - (np. jeden użytkownik zakończył w bankowości podpisywanie, zaczyna pracować drugi i przechodzi do podpisywania ).





- **Zamknięcie aplikacji** - (do podpisywania konieczne będzie ponowne uruchomienie aplikacji)
- **Wyciągnięcie karty mikroprocesorowej z czytnika kart** powoduje wylogowanie z aplikacji e-Podpis, ale nie powoduje wylogowania z bankowości internetowej, ikona na pasku narzędzi jest w kolorze szarym.
- **Logowanie podczas pracy** z aplikacji e-Podpis na komputerze klienta. Logi aplikacji e-Podpis – po pobraniu aplikacji zostaje utworzona struktura (katalog), w którym zjadają się pliki konfiguracyjne oraz logi z działania aplikacji (np. c:\Users\imie.nazwisko\.scsa\cui\).



## PRZED MIGRACJĄ

### Logowanie do obecnej bankowości elektronicznej def3000/CEB – uruchamianie aplikacji e-Podpis

Logowanie do systemu za pomocą wybranej metody pozostaje bez zmian.

## Autoryzacja

**Proszę wprowadzić PIN  
oraz nacisnąć przycisk "Zatwierdź".**

**Logowanie:** Logowanie kartą mikroprocesorową ?

**PIN:**  ?

## Autoryzacja zleceń za pomocą karty mikroprocesorowej

Po zalogowaniu do aplikacji internetowej, klient na formacie autoryzacji przelewu ma możliwość pobrania „launch.jnlp” i uruchomienia aplikacji e-Podpis. Proces pobrania i uruchomienia wykorzystując do tego JWS Client lub Javy nie będzie się różnił od tego jak to zostało zaprezentowane powyżej w dokumentacji.

## Podpis na formacie przelewu

1. Na formacie akceptowania przelewu pojawia się opcja „Uruchom aplikację SCSA” jest on widoczny, gdy klient ma dodaną konfigurację w Bank Admin do podpisu „Użytkownicy klienta kolumna Typ podpisu – aplikacja SCSA”.

Zlecenie przelewu - Internet Explorer

### Przelew - akceptowanie

Referencje:	Przeelw_01
Rachunek do obciążenia:	92 8809 0005 2001 0002 3243 0001
Nazwa kontrahenta:	Tomasz Test Testowa12 23-098 Test Poland
Nr rachunku kontrahenta:	20 1140 2017 0000 4302 0510 6903
Tytułem:	Przelew testowy
Przelew VAT:	Nie
Kwota:	1,00 PLN
Droga płatności:	Elixir
Data:	2021-01-15
Zleceniodawca:	firma dla ceb POLNA 11 22-333 WARSZAWA

Uruchom aplikację SCSA

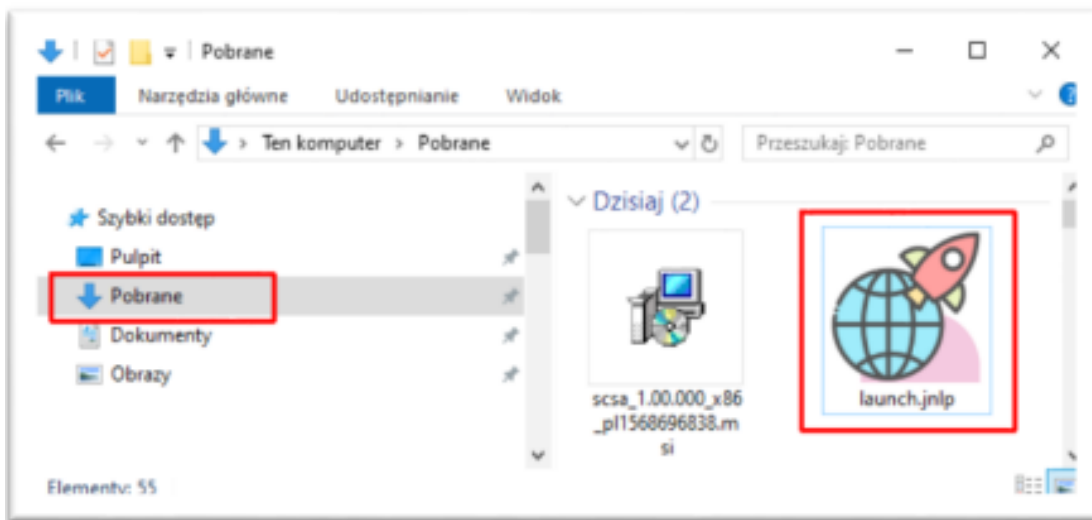
Log:  
2021-01-15 12:17 Nowy przelew - a p

100%

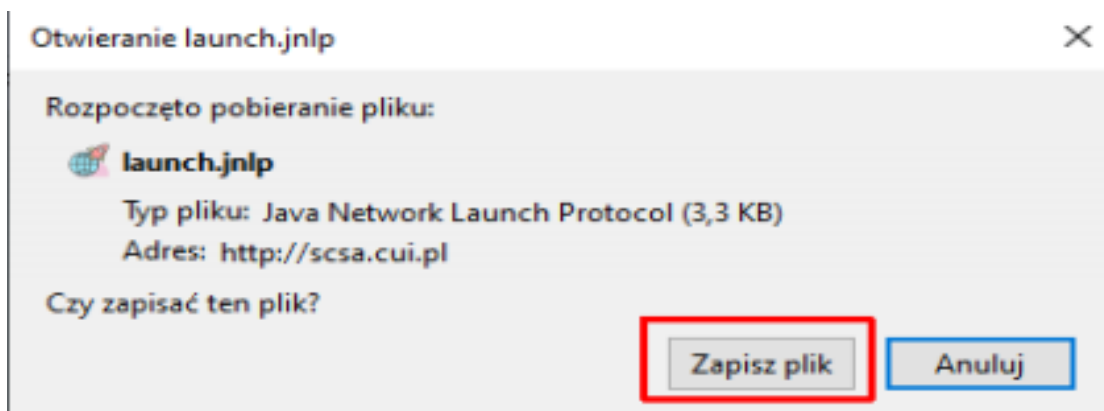
2. W zależności od przeglądarki plik „launch.jnlp” może zostać bezpośrednio uruchomiony – przycisk „Otwórz”



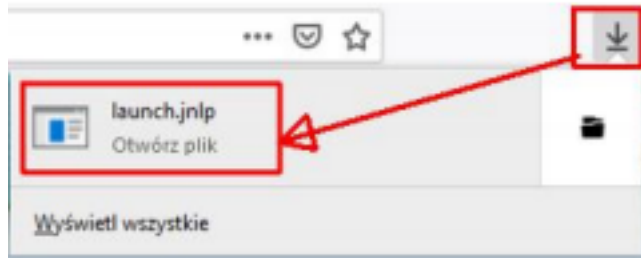
lub jest zapisywany (domyślnie w folderze „Pobrane”)



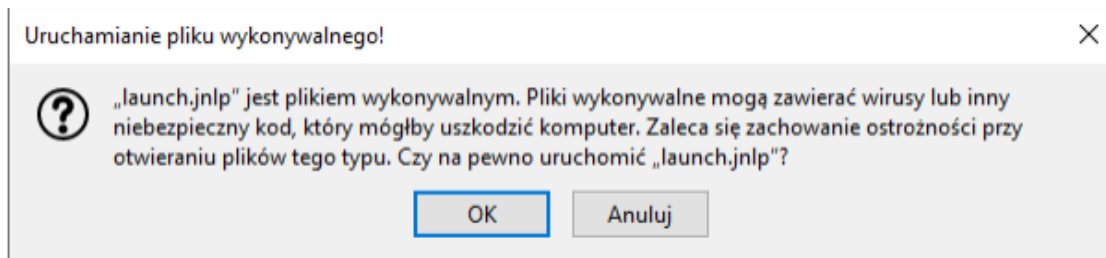
i wtedy należy uruchomić ten pobrany plik z folderu „Pobrane”



lub jeśli jest taka możliwość to uruchomić go z poziomu przeglądarki.



3. Pojawi się ostrzeżenie o uruchamianiu pliku wykonywalnego „launch.jnlp” – należy potwierdzić przyciskiem „OK” dla JWS Client.

