



**BANK SPÓŁDZIELCZY  
w BIECZU**

**Podręcznik użytkownika aplikacji SCSA  
(e-Podpis)**

Version 6.14.2



## Spis treści

1. Konwencje typograficzne .....	1
2. Wstęp .....	2
3. Oprogramowanie .....	3
3.1. Zmiana metody logowania i autoryzacji z apletu Java na e-Podpis .....	3
3.2. Instalacja oprogramowania OpenWebStart dla uruchamiania aplikacji JavaWebStart .....	6
4. Pobieranie i zapis na dysku aplikacji e-Podpis (SCSA) .....	15
5. Uruchomienie aplikacji e- Podpis z wykorzystaniem oprogramowania OpenWebStart lub Javy. ....	17
6. Obsługa e-Podpisu .....	23
6.1. Podpis niekwalifikowany .....	23
6.2. Podpis kwalifikowany .....	25
7. Logowanie do systemu bankowości internetowej def3000/EBP – uruchamianie aplikacji e-Podpis . . . .	29
8. Autoryzacja zleceń za pomocą karty mikroprocesorowej .....	43

## Rozdział 1. Konwencje typograficzne

W dokumentacji stosowane są następujące konwencje typograficzne:

Konwencja typograficzna lub znak wizualny	Opis
Standardowy	Podstawowy tekst dokumentacji
Tabela	Tekst w tabeli
<b>Nowe pojęcie</b>	Nowe pojęcia. Wyróżnienie ważnych fragmentów tekstu.
<i>Kursywa</i>	Pozycje na listach wartości. Komunikaty systemowe. Parametry lub zmienne, których rzeczywiste nazwy lub wartości mają być dostarczane przez użytkownika. Nazwy opcji systemu. Ścieżki, np. <i>Dane archiwalne</i> → <i>Przeglądanie</i> .
<b>Uwaga</b>	<p>Tekst uwagi, komentarza, zastrzeżenia - informacje, na które należy zwrócić uwagę podczas czytania dokumentacji lub pracy z systemem np.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p><b>NOTE</b></p> <p>PODANY POWYŻEJ ADRES INTERNETOWY JEST PRZYKŁADOWY. INFORMACJĘ O ADRESIE STRONY USŁUG INTERNETOWYCH UDOSTĘPNIŁ BANK.</p> </div>
<b>Ostrzeżenie</b>	<p>Tekst ostrzeżenia - ostrzeżenia zawierają bardzo ważne informacje, na które należy zwrócić szczególną uwagę podczas czytania dokumentacji lub pracy z systemem, np.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p><b>WARNING</b></p> <p>ZMIANY PRZEKSIĘGOWAŃ NIE SĄ KONTROLOWANE PRZEZ SYSTEM I WYKONYWANE SĄ WYŁĄCZNIE NA WŁASNĄ ODPOWIEDZIALNOŚĆ OPERATORA!</p> </div>
<b>Link</b>	Odwołania do innych rozdziałów lub fragmentów tekstu. Adresy URL
Kod źródłowy	<p>Fragmenty kodu źródłowego. Przykłady wydruków</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <pre>{   "a": "b" }</pre> </div>
CAPS LOCK	Wyróżnienie nagłówków akapitów. Nazwy klawiszy na klawiaturze - kombinacje klawiszy, które należy nacisnąć jednocześnie zawierają znak "+" pomiędzy, np. CTRL+F.
[ ]	Nazwy przycisków, np. [Czynności]



## **Rozdział 2. Wstęp**

W bankowości elektronicznej dla Klientów Korporacyjnych oraz def3000/EBP 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. Udostępniono aplikację e-Podpis (SCSA) umożliwiającą autentykację użytkownika i autoryzację zleceń.

## Rozdział 3. Oprogramowanie


Dla korzystania z aplikacji e-Podpis (SCSA) należy zainstalować oprogramowanie Java lub darmowe oprogramowanie OpenWebStart ([ <https://openwebstart.com> | <https://openwebstart.com/download/>]) umożliwiające komunikację systemu z czytnikami kart mikroprocesorowych zapewniające funkcjonalność autoryzacji z pominięciem apletu Java. Oprogramowanie wymaga zainstalowanej Javy na komputerze użytkownika, którą można pobrać ze strony producenta firmy Oracle. Oprogramowanie jest przydatne/niezbędne do uruchomienia aplikacji Asseco "e-Podpis" z pliku JNLP.

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 darmowego oprogramowania OpenWebStart ([ <https://openwebstart.com> | <https://openwebstart.com/download/>]), umożliwiającego uruchamianie aplikacji JavaWebStart (pliki \*.jnlp).

Z metody uwierzytelniania e-Podpis można korzystać:

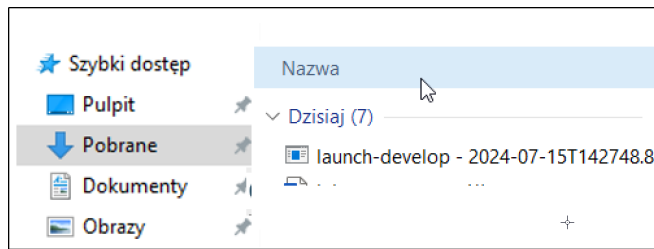
- poprzez jednorazowe zainstalowanie aplikacji na komputerze i późniejsze uruchamianie jej ze skrótu na pulpicie
- każdorazowe uruchamianie aplikacji z pozycji bankowości elektronicznej (klawisz [Uruchom aplikację SCSA]). Aplikacja e-Podpis SCSA wymaga zainstalowanej wersji Javy (min. 1.8\_144) lub OpenWebStart.

 Aplikacja e-Podpis wykorzystuje bibliotekę oprogramowania opracowaną przez Stiftung SIC. Więcej informacji na stronie ([<https://sic.tech/products/core-crypto-toolkits/pkcs11-wrapper/#License> | <https://sic.tech/products/core-crypto-toolkits/pkcs11-wrapper/#License>])

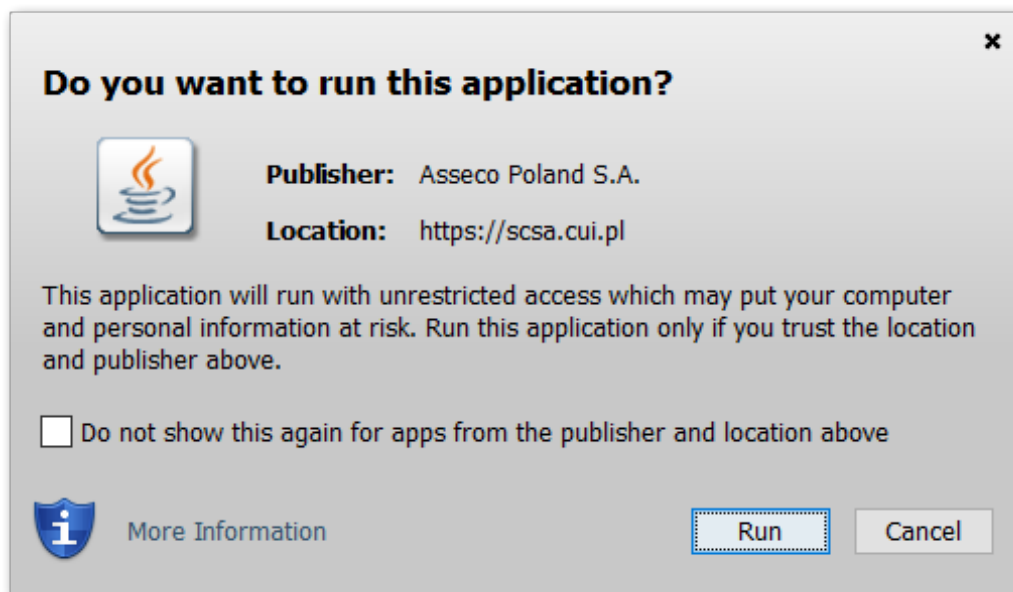
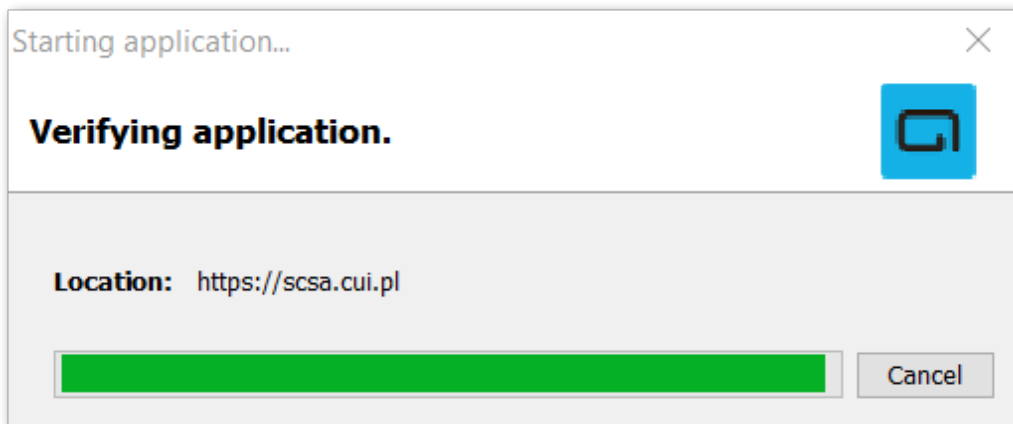
### 3.1. Zmiana metody logowania i autoryzacji z apletu Java na e-Podpis

Dla klientów, którzy używają obecnie autoryzacji lub logowania do aplikacji z wykorzystaniem karty mikroprocesorowej i apletu java zmiana na nową metodę wymaga zainstalowania aplikacji e-Podpis. W tym celu należy:

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



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



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

e-Podpis (podpis niekwalifikowany)

e-Podpis

**ASSECO**  
POLAND

Dane do podpisu:

Logowanie do e-Podpis

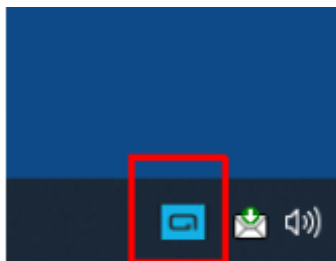
[Zmień metodę akceptacji](#)

Podaj PIN:

Anuluj Podpisz



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



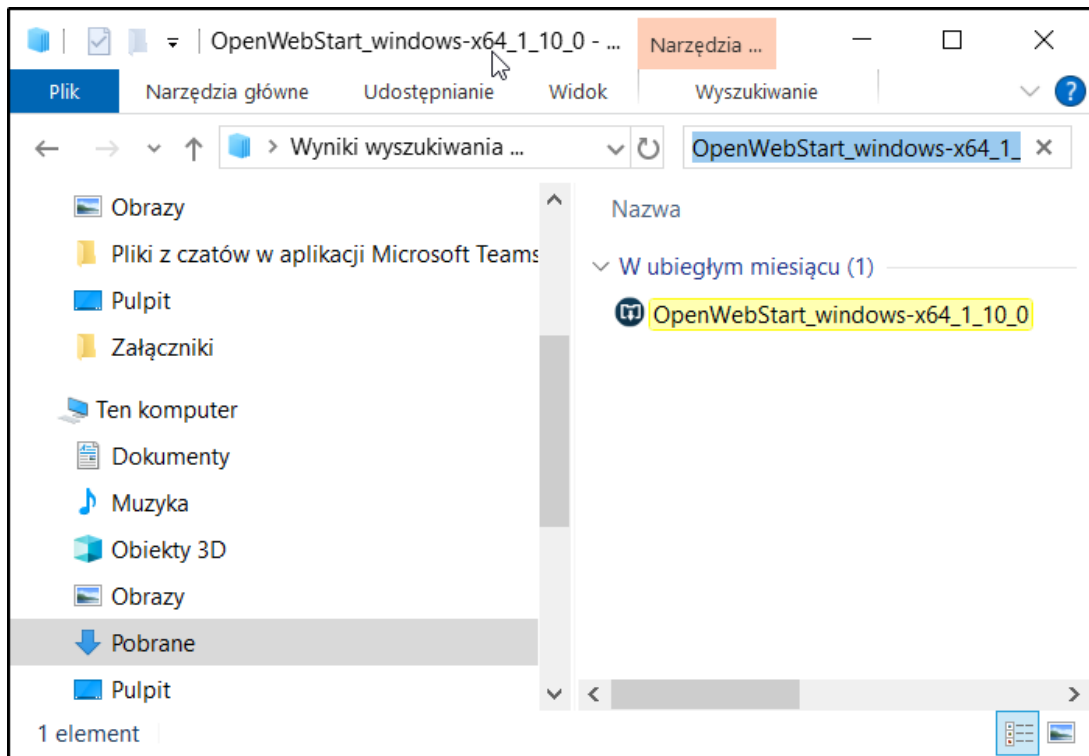
W przypadku braku możliwości zalogowania się do aplikacji e-Podpis lub nie pojawienia się e-Podpisu należy pobrać i wysłać logi do banku w celu dalszej diagnostyki:

- 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\).