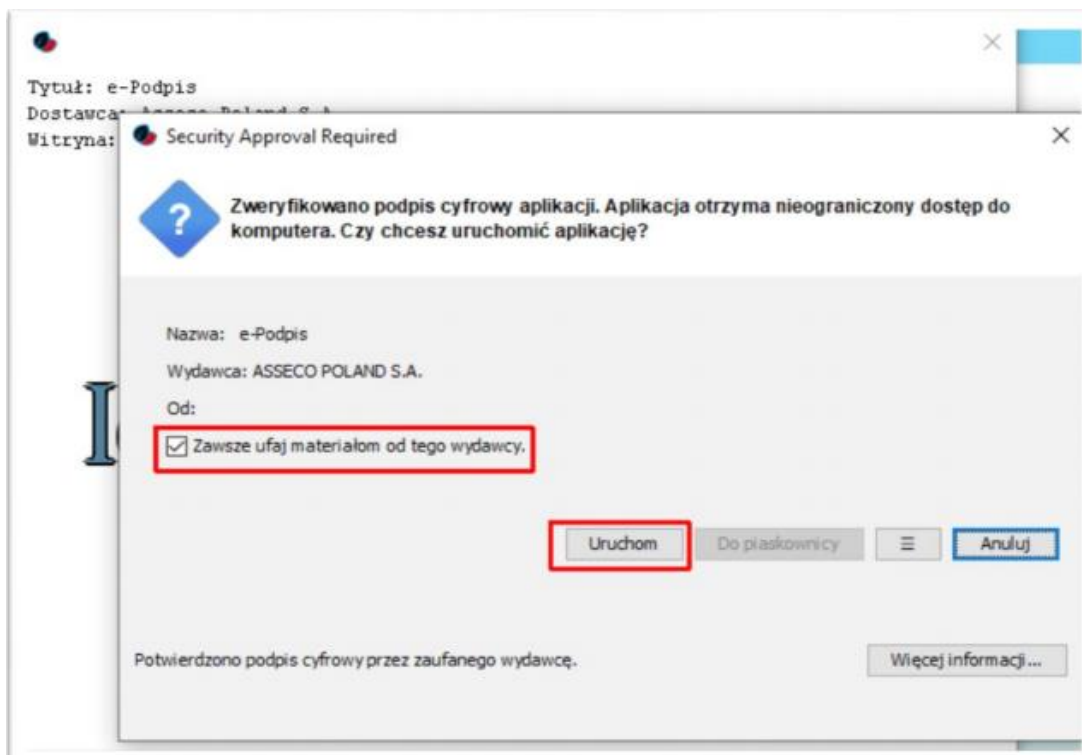


4. Uruchomiony zostaje e-Podpis

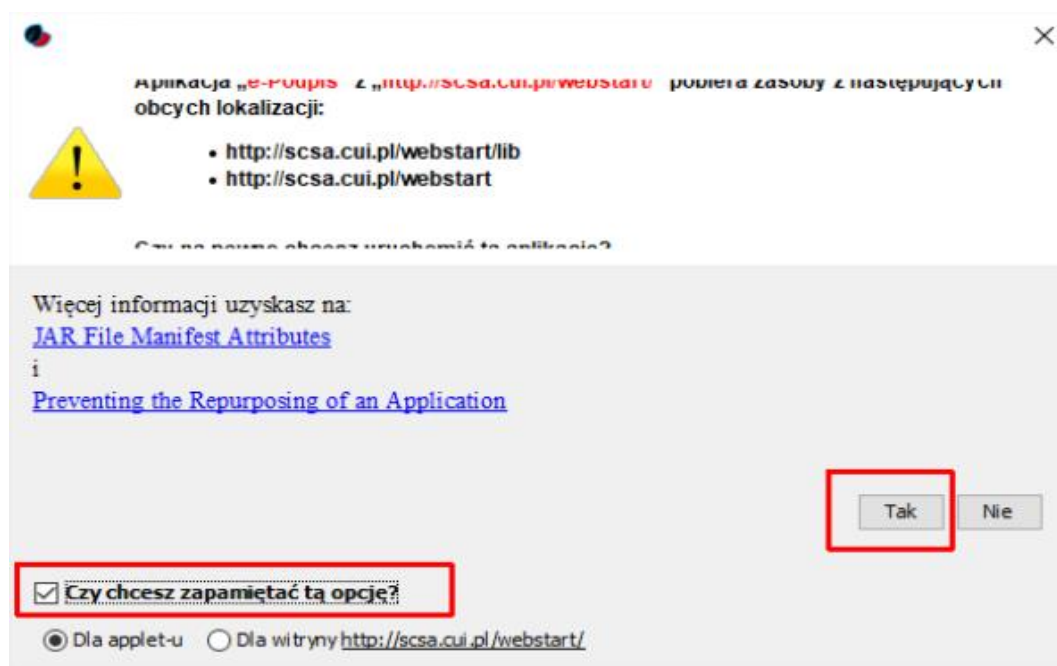


w wersji (jws-client-windows-1.00.001-x86-pl.msi) ekran nie jest prezentowany.

5. Wyświetlone zostanie okno zabezpieczeń „Security Approval Required” w którym jest informacja „Nazwa: e-Podpis” i „Wydawca: ASSECO POLAND S.A.” – należy zaznaczyć „Zawsze ufaj materiałom od tego wydawcy” (czyli zapamiętanie danych jako zaufanych) a następnie nacisnąć przycisk „Uruchom”.

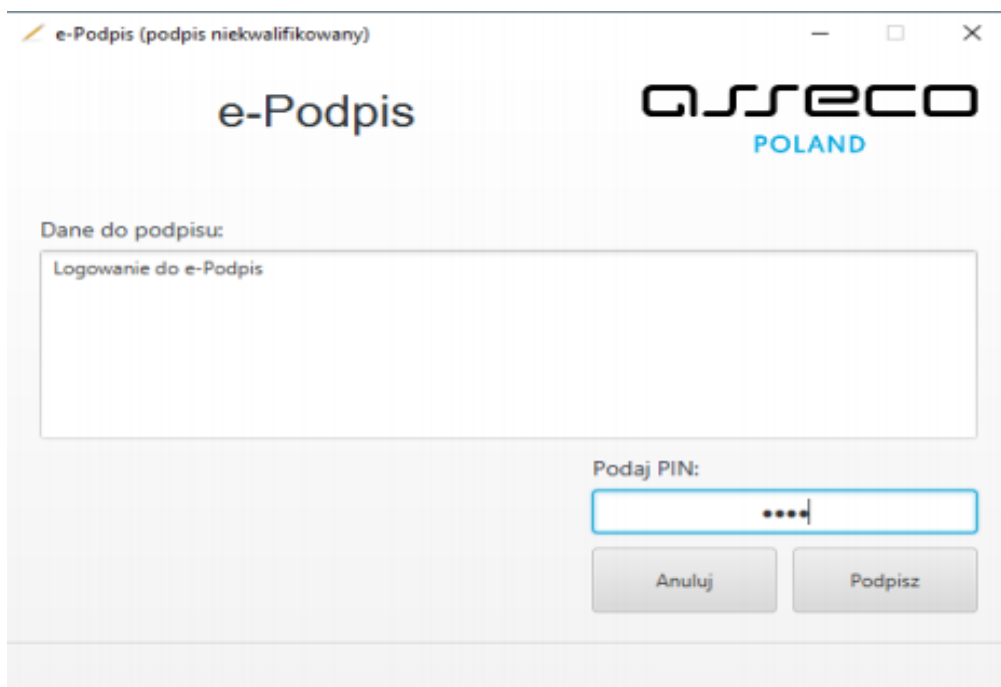


6. W kolejnym oknie wyświetlana jest informacja o pobieraniu przez e-Podpis danych z <https://scsa.cui.pl/webstart/lib> i <https://scsa.cui.pl/webstart> - należy zaznaczyć checkbox „Czy chcesz zapamiętać tę opcję” i następnie nacisnąć przycisk „Tak”.



7. Pkt. 5 i 6. powinny pojawić się tylko przy pierwszym uruchamianiu, jeśli zaznaczono „Zawsze ufaj materiałom od tego wydawcy” i „Czy chcesz zapamiętać tę opcję” tak jak opisano powyżej.

8. Włożyć kartę do czytnika i zalogować się do e-Podpisu wpisując PIN karty mikroprocesorowej.



The screenshot shows a window titled "e-Podpis (podpis niekwalifikowany)". The window contains the "e-Podpis" logo on the left and the "ASSECO POLAND" logo on the right. Below the logos, there is a section titled "Dane do podpisu:" containing a text box with the text "Logowanie do e-Podpis". To the right of this section is a "Podaj PIN:" label above a PIN input field containing four asterisks. Below the PIN field are two buttons: "Anuluj" and "Podpisz".

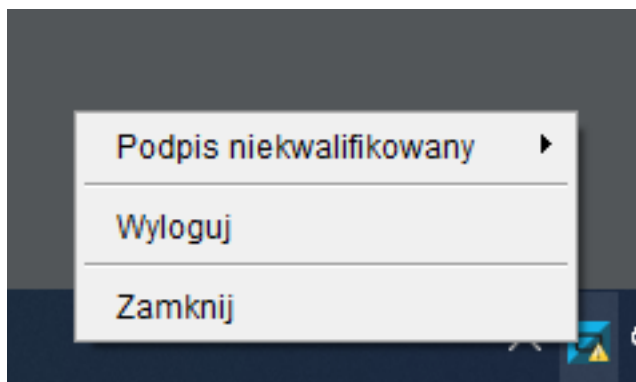
9. W oknie dialogowym „Dane do podpisu” pojawi się komunikat „Logowanie do systemu e-Podpis”. Prawidłowe podanie kodu PIN powoduje zalogowanie do bankowości elektronicznej i pojawienie się komunikatu „poprawnie wysłano podpisane dane”.



The screenshot shows the same window as above, but with a large green checkmark icon in the bottom left corner. The text "Logowanie do e-Podpis" is still visible in the text box. A "Zamknij (1)" button is now visible in the bottom right corner. At the bottom of the window, a status bar displays the message "Poprawnie wysłano podpisane dane".

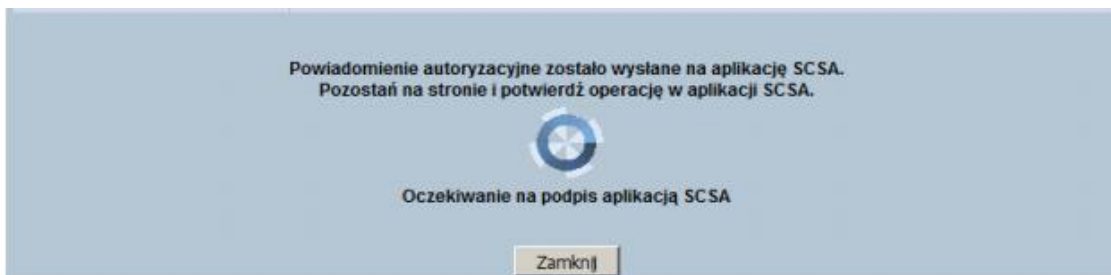
10. Powyższe okno dialogowe można zamknąć po kliknięciu na klawisz „Zamknij” lub poczekać, aż zostanie zamknięte samoczynnie po upływie 3 sekund.

Zalogowanie do e-Podpisu jest sygnalizowane niebieską ikonką w zasobniku systemowym.

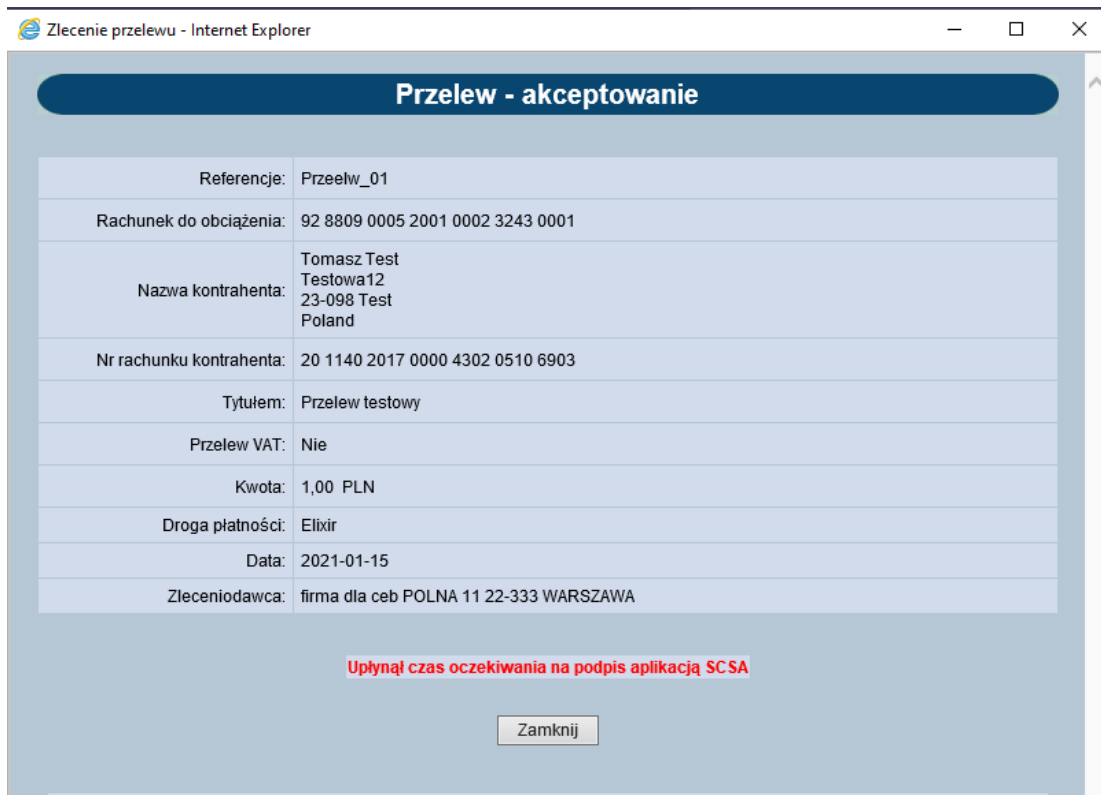


Po uruchomieniu pliku przez Użytkownika aplikacja e-Podpis będzie pracowała przez cały czas "w tle". Aplikacja e-Podpis pracuje na urządzeniach klasy PC na każdym systemie operacyjnym, na którym zainstalowana jest Java (JRE) w wersji minimum 1.8 oraz do którego producent czytnika kart mikroprocesorowych dostarcza sterownik. Aplikacja SCSA działa na komputerze użytkownika zupełnie niezależnie od przeglądarki na jakiej pracuje system def3000/CEB.

11. W przeglądarce wybrać opcję [**Podpisz**]: formatka „Przelew – akceptowanie” przejdzie w tryb „Oczekiwanie na podpis aplikacją SCSA”.



Po upływie czasu zostanie wyświetlony komunikat:



12. W aplikacji SCSA należy wykonać autoryzację zlecenia (podpis) poprzez wprowadzenie numeru PIN karty mikroprocesorowej.

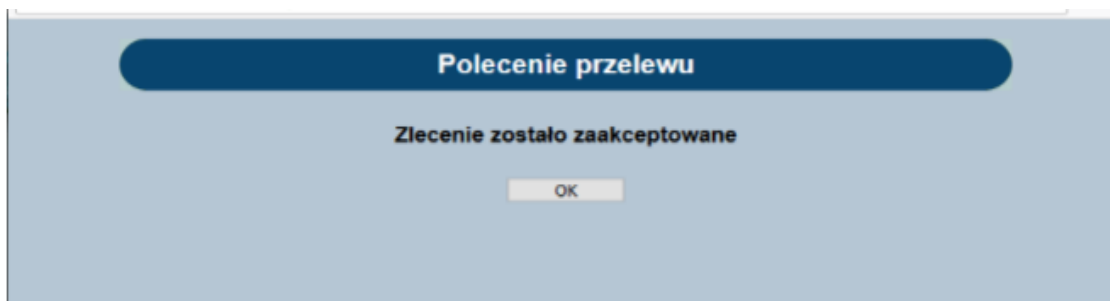




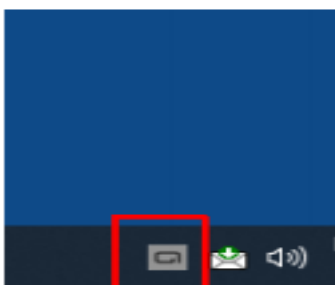
Po wprowadzeniu kodu PIN i naciśnięciu [PODPISZ] system prezentuje formularz z informacją o poprawnej autoryzacji dyspozycji.