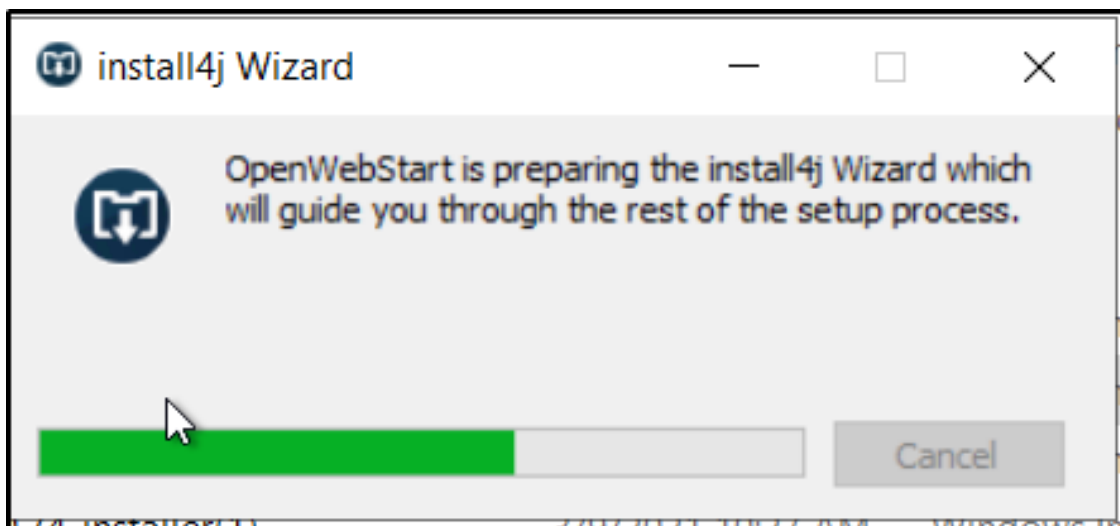
## 3.2. Instalacja oprogramowania OpenWebStart dla uruchamiania aplikacji JavaWebStart

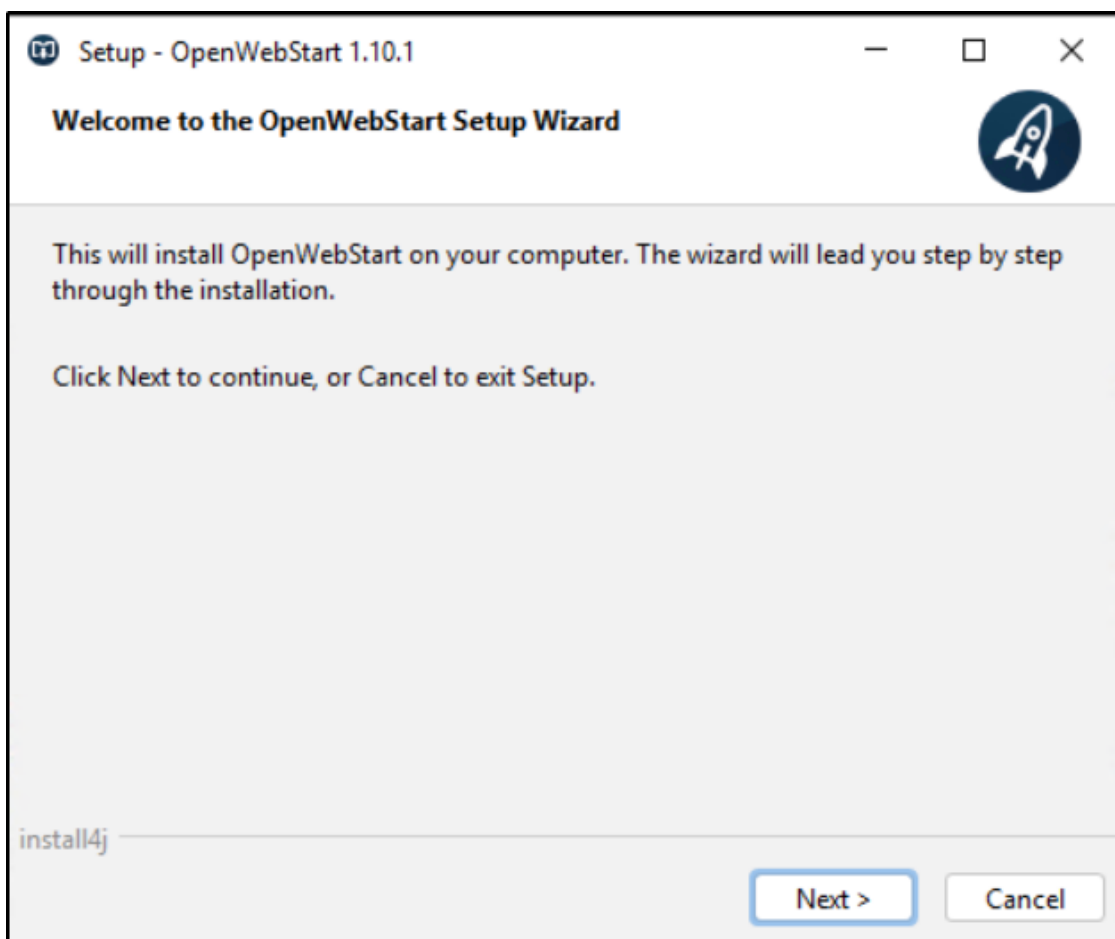
W celu zainstalowania aplikacji OpenWebStart należy:

Wybrać adres strony OpenWebStart lub skorzystać z linku (<https://openwebstart.com> | <https://openwebstart.com/>)

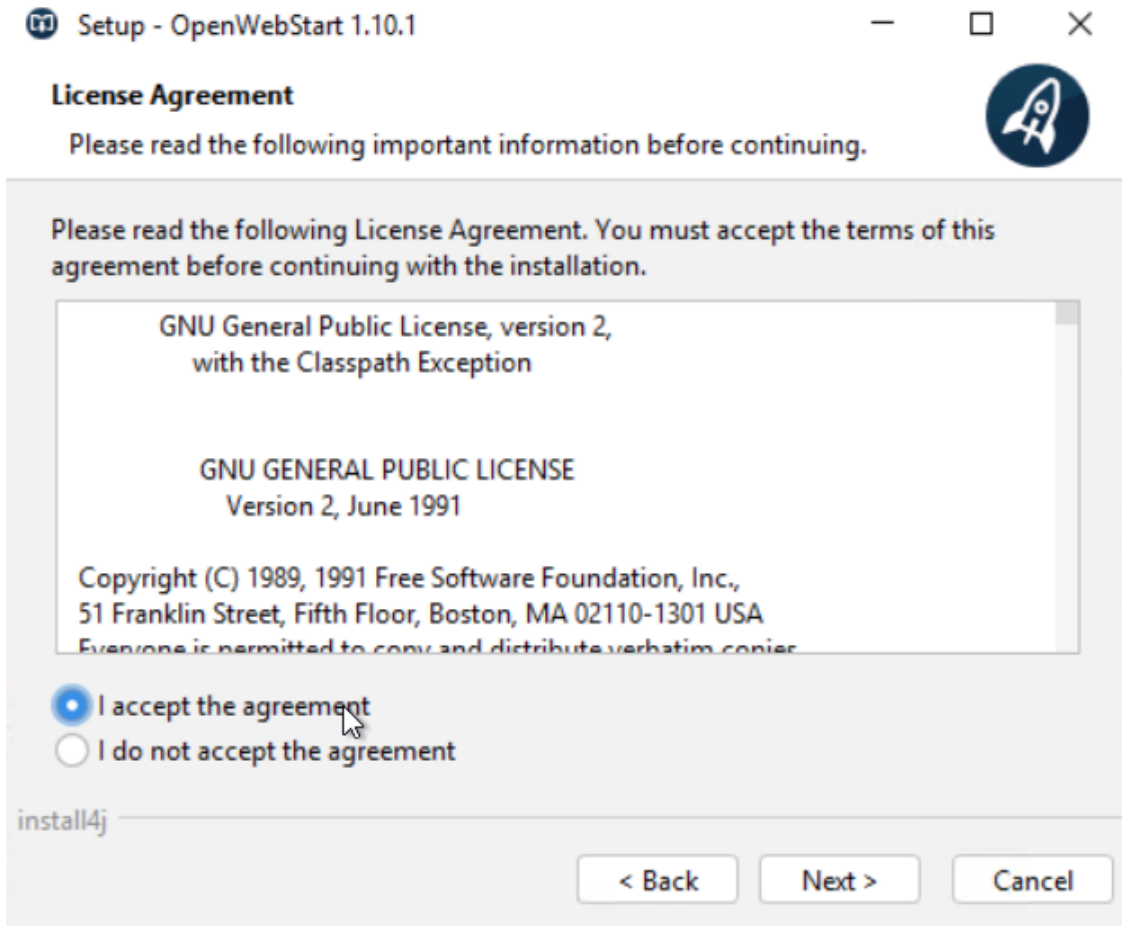


Uruchomić pobrany plik OpenWebStart\_windows (domyślnie jest zapisywany w folderze „Pobrane”).

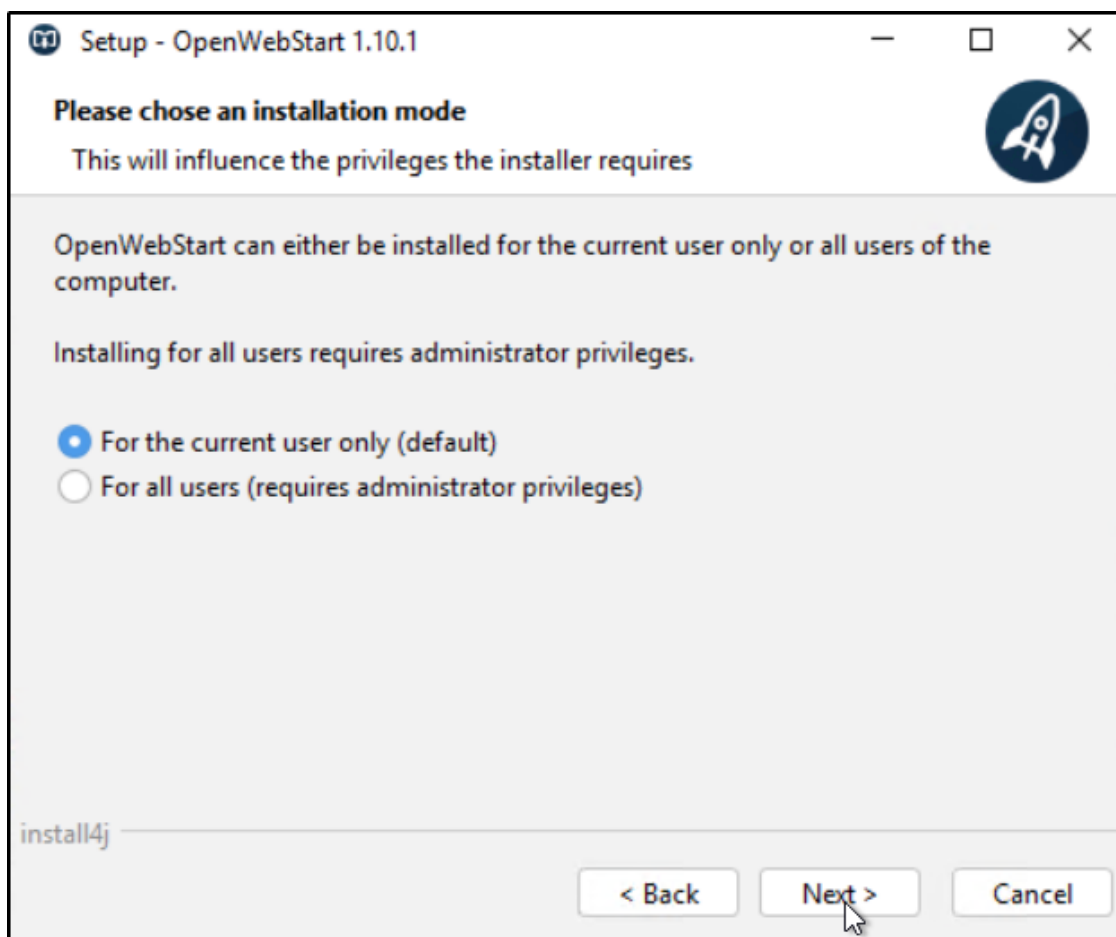




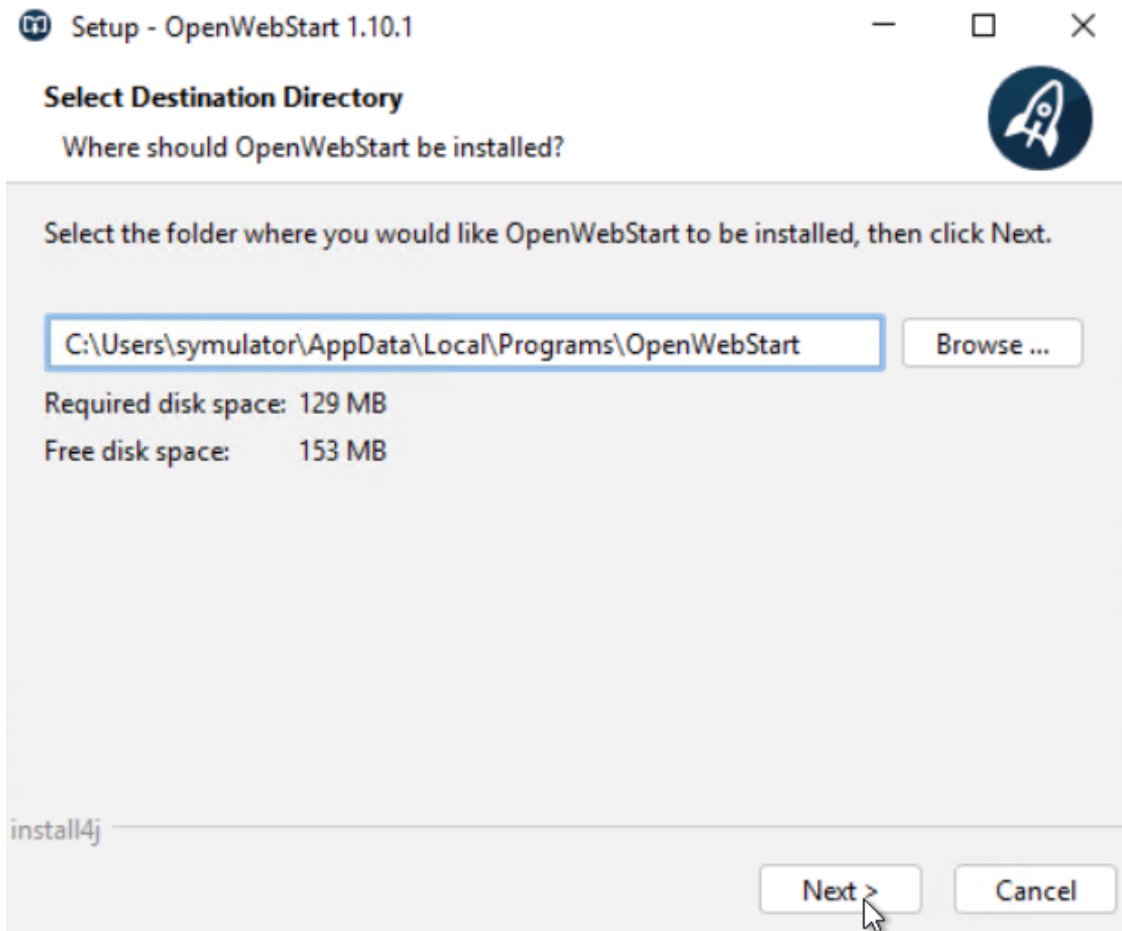
W kolejnym oknie zaakceptować warunki licencji oprogramowania i nacisnąć „Dalej”.