13. Po naciśnięciu [ZAMKNIJ] system prezentuje formularz z potwierdzeniem realizacji dyspozycji.



14. Po zakończeniu podpisów kartą należy wyjąć z czytnika - ikona w zasobniku systemowym zmieni kolor na szary.



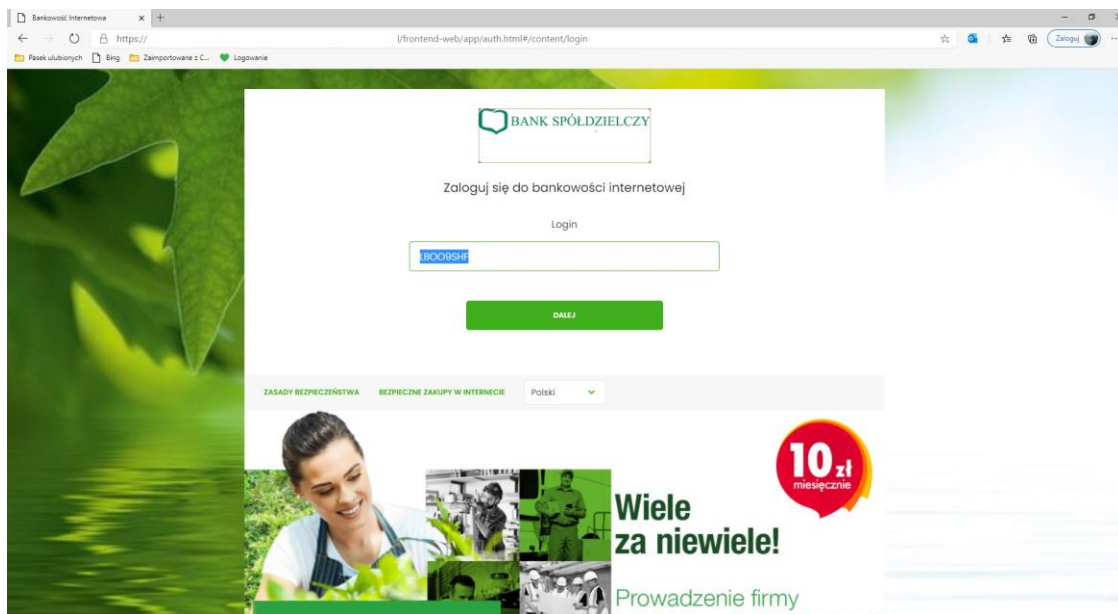
## PO MIGRACJI

### Logowanie do nowego systemu bankowości internetowej Asseco EBP – uruchamianie aplikacji e-Podpis

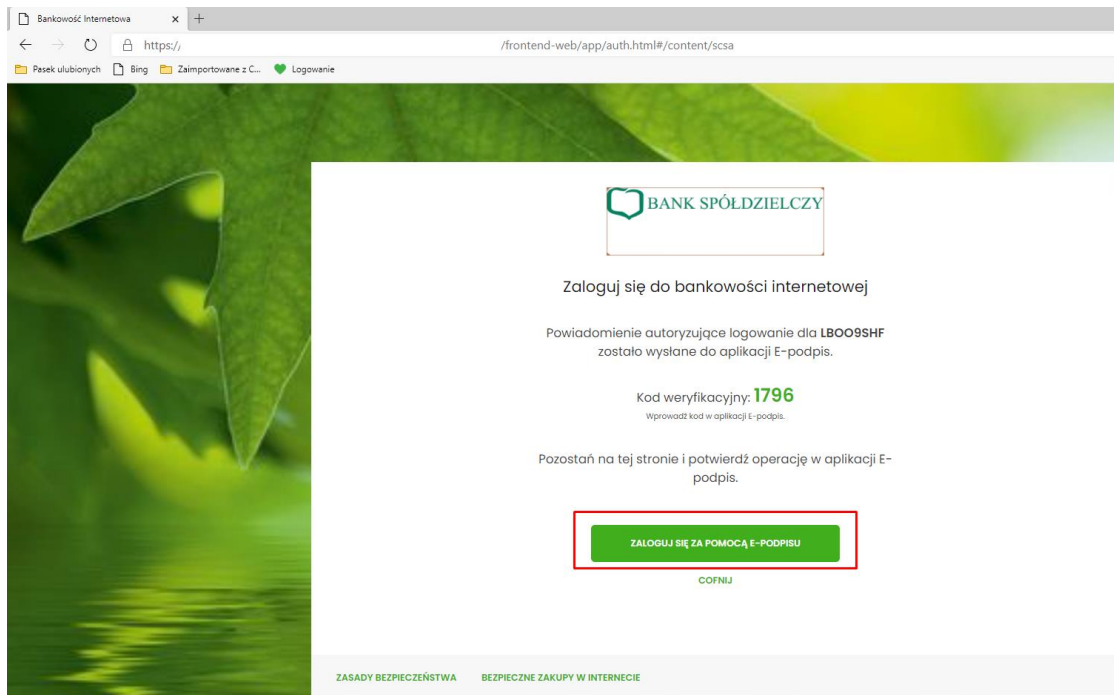
W procesie uwierzytelniania i autoryzacji zleceń przy pomocy karty mikroprocesorowej, system bankowości internetowej pobiera i uruchamia aplikację e-Podpis SCSA. W procesie uruchomienia wykorzystane będzie JWS Client lub Java.

Proces pierwszego logowania przy użyciu karty mikroprocesorowej do aplikacji, będzie przebiegał następująco:

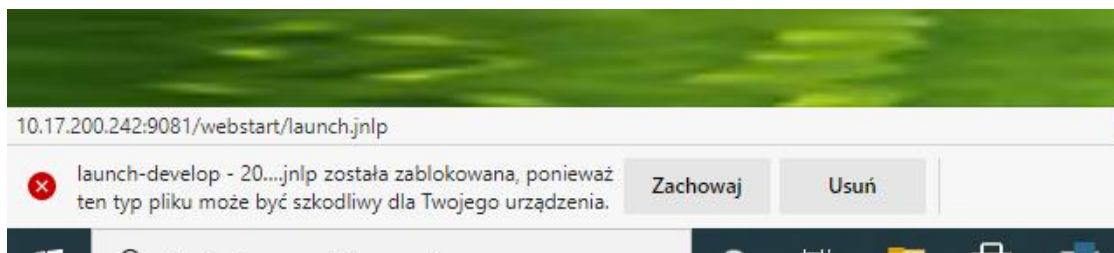
1. Podać identyfikator klienta i wybrać [DALEJ]. **W przypadku gdy Użytkownik nie pamięta Identyfikatora/Loginu konieczny będzie kontakt z Bankiem.**



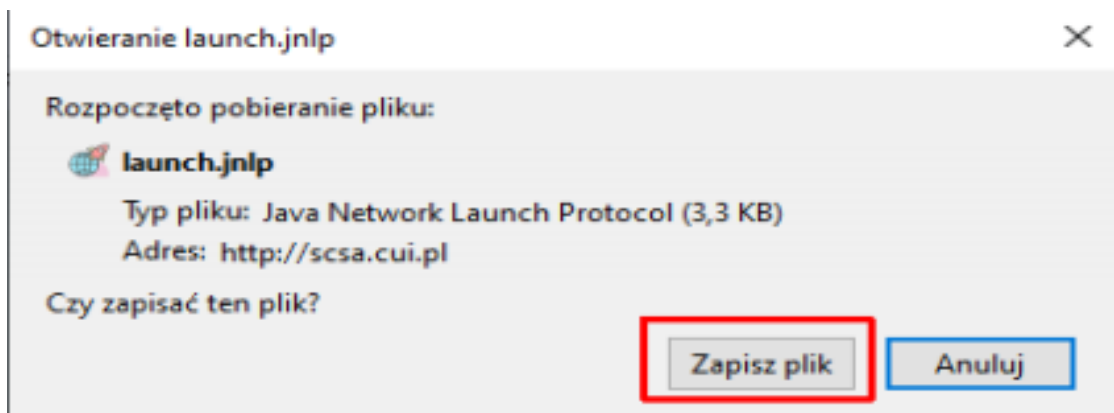
2. Po wpisaniu identyfikatora zostaniemy przeniesieni do kolejnej strony, na której będziemy mieć możliwość pobrania i uruchamiania e-Podpisu SCSA poprzez wybranie opcji: "Zaloguj się za pomocą E-Podpisu". Na formatce zostanie zaprezentowany: Identyfikator osoby logującej się i kod weryfikacyjny.



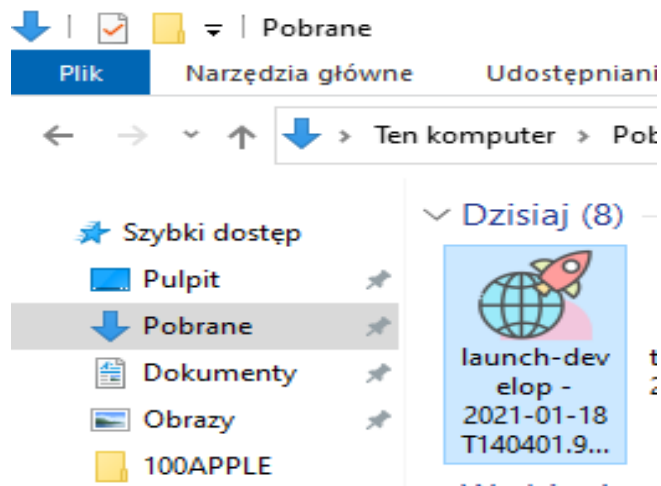
3. Po wybraniu opcji [ZALOGUJ SIĘ ZA POMOCĄ EPODPISU] zostanie pobrany plik „launch-develop - 2021-01-18T140401.jnlp”. W zależności od przeglądarki plik „launch.jnlp” może zostać bezpośrednio uruchomiony – przycisk „Otwórz”



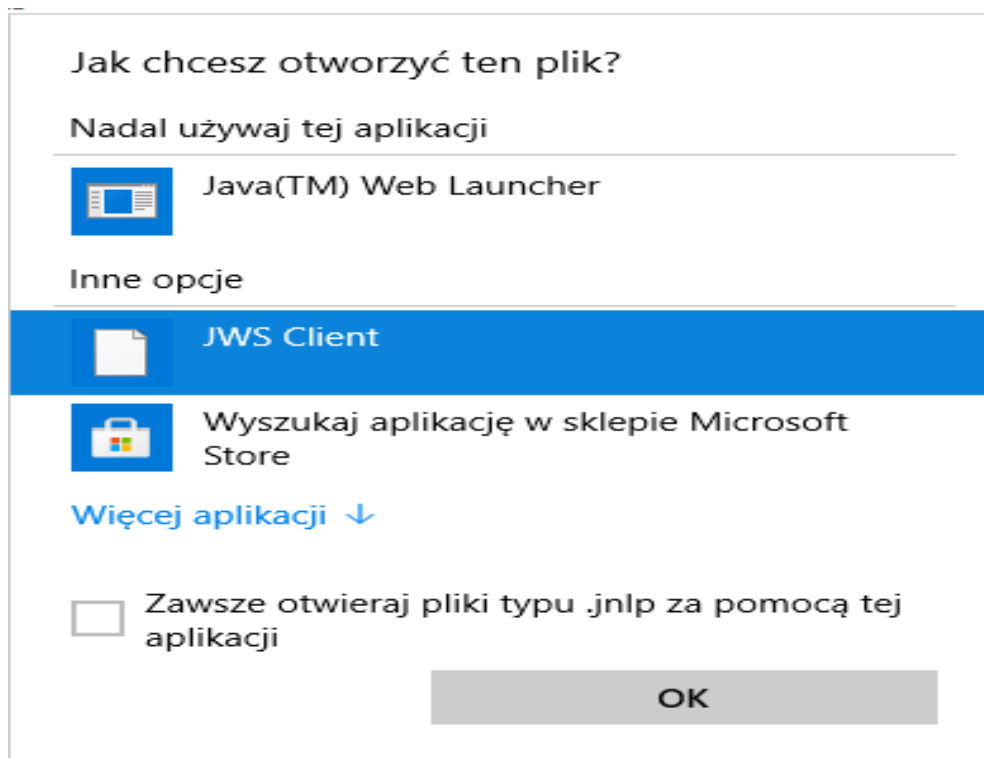
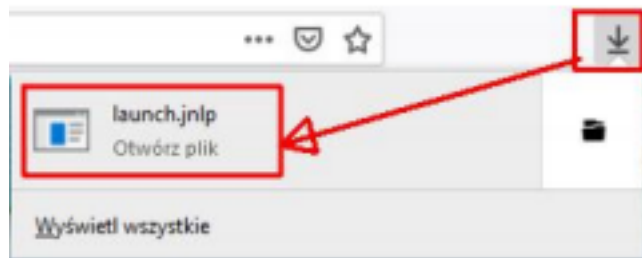
lub jest zapisywany (domyślnie w folderze „Pobrane”)



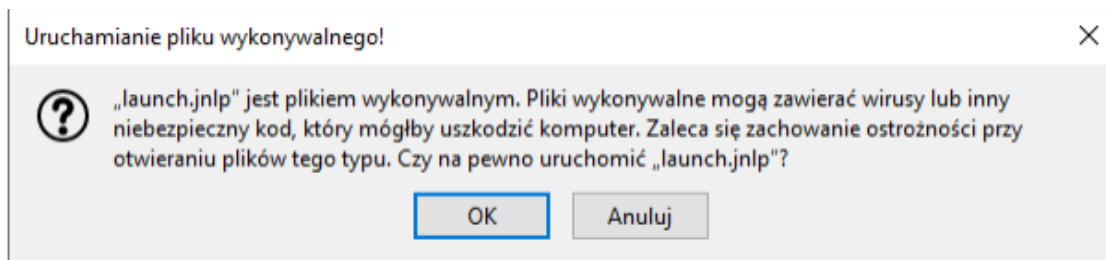
i wtedy należy uruchomić pobrany plik z folderu „Pobrane”



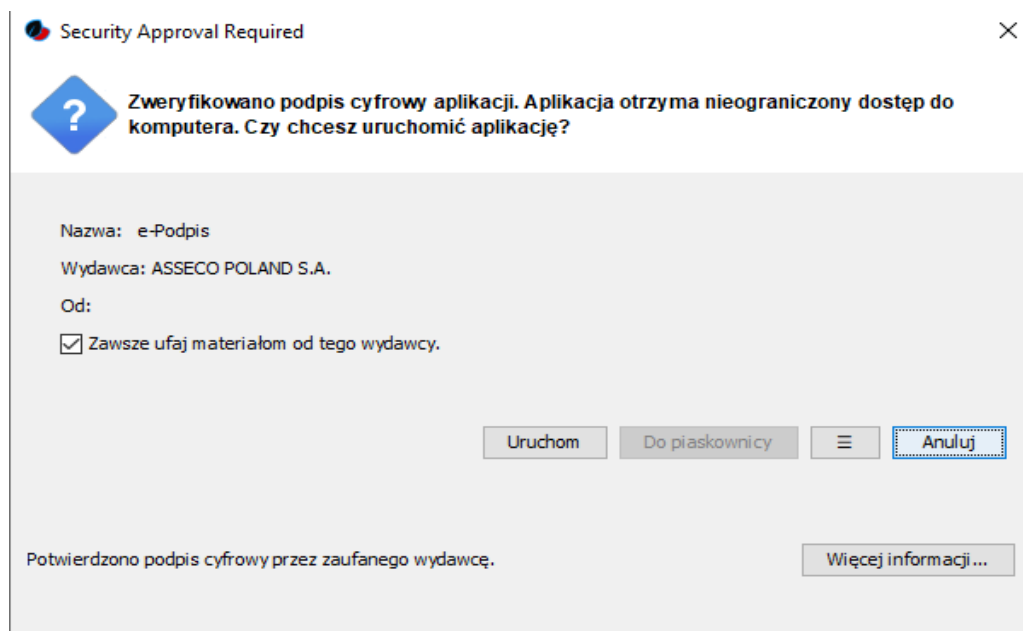
lub jeśli jest taka możliwość to uruchomić go z poziomu przeglądarki jako JWS Client.