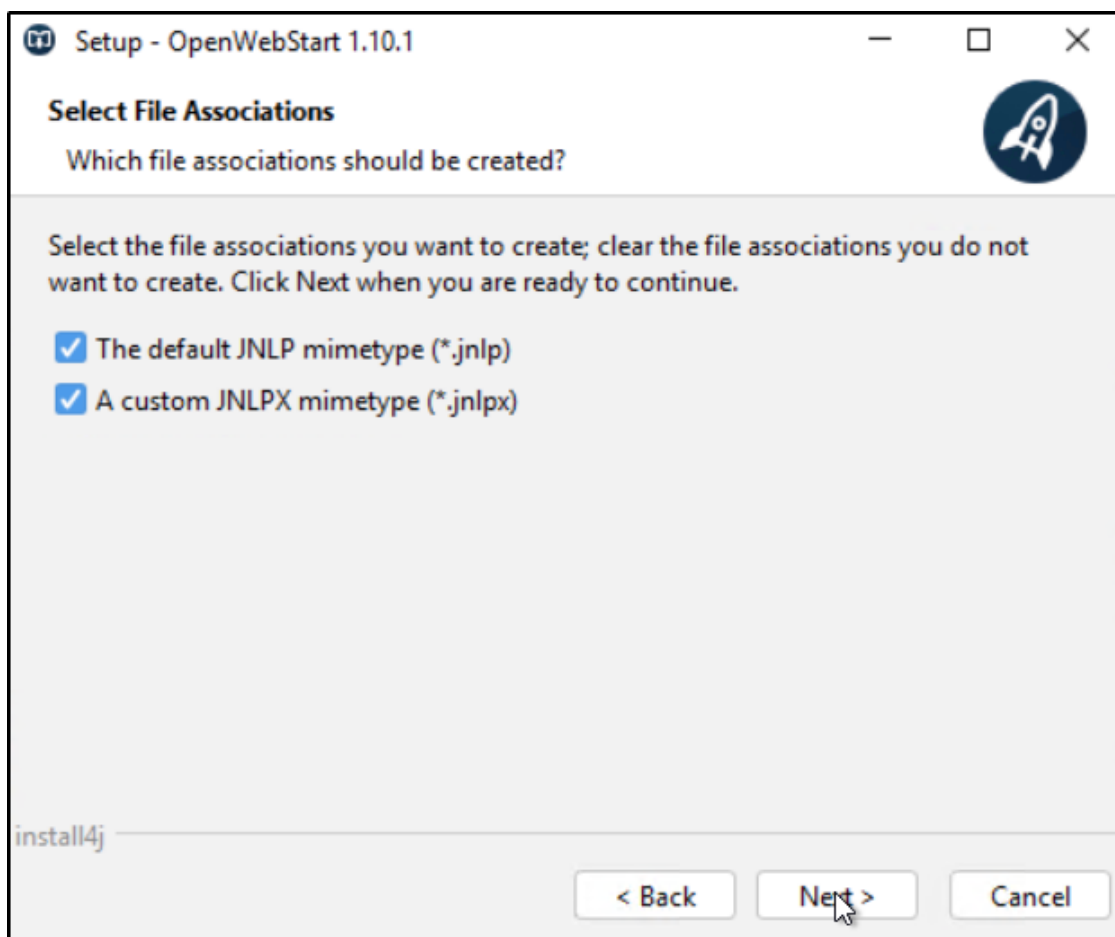
W następnym oknie, Tryb instalacji - dostęp do aplikacji wybrać (default)".



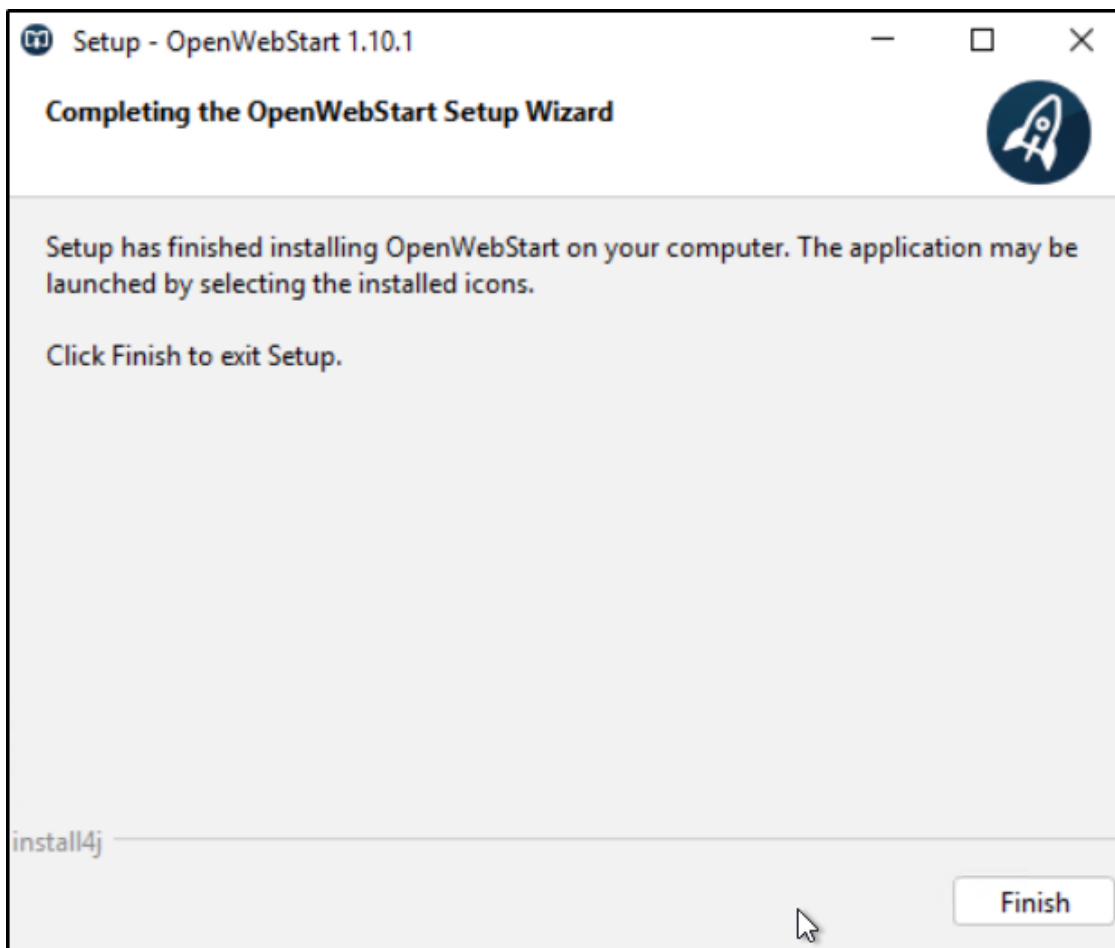
W następnym oknie, informującym o lokalizacji instalacji aplikacji wybrać inne miejsce lub pozostawić domyślne i nacisnąć "Dalej".



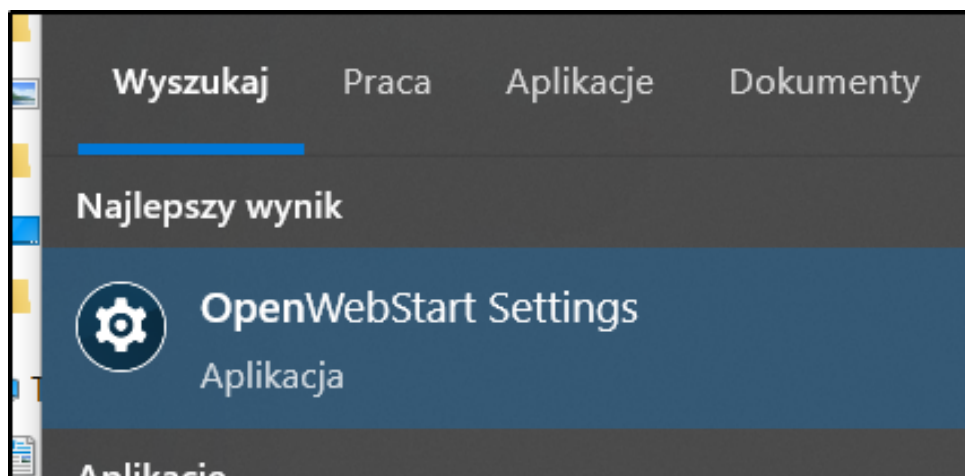
W następnym oknie, informującym, o skojarzeniu pliku(\*.jnlp) z aplikacją OpenWebStart, można zaznaczyć opcje lub odnaczyć domyślne i nacisnąć "Dalej" po tej akcji zostanie uruchomiony proces instalacji aplikacji.



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



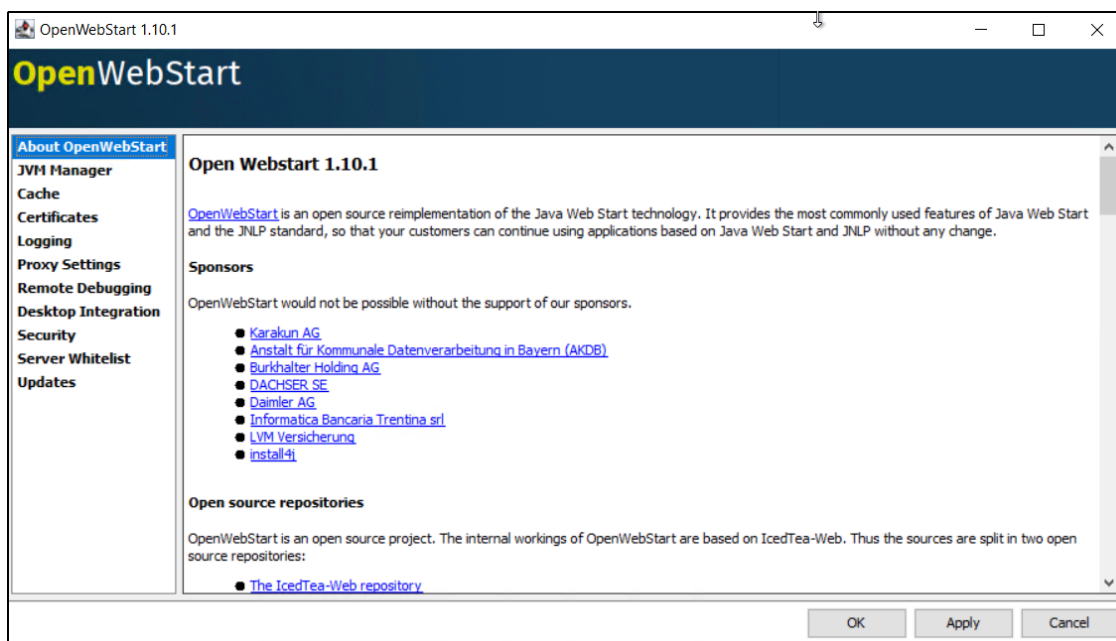
Aplikacja jest gotowa do uruchomienia i należy wykonać polecenie z paska windows OpenWebStart



lub uruchomić ją z lokalizacji

AppData > Roaming > Microsoft > Windows > Start Menu > Programs > OpenWebStart			
Nazwa	Data modyfikacji	Typ	Rozmiar
OpenWebStart Settings	24.06.2024 15:04	Skrót	3 KB

Aplikacja OpenWebStart jest gotowa do pracy.