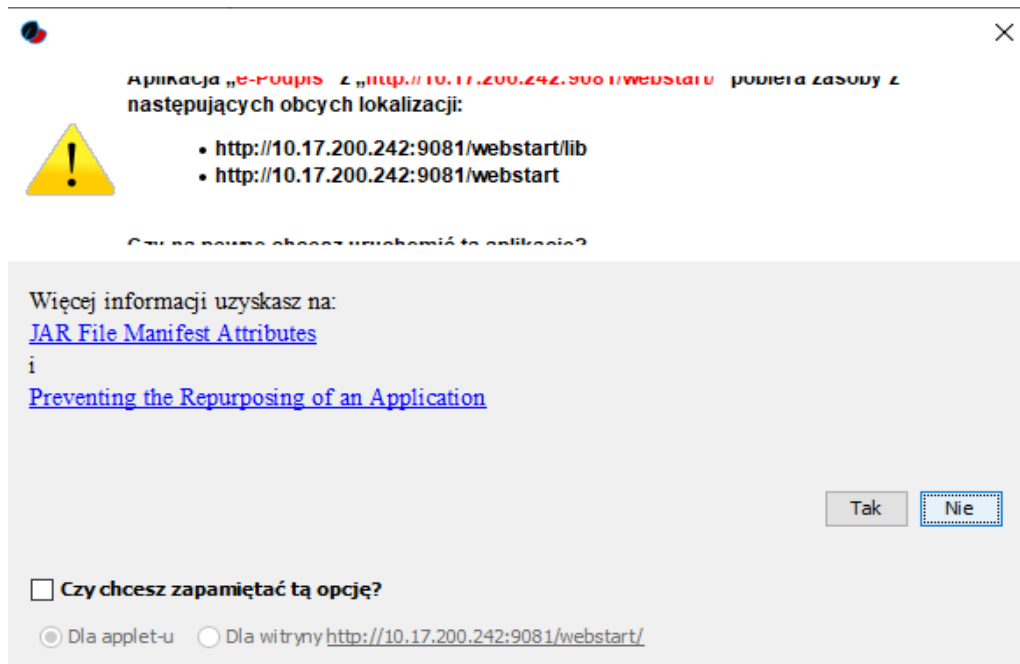
4. Pojawi się ostrzeżenie o uruchamianiu pliku wykonywalnego „launch.jnlp” – należy potwierdzić przyciskiem „OK”.



5. Wyświetlone zostanie okno zabezpieczeń „Security Approval Required” w którym jest informacja „Nazwa: e-Podpis” i „Wydawca: ASSECO POLAND S.A.” – należy zaznaczyć „Zawsze ufaj materiałom od tego wydawcy” (czyli zapamiętanie danych jako zaufanych) a następnie nacisnąć przycisk „Uruchom”.

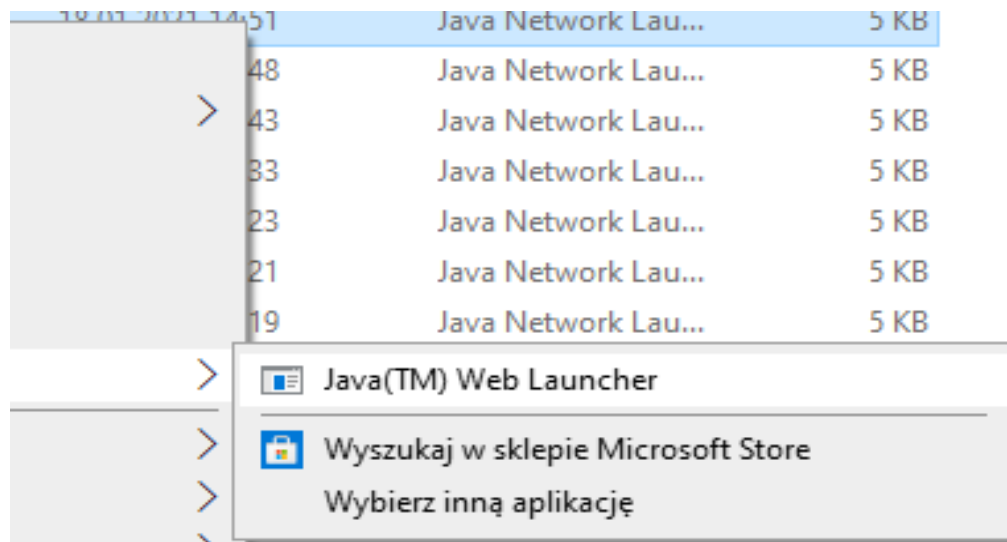


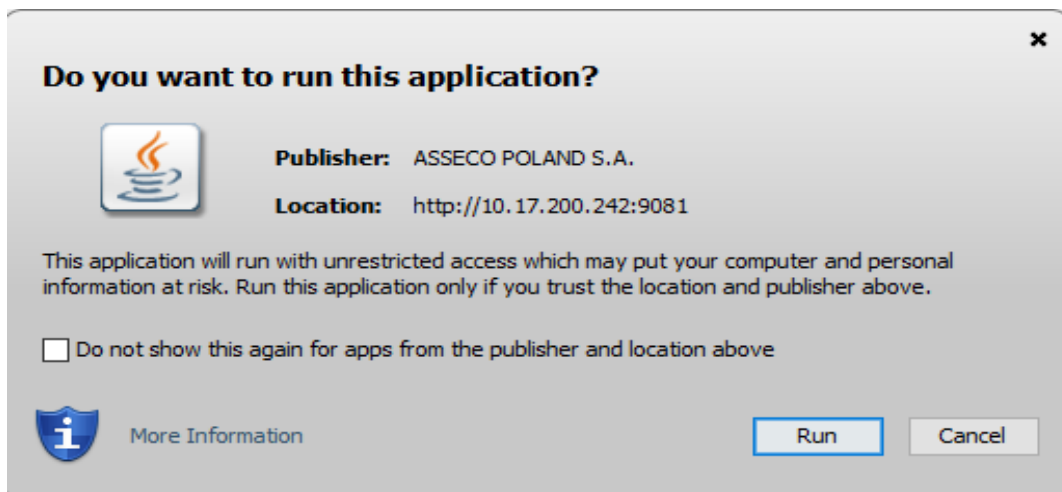
6. W kolejnym oknie wyświetlana jest informacja o pobieraniu przez e-Podpis danych z <https://scsa.cui.pl/webstart/lib> i <https://scsa.cui.pl/webstart> - należy zaznaczyć checkbox „Czy chcesz zapamiętać tę opcję” i następnie nacisnąć przycisk „Tak”.



7. Pkt. 5 i 6 powinny pojawić się tylko przy pierwszym uruchamianiu, jeśli zaznaczono „Zawsze ufaj materiałom od tego wydawcy” i „Czy chcesz zapamiętać tę opcję” tak jak opisano powyżej.

8. Dla uruchomienia z Java będziemy mieć:

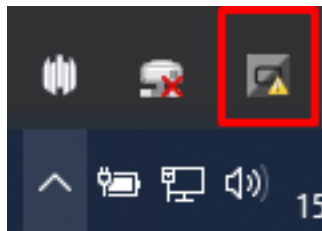




9. Po uruchomieniu aplikacji przy pomocy Java, system wyświetli okno, w którym będzie zaprezentowane okno do weryfikacji danych.



10. Po poprawnej weryfikacji zaprezentuj się okno „Logowanie do e-Podpis”.
11. Po poprawnym przejściu krok 1-10 Włożyć kartę do czytnika i zalogować się do e-Podpisu wpisując PIN karty mikroprocesorowej.



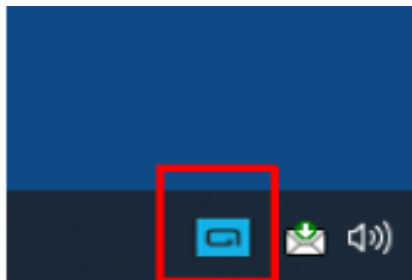
12. W oknie dialogowym „Dane do podpisu” pojawia się komunikat „Logowanie do systemie e-Podpis” Prawidłowe podanie kodu PIN powoduje zalogowanie do bankowości elektronicznej i pojawienie się komunikatu „poprawnie wysłano podpisane dane”.





13. Powyższe okno dialogowe można zamknąć po kliknięciu na klawisz „Zamknij” lub poczekać, aż zostanie zamknięte samoczynnie po upływie 3 sekund.

Zalogowanie do e-Podpisu jest sygnalizowane niebieską ikonką w zasobniku systemowym.



Przy kolejnym logowaniu do systemu bankowości internetowej, po wpisaniu identyfikatora system automatycznie wyświetla okno aplikacji SCSA do uwierzytelnienia klienta w aplikacji dla bankowości internetowej.

1. Pojawi się kolejne okno e-Podpisu do uwierzytelnienia klienta w aplikacji dla bankowości internetowej. Klient musi podać Kod weryfikacyjny oraz PIN karty

e-Podpis (podpis niekwalifikowany)

e-Podpis

ASSECO  
POLAND

Dane do podpisu:

Logowanie BS

Kod weryfikacyjny:

Podaj PIN:

Anuluj Podpisz

2. Po sprawdzeniu i wprowadzeniu kodu weryfikacyjnego i poprawnym wprowadzeniu PIN-u system loguje użytkownika do bankowości internetowej.

e-Podpis (podpis niekwalifikowany)

e-Podpis

ASSECO  
POLAND

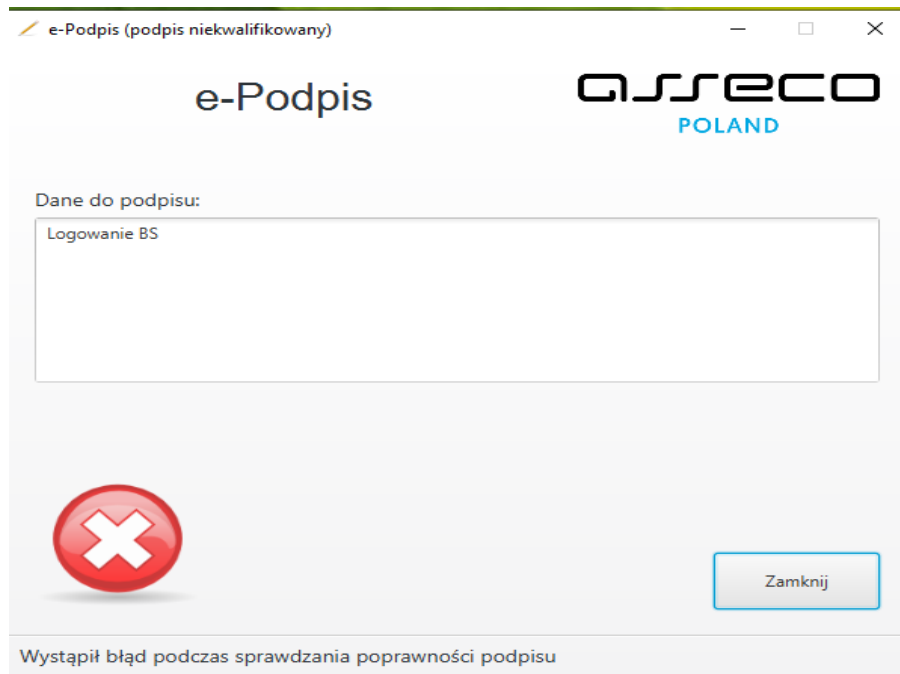
Dane do podpisu:

Logowanie BS

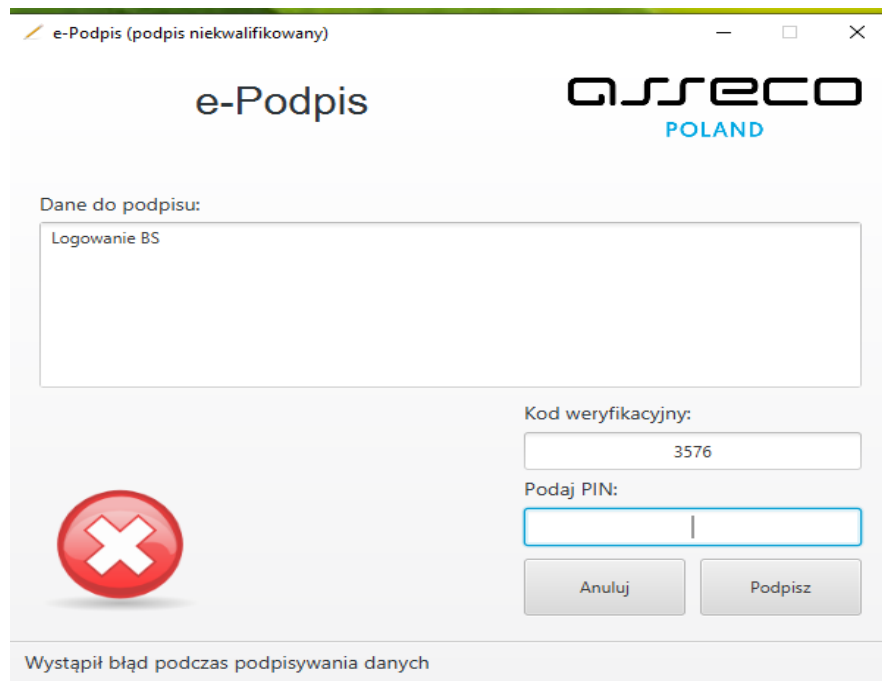
Zamknij (2)

Poprawnie wysłano podpisane dane

3. W przypadku gdy użytkownik wprowadzi błędny kod PIN i błędny kod weryfikacyjny, system zaprezentuje komunikat:

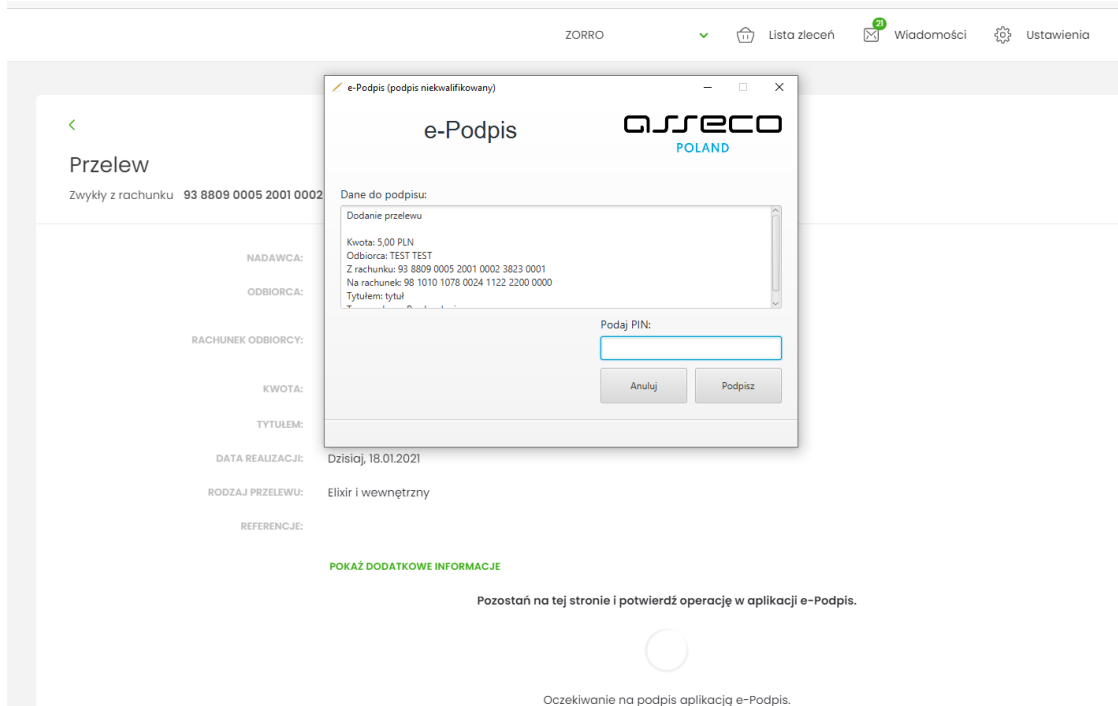


4. W przypadku gdy użytkownik wprowadzi błędny kod PIN i poprawny kod weryfikacyjny, system zaprezentuje komunikat:



## Autoryzacja zleceń za pomocą karty mikroprocesorowej

Na formatce dyspozycji dodania przelewu po wprowadzeniu danych wybieramy [dalej] system prezentuje formularz potwierdzenia wprowadzonych danych wraz z oknem do wprowadzenia kodu PIN.