## Rozdział 4. Pobieranie i zapis na dysku aplikacji e-Podpis (SCSA)

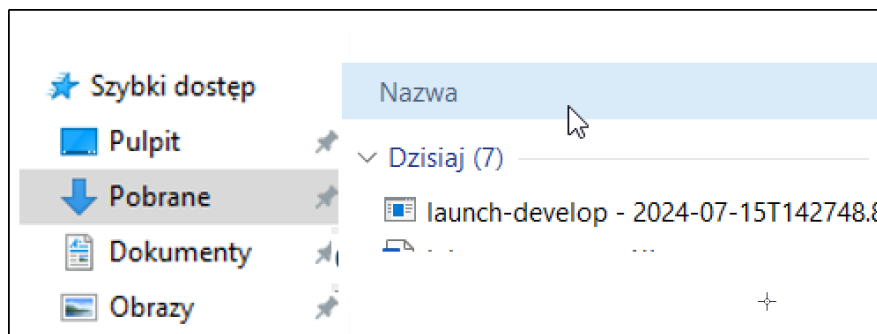
Aplikacje e-Podpis SCSA można pobrać z bankowości elektronicznej poprzez przycisk do uruchomienia w procesie logowania (Zaloguj za pomocą e-Podpisu), lub z linku <https://scsa.cui.pl/webstart>:

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

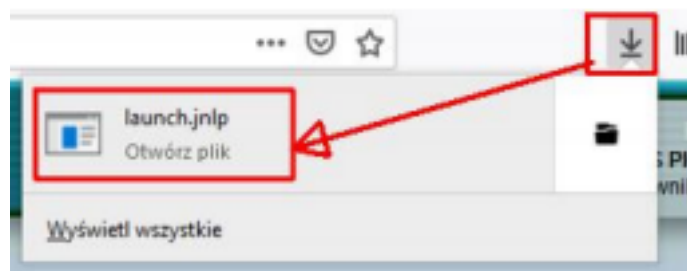
Instalacja skrótu na pulpicie wymaga uruchomienia pobranej aplikacji. Podczas instalacji, w zależności od posiadanej wersji Javy, pojawia się komunikat ostrzegający o otwarciu komponentu Javy



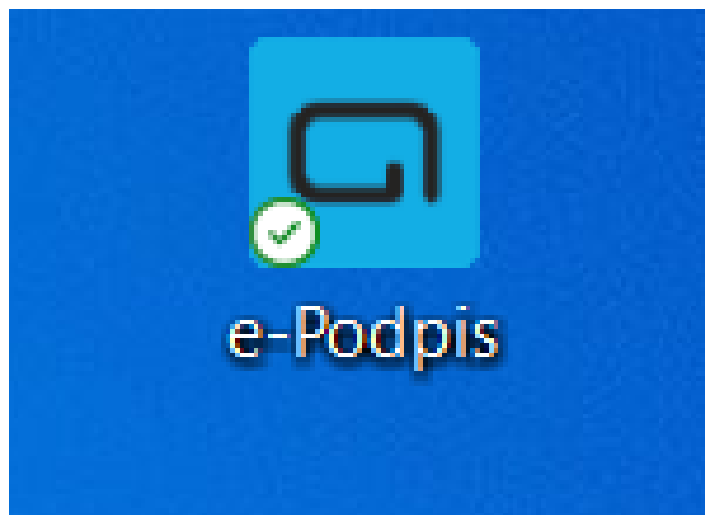
lub jest zapisywany (domyślnie w folderze „Pobrane”) wówczas należy uruchomić pobrany plik z folderu „Pobrane”



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



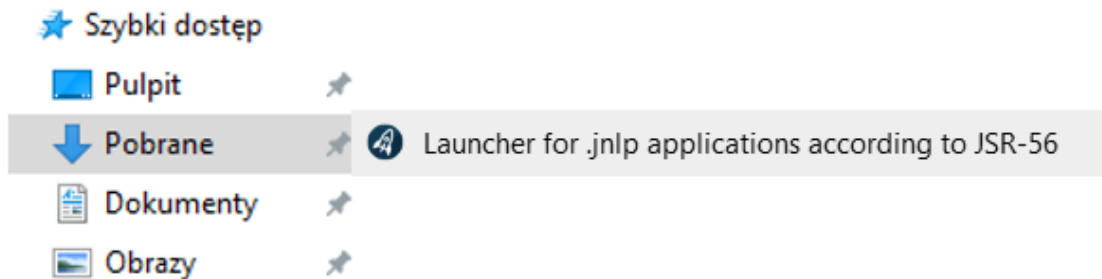
lub uruchomienie ze skrótu na pulpicie dla aplikacji OpenWebStart



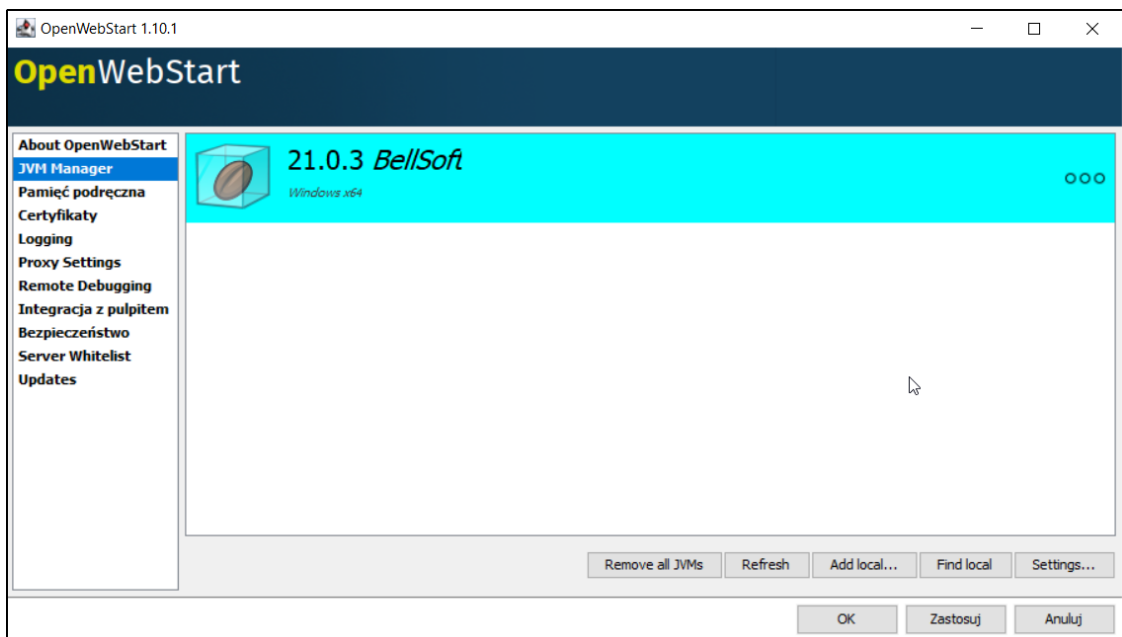
## Rozdział 5. Uruchomienie aplikacji e- Podpis z wykorzystaniem oprogramowania OpenWebStart lub Javy.

Dla aplikacji **OpenWebStart** po uruchomieniu launch-develop proces będzie przebiegał:

- Po kliknięciu zostanie uruchomiony proces aplikacji e-Podpis „**launch.jnlp**”.



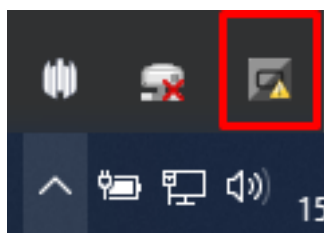
- Uruchomiony zostaje e-Podpis przy pomocy OpenWebStart. Aplikacja automatycznie pobiera wymagane oprogramowanie Java i uruchamia e-Podpis.



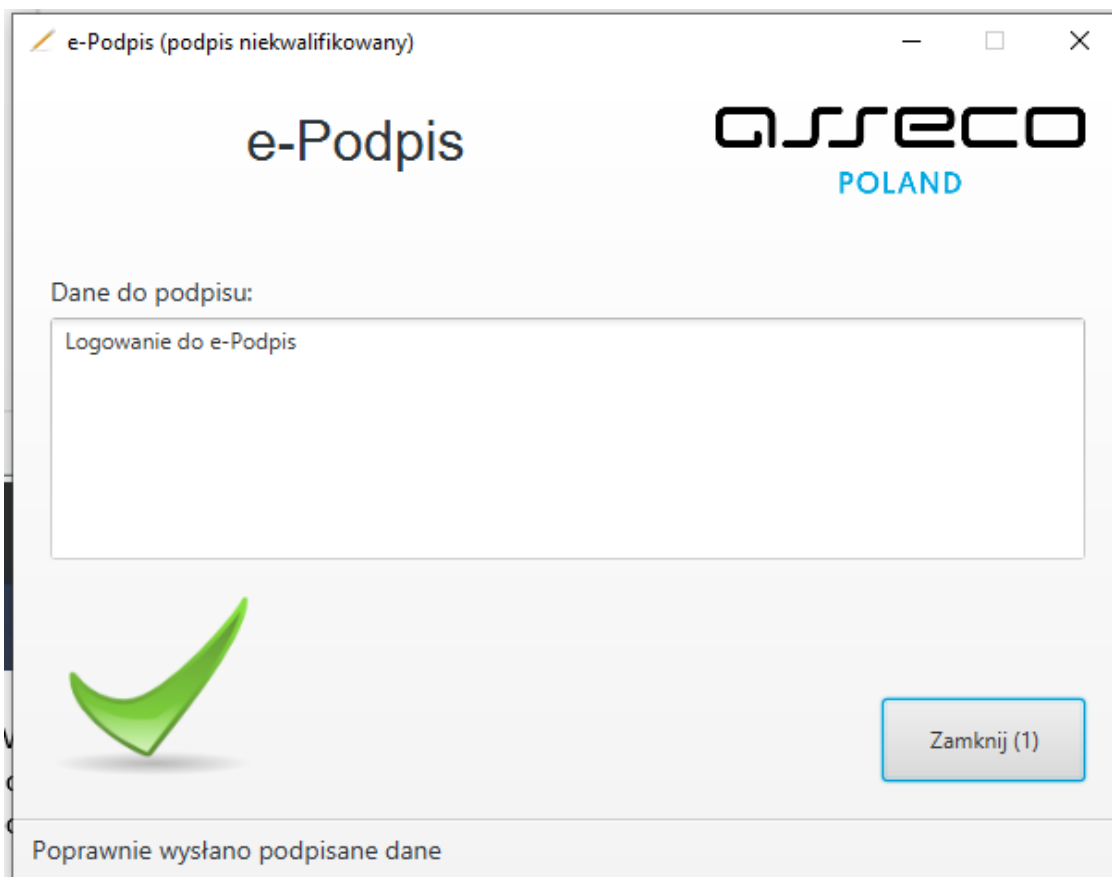
- Należy następnie włożyć kartę do czytnika i zalogować się do e-Podpisu wpisując PIN karty mikroprocesorowej.



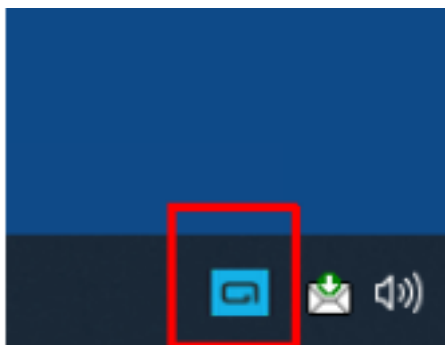
Przed zalogowaniem do aplikacji e-Podpis ikona znajdująca się w zasobniku jest szara (na rzucie ekranu oznaczona czerwonym kwadratem):



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



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 rzucie ekranu oznaczona czerwonym kwadratem)

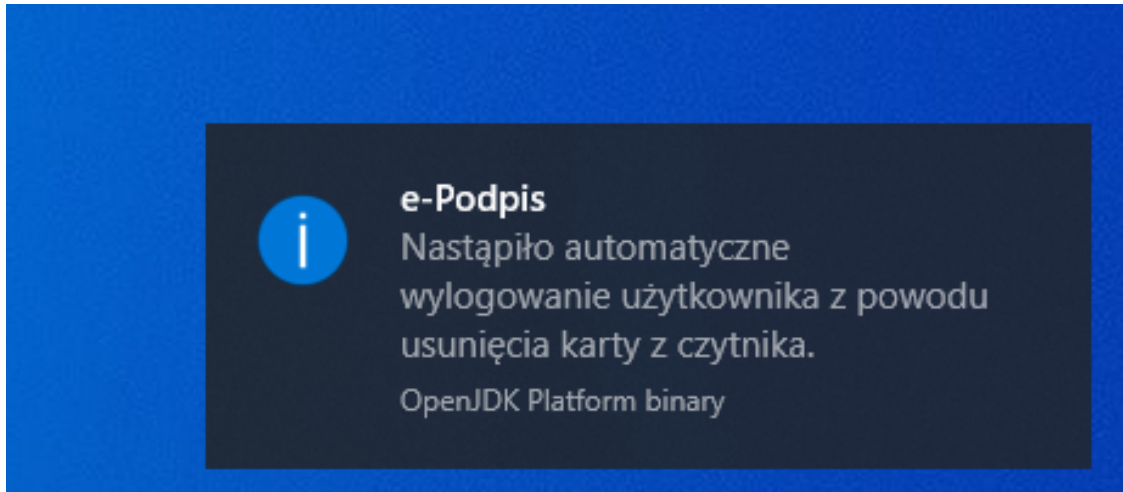


#### WARNING

WAŻNE ZALECENIA BEZPIECZEŃSTWA.

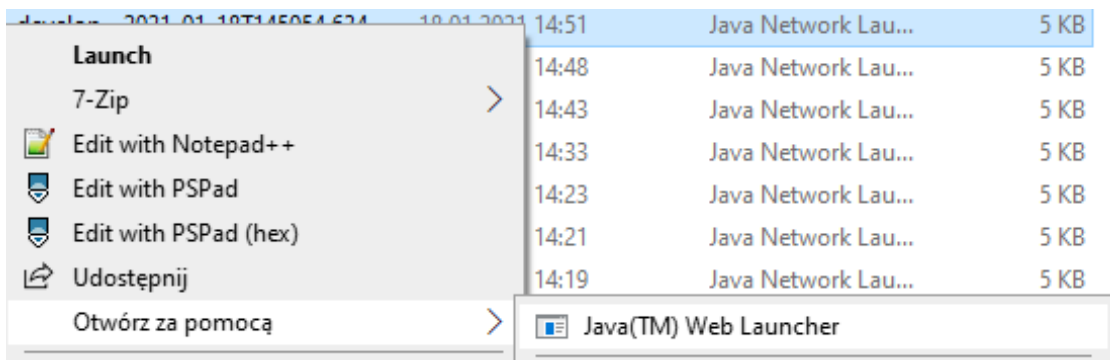
KARTĘ MIKROPROCESOROWĄ WKŁADAMY DO CZYTNIKA KART WYŁĄCZNIE W MOMENCIE PROCESU LOGOWANIA LUB AUTORYZACJI DYSPOZYCJI. NIE JEST ZALECANE, ABY KARTA MIKROPROCESOROWA ZNAJDOWAŁA SIĘ PRZEZ CAŁY CZAS W CZYTNIKU.

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

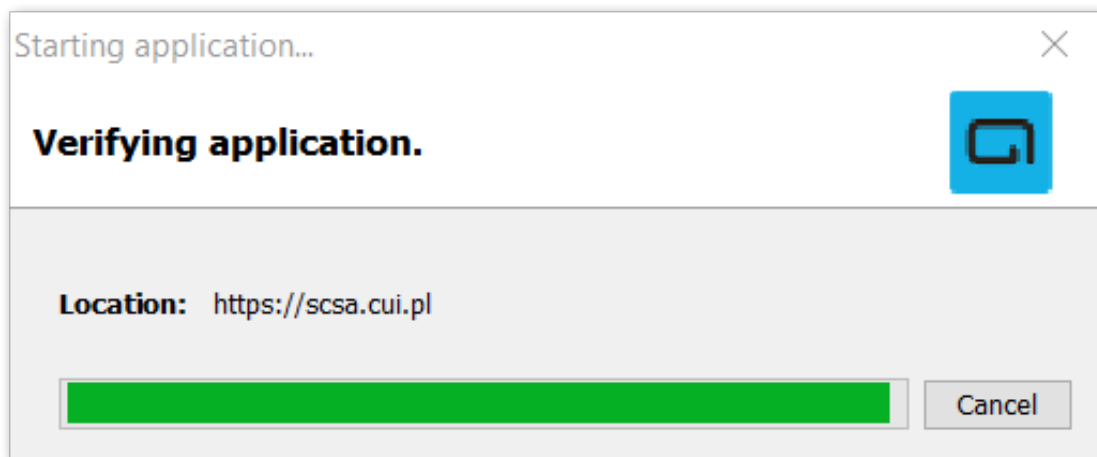


Ikona na pasku narzędzi zmienia się na kolor szary. Dodatkowo prezentowany jest komunikat: „Nastąpiło automatyczne wylogowanie użytkownika z powodu usunięcia karty z czytnika. Włożenie karty do czytnika, gdy aplikacja e-Podpis działa w tle, spowoduje automatyczne wywołanie okna do zalogowania się do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

- 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 zaprezentuje się okno „Logowanie do e-Podpis”.



e-Podpis (podpis niekwalifikowany)

e-Podpis

ASSECO  
POLAND

Dane do podpisu:

Logowanie do e-Podpis

[Zmień metodę akceptacji](#)

Podaj PIN:

Anuluj Podpisz

Dla użytkownika, który nie wykonywał logowania do aplikacji za pomocą e-Podpisu, system zapewni możliwość wyboru metody akceptacji.



Po zdefiniowaniu metody akceptacji, system stworzy na komputerze klienta katalog z plikami c:\Users\imie.nazwisko\.scsa\cui\user-settings.properties służącymi do e-Podpisu.

Plik user-settings.properties będzie zawierał informacje o wybranym typie podpisu umożliwia :

- Podpis kwalifikowany

user.sign.type = QUALIFIED user.sign.type.qualified.provider = KIR\_GRAPHITE

- Podpis niekwalifikowany

user.sign.type = NON\_QUALIFIED

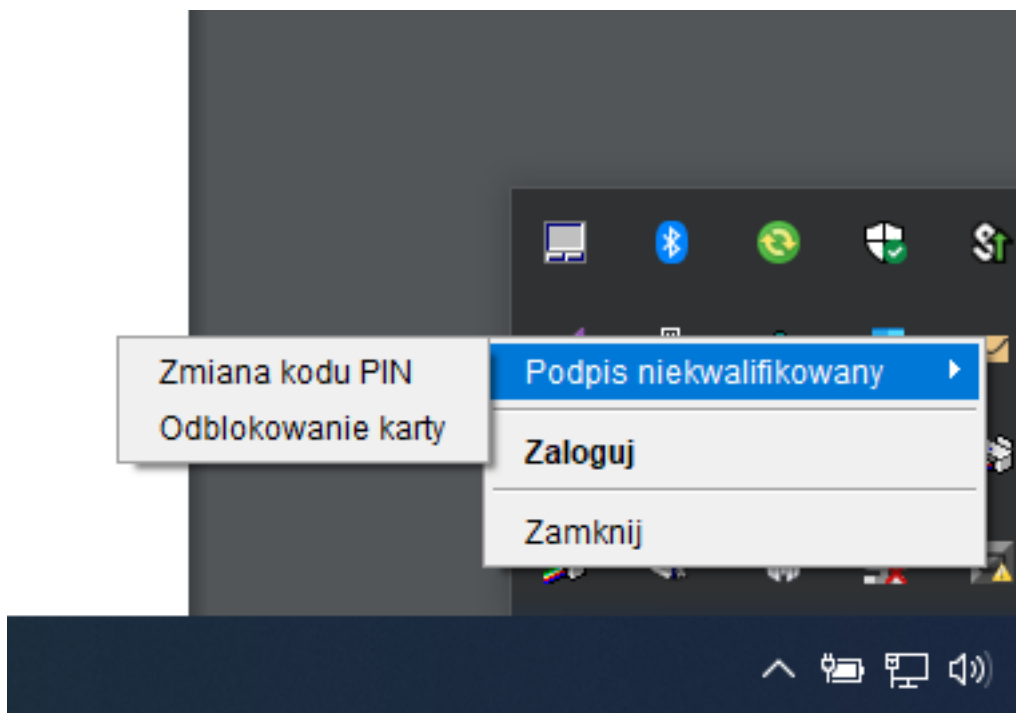
## Rozdział 6. Obsługa e-Podpisu

Jeśli aplikacja została już wcześniej uruchomiona to w zasobniku systemowym wyświetlana jest jej ikona, która umożliwia uruchomienie procesu e-Podpisu w aplikacji.

### 6.1. Podpis niekwalifikowany

Obsługa podpisu niekwalifikowanego umożliwia:

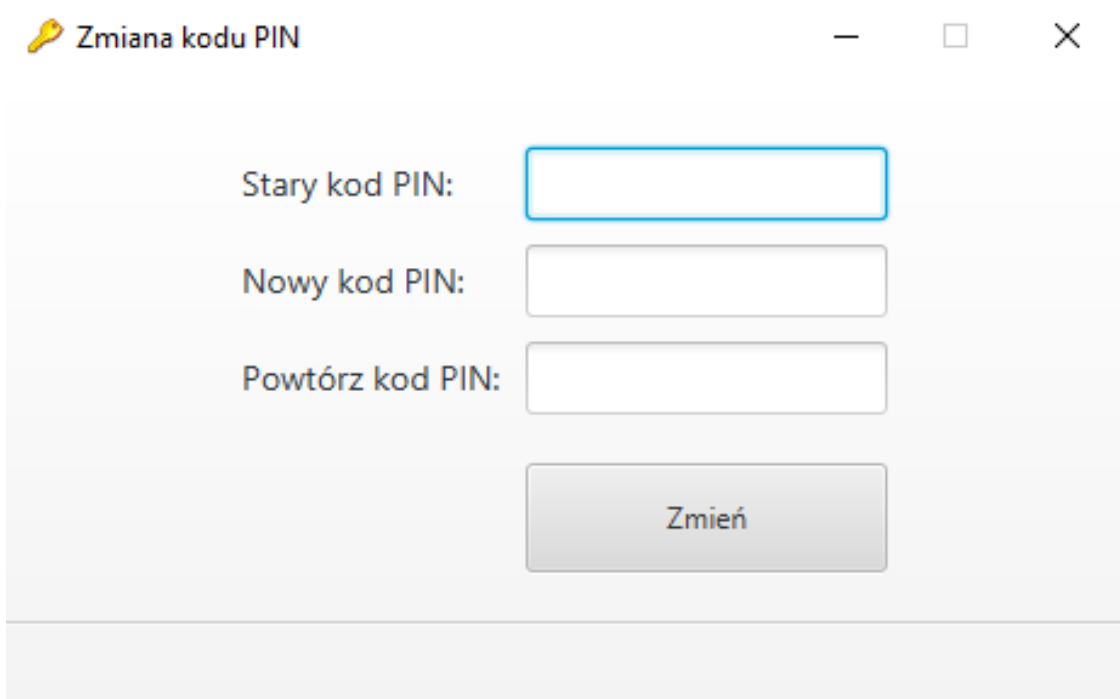
- a) zmianę kodu PIN karty,
- b) odblokowanie karty w przypadku jej zablokowania,
- c) zalogowanie się,
- b) zamknięcie aplikacji e-Podpis.



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**

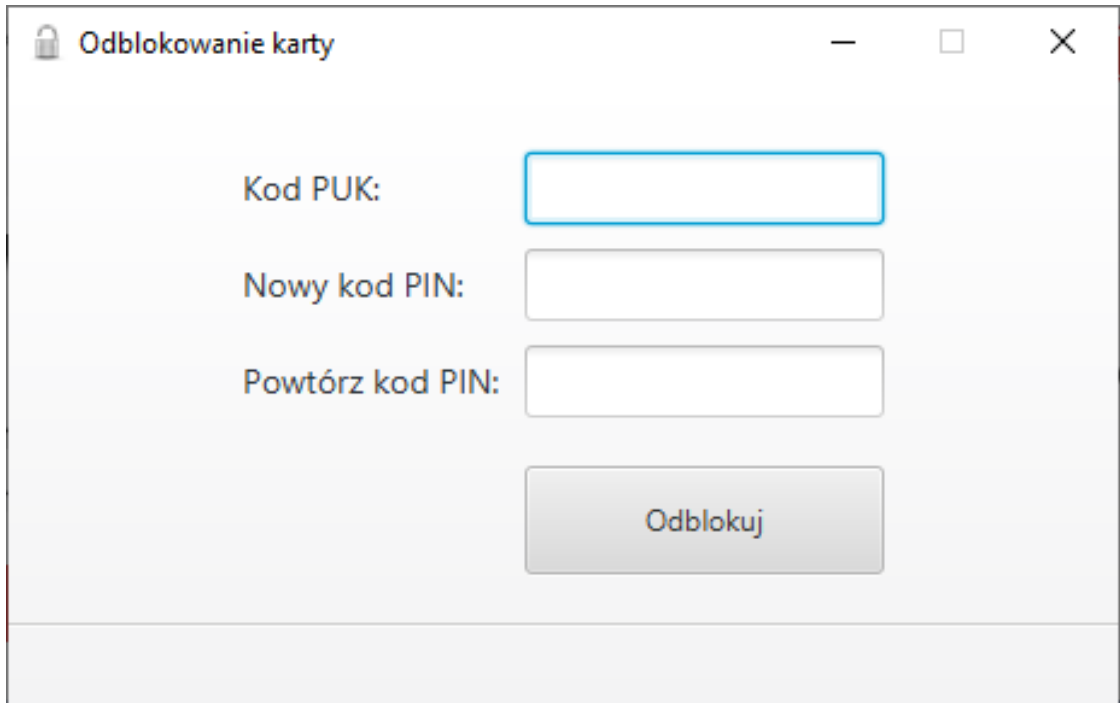
Stary kod PIN:

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:

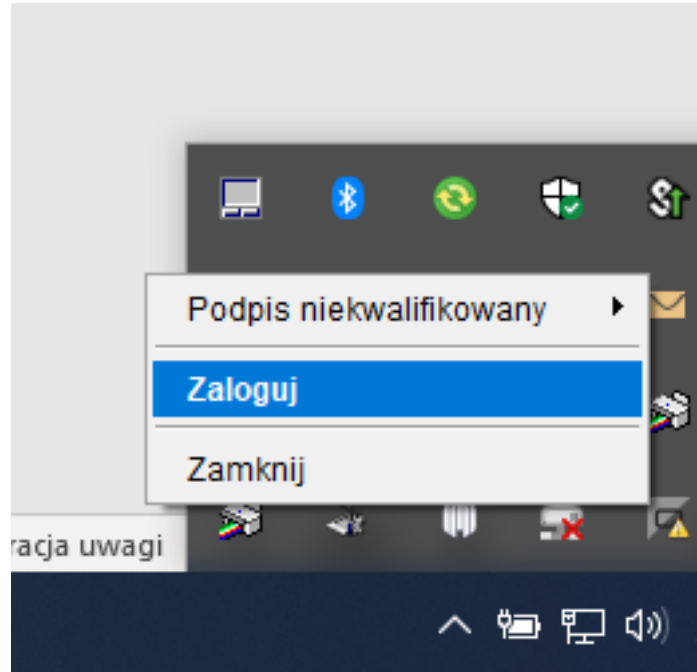
Odblokuj

#### **NOTE**

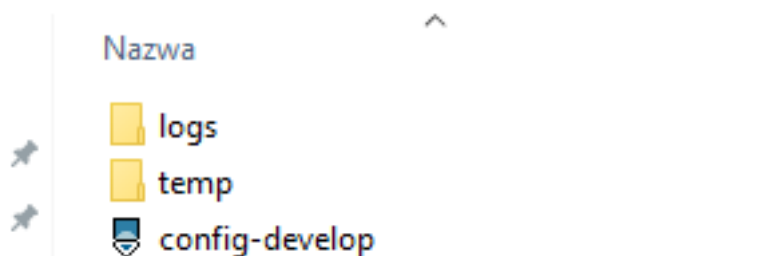
AKTYWNA APLIKACJA E-PODPIS DZIAŁA W TLE NIEZALEŻNIE OD POSIADANEJ PRZEGLĄDARKI INTERNETOWEJ, NA PASKU NARZĘDZI JEST WIDOCZNA JAKO NIEBIESKA

IKONA BANKU [KARTA MIKROPROCESOROWA ZNAJDUJE SIĘ W CZYTNIKU KART].