The screenshot shows the 'e-PODPIS' application interface. A modal window titled 'e-PODPIS' is open, displaying the following information:

- Dane do podpisu:**
  - Dodanie przelewu
  - Kwota: 5,00 PLN
  - Odbiorca: TEST TEST
  - Z rachunku: 93 8809 0005 2001 0002 3823 0001
  - Na rachunek: 98 1010 1078 0024 1122 2200 0000
  - Tytułem: tytuł
- Podaj PIN:** [input field]
- Buttons:** Anuluj, Podpisz

Below the modal, the main page shows details for a transfer:

- Przelew**
- Zwykły z rachunku 93 8809 0005 2001 0002
- NADAWCA:**
- ODBIORCA:**
- RACHUNEK ODBIORCY:**
- KWOTA:**
- TYTUŁEM:**
- DATA REALIZACJI:** Dzisiaj, 18.01.2021
- RODZAJ PRZELEWU:** Elixir i wewnętrzny
- REFERENCJE:**

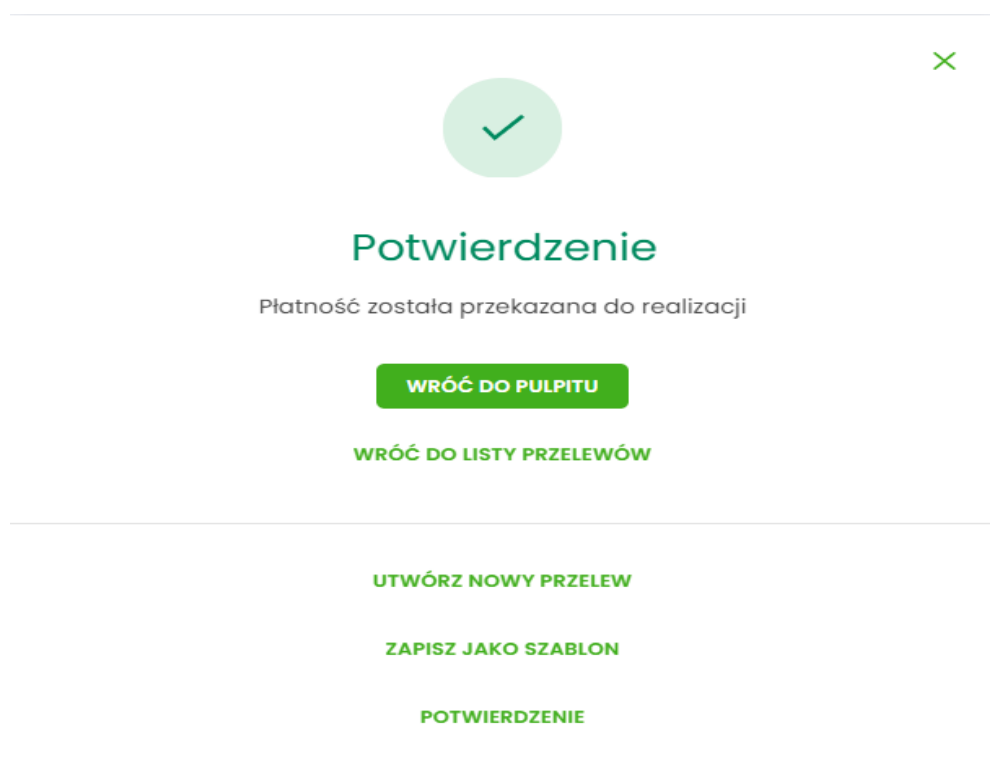
At the bottom, there is a green link: **POKAŹ DODATKOWE INFORMACJE** and a loading indicator with the text: **Oczekiwanie na podpis aplikacją e-PODPIS.**

Na formularzu E-PODPIS dostępne są akcje:

- [ANULUJ] – umożliwia rezygnację z podpisania dyspozycji.
- [PODPISZ] – umożliwia podpisanie dyspozycji. Po wprowadzeniu kodu PIN i naciśnięciu [PODPISZ] system prezentuje formularz z informacją o poprawnej autoryzacji dyspozycji.



Po naciśnięciu [ZAMKNIJ] system prezentuje formularz z potwierdzeniem realizacji dyspozycji.



Na formularzu POTWIERDZENIE dostępne są akcje:

- [WRÓĆ DO PULPITU] – umożliwia powrót do pulpitu,
- [UTWÓRZ NOWY PRZELEW] – umożliwia utworzenie nowej dyspozycji,

- [ZAPISZ JAKO SZABLON] – umożliwia zapisanie dyspozycji jako szablon,
- [POTWIERDZENIE] – wydruk dyspozycji do PDF.

W przypadku gdy użytkownik wprowadzi błędny kod PIN, system zaprezentuje komunikat:

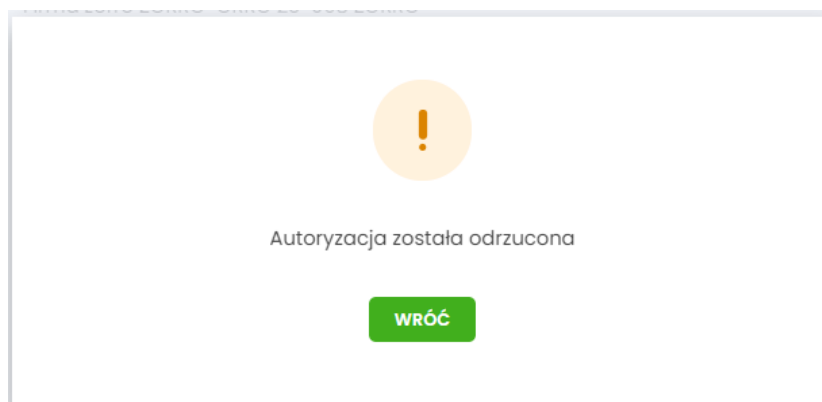


The screenshot shows a window titled "e-Podpis (podpis niekwalifikowany)". The window contains the "e-Podpis" logo and the "ASSECO POLAND" logo. Below the logos, there is a section titled "Dane do podpisu:" containing a scrollable text area with the following information: "Dodanie przelewu", "Kwota: 5,00 PLN", "Odbiorca: Test Test", "Z rachunku: 93 8809 0005 2001 0002 3823 0001", "Na rachunek: 44 8857 1054 9544 1571 7332 4226", and "Tytułem: tytuł". To the right of this text area is a "Podaj PIN:" label and an empty input field. Below the input field are two buttons: "Anuluj" and "Podpisz". On the left side of the window, there is a large red circular icon with a white 'X' inside. At the bottom of the window, a message reads "Wystąpił błąd podczas podpisywania danych".

Na formularzu E-PODPIS dostępne są akcje:

- [ANULUJ] – umożliwia rezygnację z podpisania dyspozycji,
- [PODPISZ] – umożliwia wprowadzenie poprawnego kodu i podpisanie dyspozycji.

Po odrzuceniu dyspozycji za pomocą przycisku [ANULUJ], system prezentuje następujący komunikat:



The screenshot shows a central message box with a yellow circular icon containing a black exclamation mark. Below the icon, the text reads "Autoryzacja została odrzucona". At the bottom of the message box is a green button with the text "WRÓC" in white capital letters.

Przy kolejnym autoryzowaniu dyspozycji system automatycznie wyświetla okno aplikacji SCSA do podpisania dyspozycji w aplikacji dla bankowości internetowej.

Wylogowanie się z e- Podpis lub wylogowanie się z komputera, powoduje, że musimy ponownie zalogować się do e-Podpisu.