- **Zalogowanie** - (np. jeden użytkownik zakończył w bankowości podpisywanie, zaczyna pracować drugi i przechodzi do podpisywania - pkt. 6.5).



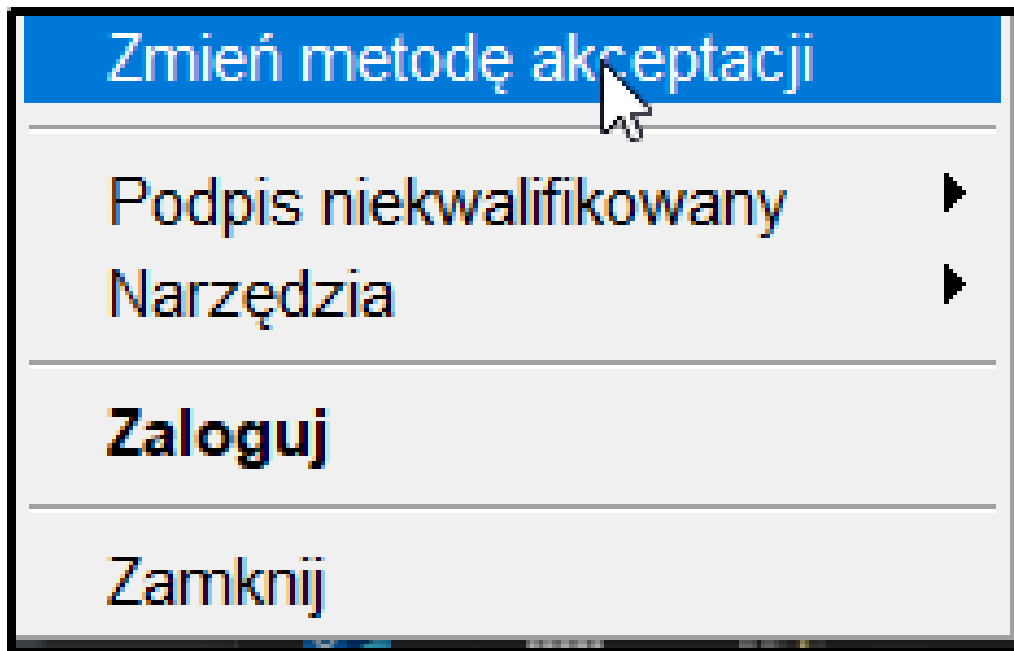
- **Zamknięcie aplikacji** - (do podpisywania konieczne będzie ponowne uruchomienie aplikacji pkt.5.1.)
- **Wyciągnięcie karty mikroprocesorowej z czytnika kart** powoduje wylogowanie z aplikacji e-Podpis, ale nie powoduje wylogowania z bankowości internetowej, ikona na pasku narzędzi jest w kolorze szarym.
- **Logowanie podczas pracy** z aplikacji e-Podpis na komputerze klienta. Logi aplikacji e-Podpis – po pobraniu aplikacji zostaje utworzona struktura (katalog), w którym znajdują się pliki konfiguracyjne oraz logi z działania aplikacji (np. c:\Users\imie.nazwisko\scsa\cui\).



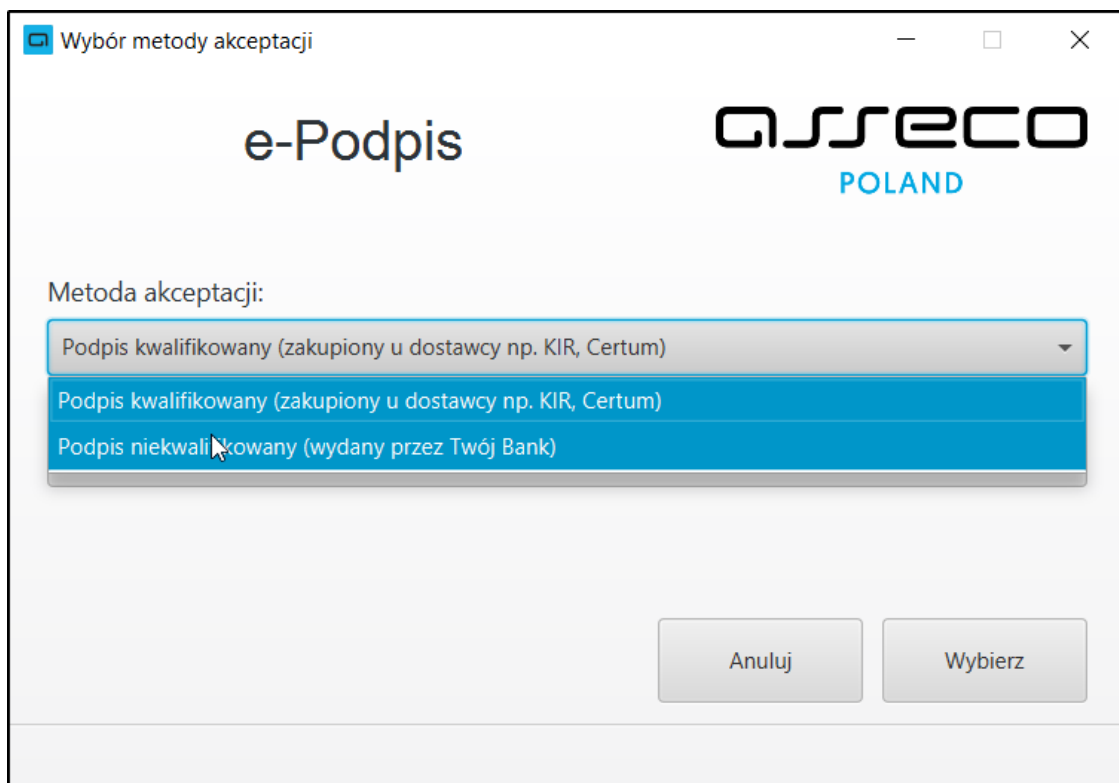
## 6.2. Podpis kwalifikowany

W celu wybrania jako środka do autentykacji użytkownika i autoryzację zleceń poprzez Podpis Kwalifikowany należy wybrać

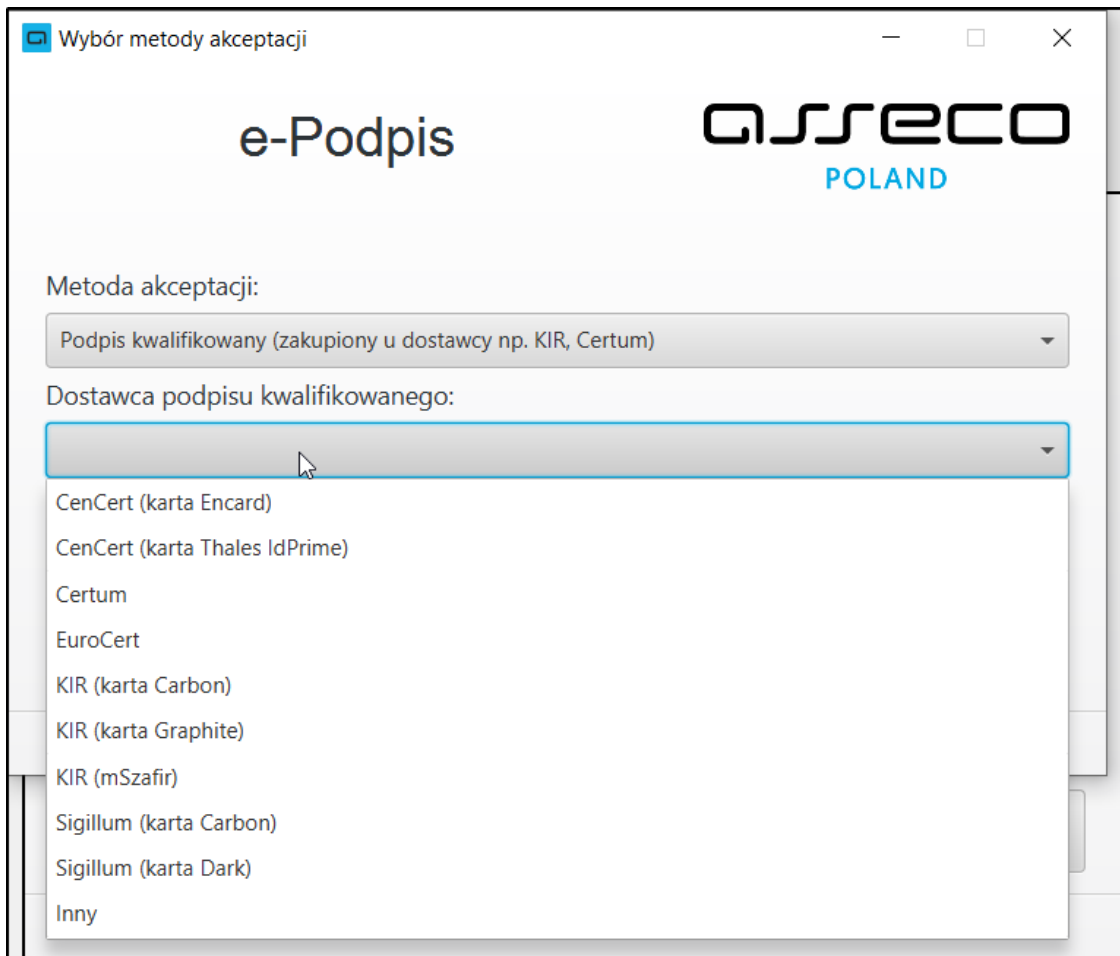
"Przycisk "zmień metodę akceptacji" pozwalający na wybranie jako używanej metody Podpisu kwalifikowanego.



- **Zmień metodę akceptacji** powoduje otwarcie nowej formatki do ustawiania metody akceptacji użytkownik ma możliwość wybrania:
  - Podpis niekwalifikowany - wydany przez Twój Bank
  - Podpis kwalifikowany - zakupiony u dostawcy np. KIR, Certum



Dla przypadku wybrania opcji Podpis kwalifikowany użytkownik dodatkowo wybiera dostawcę podpisu kwalifikowanego.



Wybór metody akceptacji

e-Podpis

ASSECO  
POLAND

Metoda akceptacji:

Podpis kwalifikowany (zakupiony u dostawcy np. KIR, Certum)

Dostawca podpisu kwalifikowanego:

- CenCert (karta Encard)
- CenCert (karta Thales IdPrime)
- Certum
- EuroCert
- KIR (karta Carbon)
- KIR (karta Graphite)
- KIR (mSzafir)
- Sigillum (karta Carbon)
- Sigillum (karta Dark)
- Inny

Po wybraniu dostawcy należy wybrać opcje Wybierz. Dla użytkownika prezentowana jest formatka do logowania podpisu kwalifikowanego:

- Certyfikat - wybór certyfikatu dostarczonego dla podpisu kwalifikowanego
- Podaj PIN - Pin ustalony dla podpisu kwalifikowanego

e-Podpis (podpis kwalifikowany)

e-Podpis **ASSECO**  
POLAND

Dane do podpisu:

Logowanie do e-Podpis

[Zmień metodę akceptacji](#)

Certyfikat:

Podaj PIN:

Anuluj Podpisz

## Rozdział 7. Logowanie do systemu bankowości internetowej def3000/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 oprogramowanie: OpenWebStart lub Java.

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

- Na stronie do logowania podajemy identyfikator klienta, który ma w aplikacji BackOffice skonfigurowany logowanie i autoryzację jako Karta mikroprocesorowa.

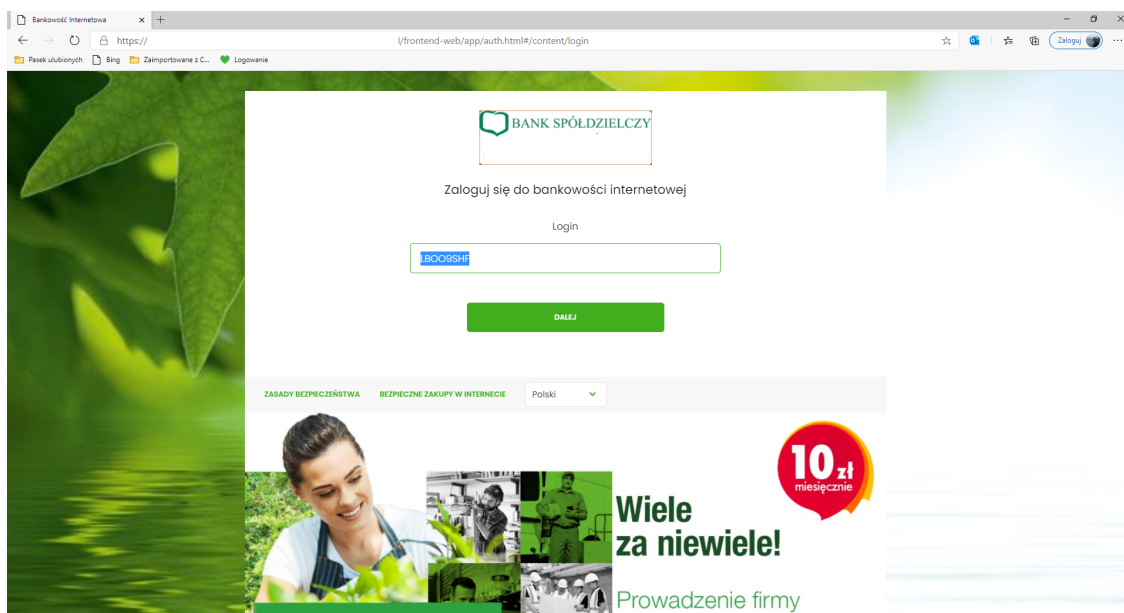
<b>Nr telefonu:</b>	489999999999
<b>Priorytetowe urządzenie do logowania:</b>	Karta mikroprocesorowa
<b>Priorytetowe urządzenie do autoryzacji:</b>	Karta mikroprocesorowa
<b>Status użytkownika:</b>	Aktywny

---

---

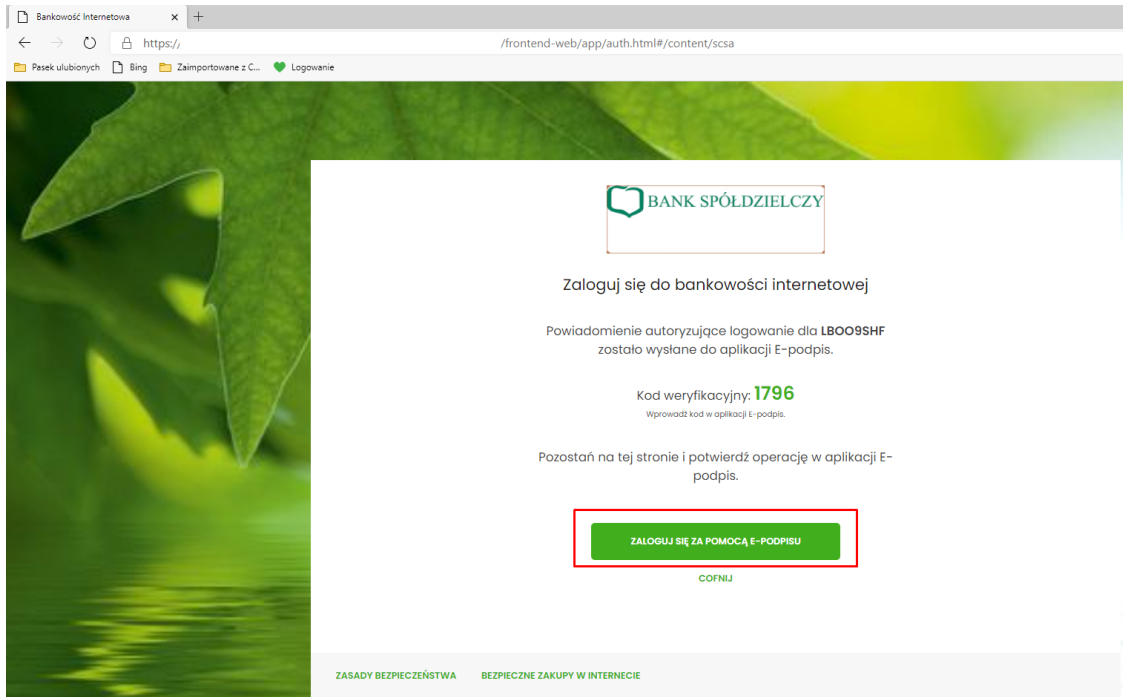
---

- Podaj identyfikator klienta i wybierz [DALEJ].

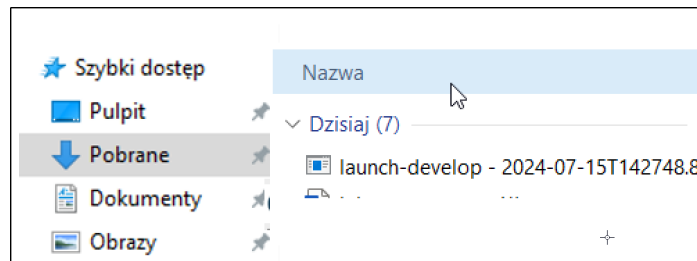


- Po wpisaniu identyfikatora zostaniemy przeniesieni do kolejnej strony, na której będziemy mieć możliwość pobrania i uruchamiania e-Podpisu (SCSA) poprzez wybranie opcji:” Zaloguj się za pomocą E-Podpisu”. Na formatce zostanie zaprezentowany: Identyfikator osoby logującej się i kod

weryfikacyjny.

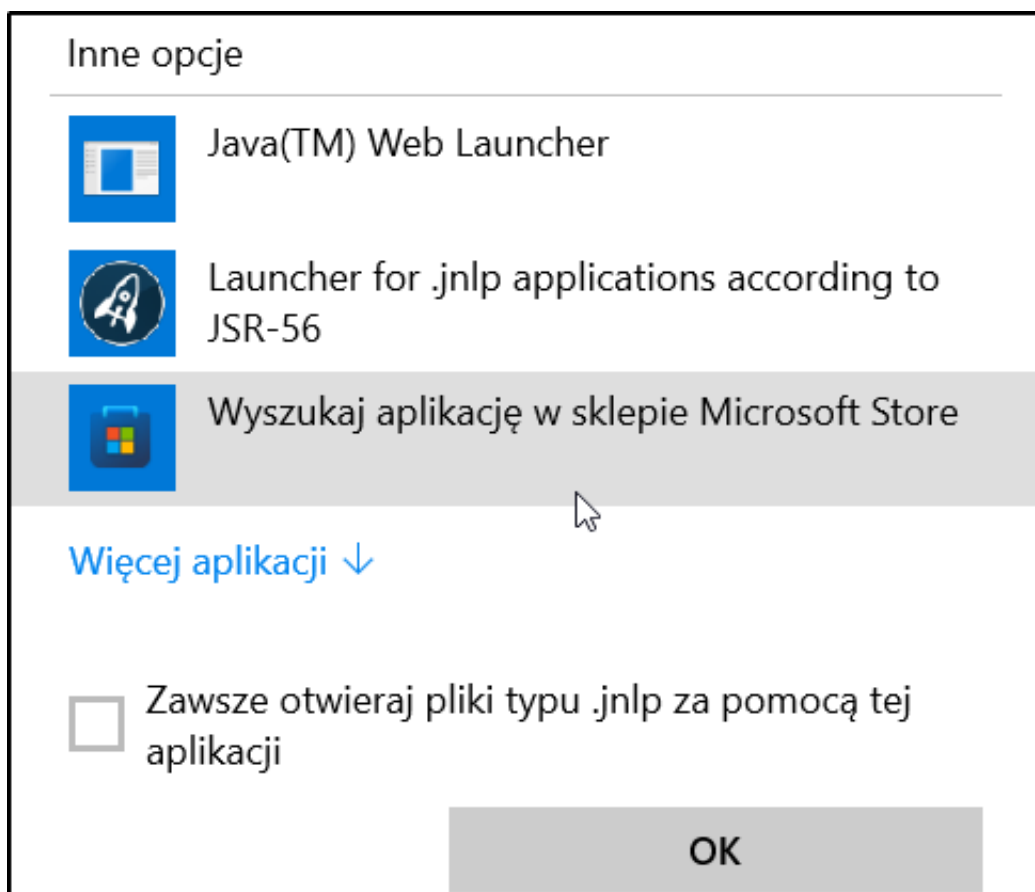


- Po wybraniu opcji [ZALOGUJ SIĘ ZA POMOCĄ E-PODPISU]” zostanie pobrany plik „launch-develop.jnlp”. W zależności od przeglądarki plik „launch.jnlp” może zostać bezpośrednio uruchomiony – przycisk „Otwórz” lub jest zapisywany (domyślnie w folderze „Pobrane”) i wtedy należy uruchomić pobrany plik z folderu „Pobrane”



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

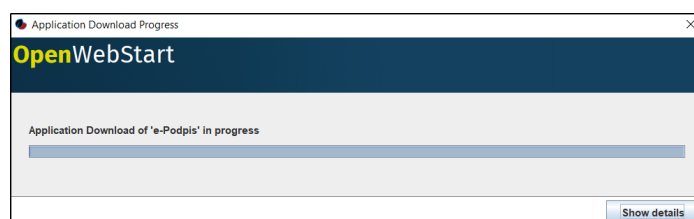
Dla uruchomienia poprzez OpenWebStart będziemy mieć:



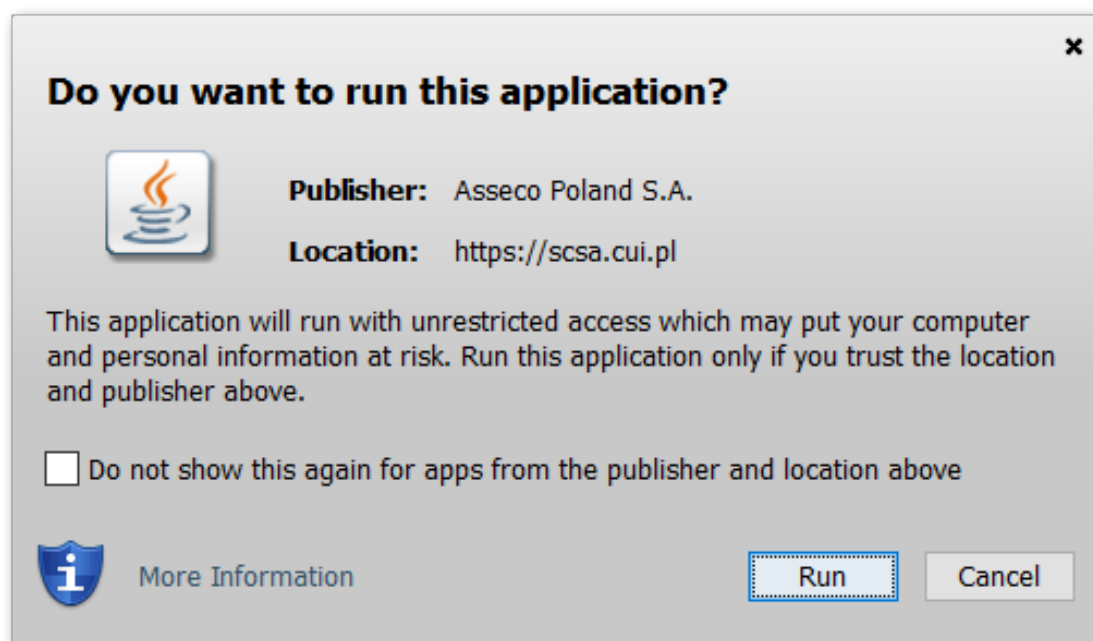
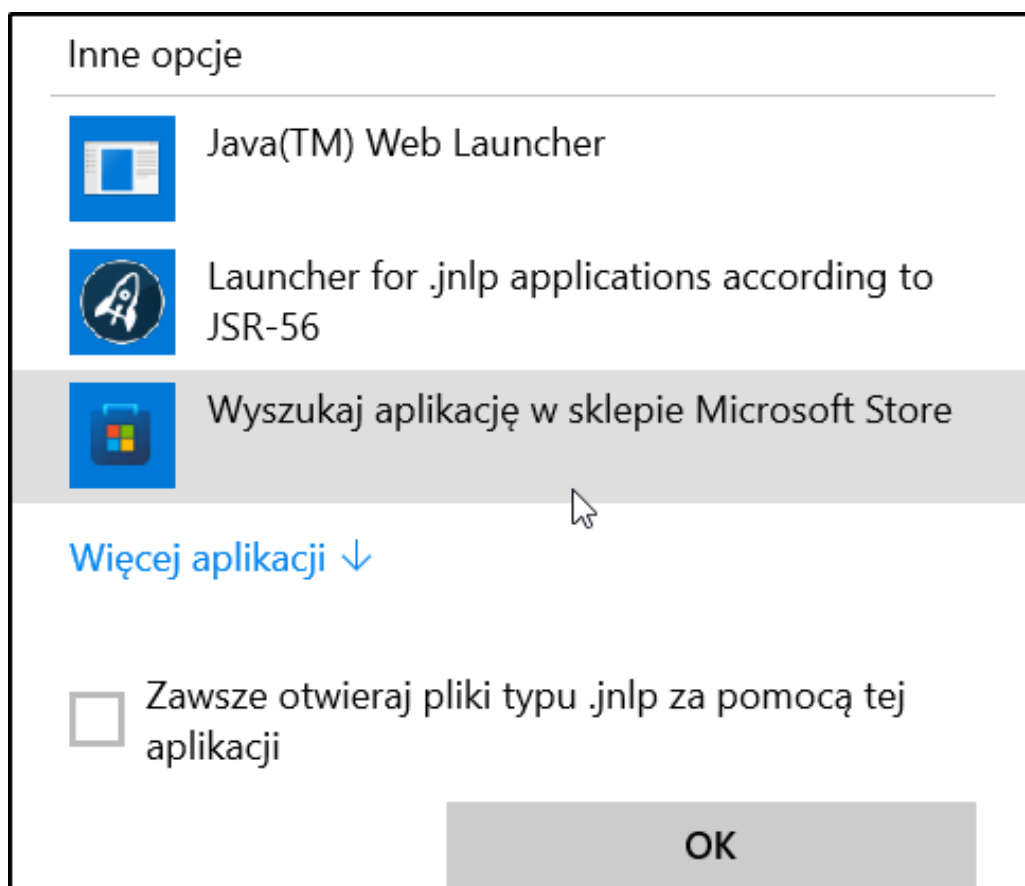
lub skrótu na pulpicie



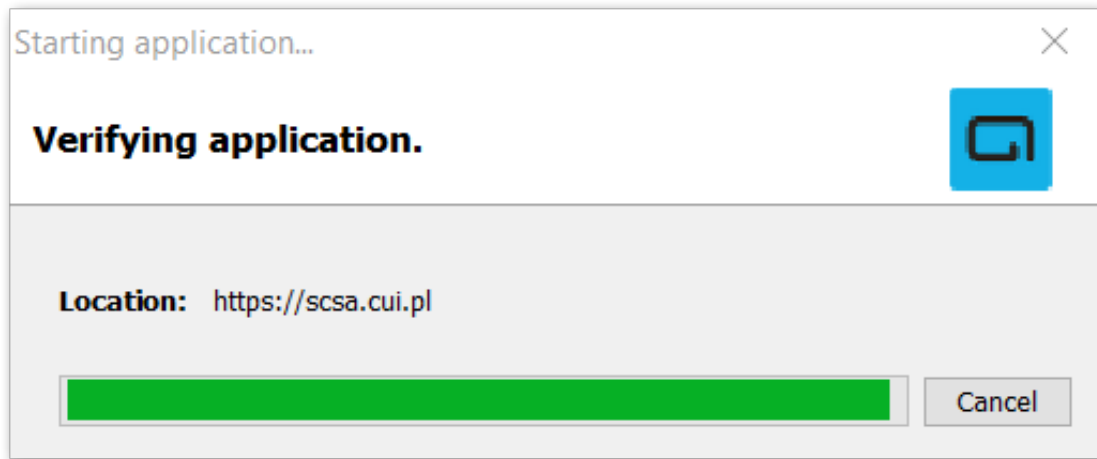
W kolejnym oknie wyświetlana jest informacja o pobieraniu przez e-Podpis danych z <https://scsa.cui.pl/webstart>.



Dla uruchomienia z pomocą **Java** będziemy mieć:



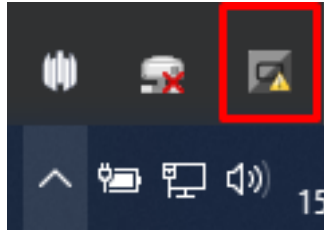
Po uruchomieniu aplikacji przy pomocy Java, system wyświetli okno, w którym będzie zaprezentowane okno do weryfikacji danych.



Po poprawnej weryfikacji zaprezentuje się okno „Logowanie do e-Podpis”.

Po poprawnym przejściu kroków konfiguracji należy włożyć kartę do czytnika i zalogować się do e-Podpisu wpisując PIN karty mikroprocesorowej.

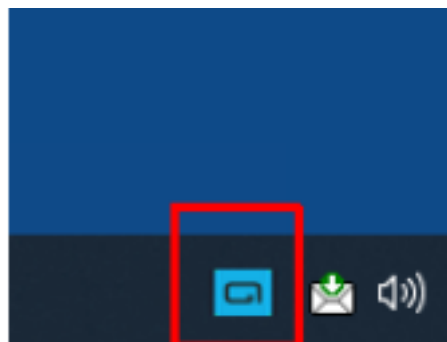




W oknie dialogowym „Dane do podpisu” pojawia się komunikat „Logowanie do e-Podpis”. Prawidłowe podanie kodu PIN powoduje zalogowanie do e-Podpisu i pojawienie się komunikatu „Poprawnie wysłano podpisane dane”.



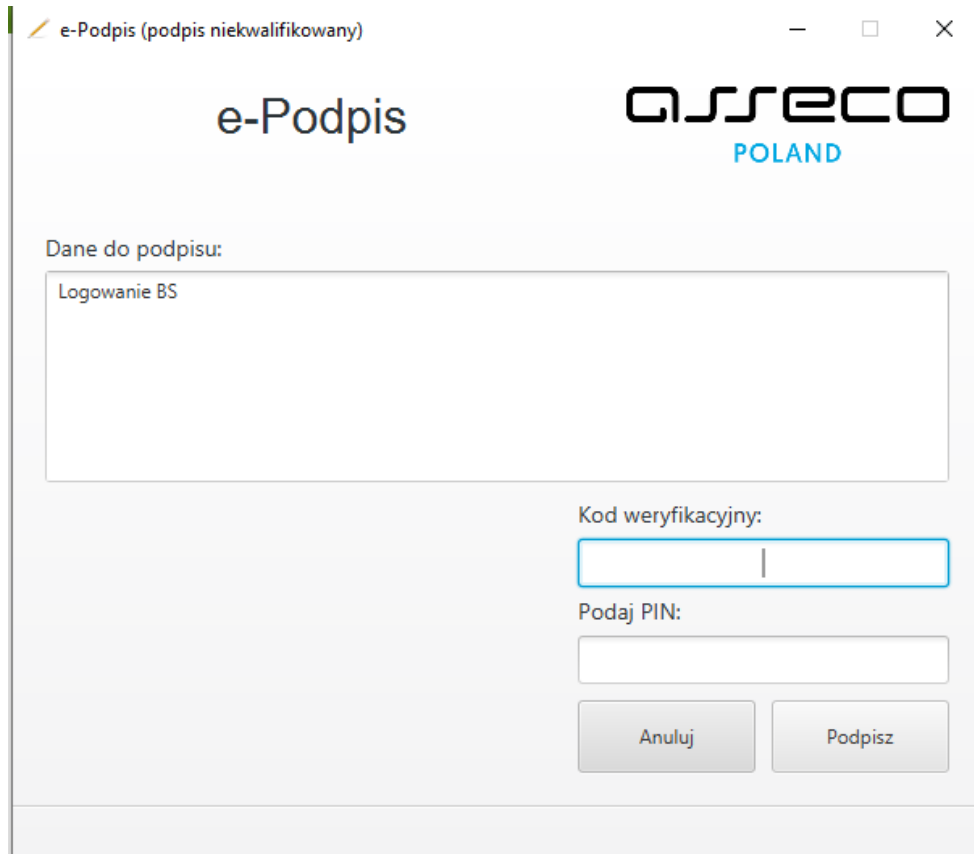
Powyższe okno dialogowe można zamknąć po kliknięciu na klawisz „Zamknij” lub poczekać, aż zostanie zamknięte samoczynnie po upływie 3 sekund. Zalogowanie do e-Podpisu jest sygnalizowane niebieską ikonką w zasobniku systemowym.



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

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

Dla e-Podpis(podpis niekwalifikowany)



Dla e-Podpis(podpis kwalifikowany)



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

Dla e-Podpis(podpis niekwalifikowany)

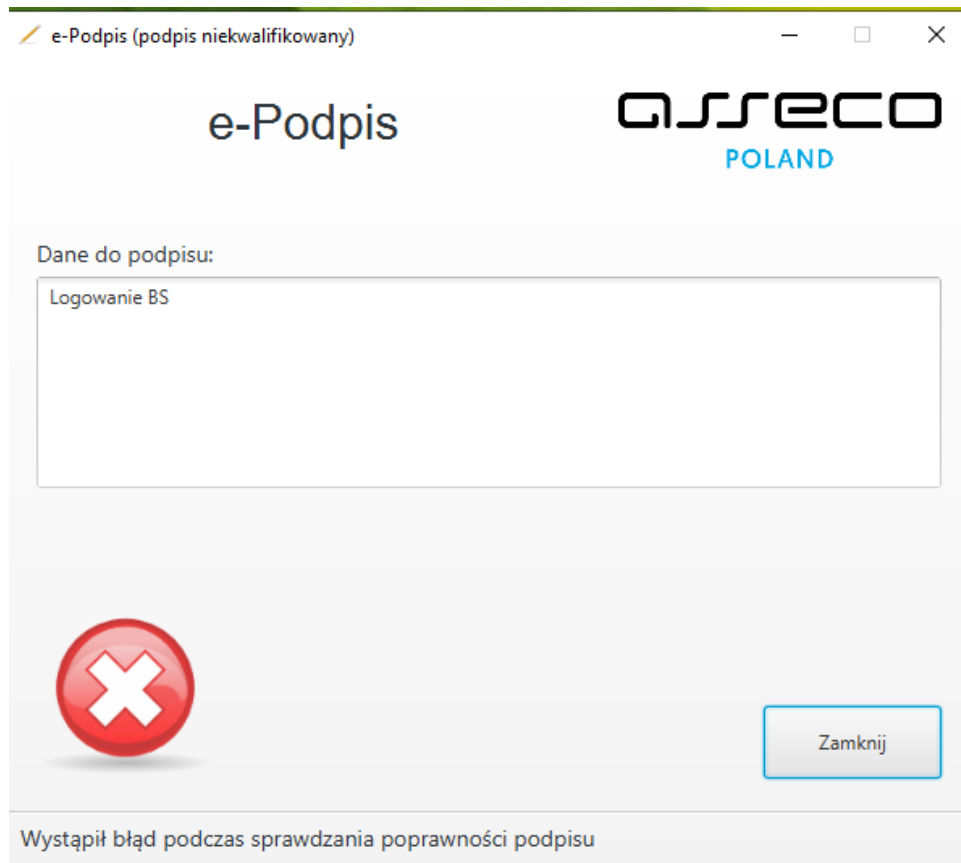


Dla e-Podpis(podpis kwalifikowany)



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

Dla e-Podpis(podpis niekwalifikowany)



Dla e-Podpis(podpis kwalifikowany)

e-Podpis (podpis kwalifikowany)

e-Podpis **ASSECO**  
POLAND

Dane do podpisu:

Logowanie do e-Podpis


[Zmień metodę akceptacji](#)

Certyfikat:  
CN= [REDACTED]

Podaj PIN:  
[ ]

Anuluj Podpisz

Wystąpił błąd podczas podpisywania danych



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

Dla e-Podpis(podpis niekwalifikowany)

e-Podpis (podpis niekwalifikowany)

e-Podpis **ASSECO**  
POLAND

Dane do podpisu:

Logowanie BS

Kod weryfikacyjny:

Podaj PIN:



Wystąpił błąd podczas podpisywania danych

Dla e-Podpis(podpis kwalifikowany)

e-Podpis (podpis kwalifikowany)

e-Podpis **assecO**  
POLAND

Dane do podpisu:

Logowanie BS

Kod weryfikacyjny:  
9480

Certyfikat:  
CN= [REDACTED]

Podaj PIN:  
[REDACTED]

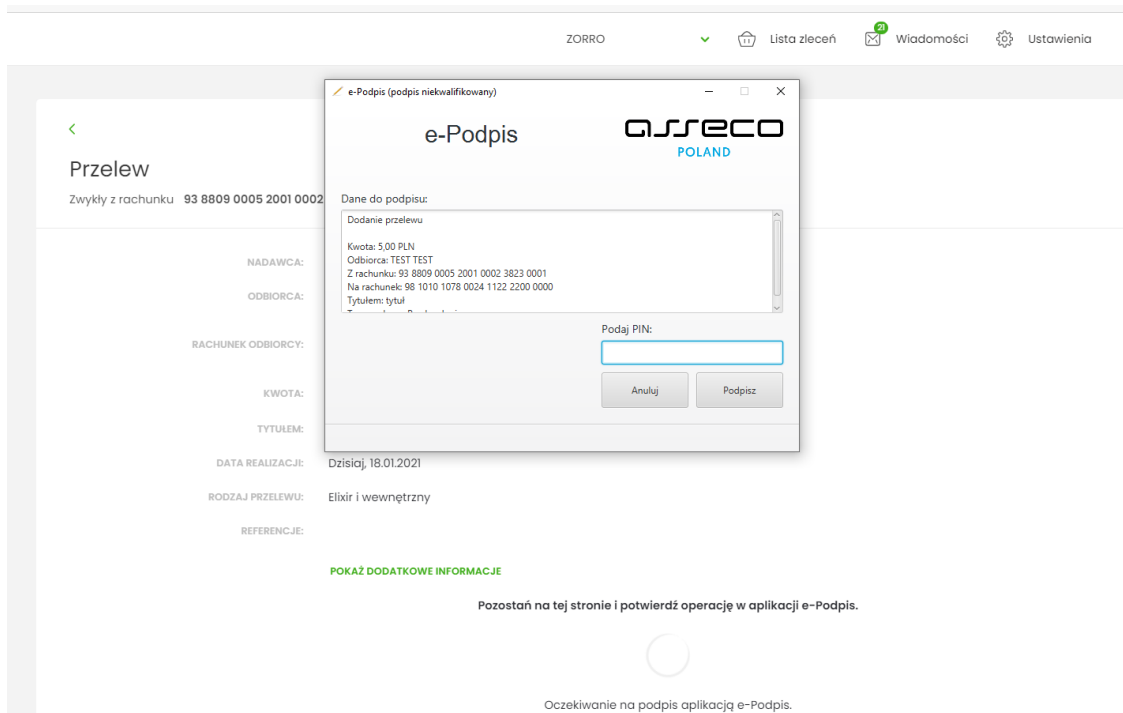
Anuluj Podpisz



Wystąpił błąd podczas podpisywania danych

## Rozdział 8. Autoryzacja zleceń za pomocą karty mikroprocesorowej

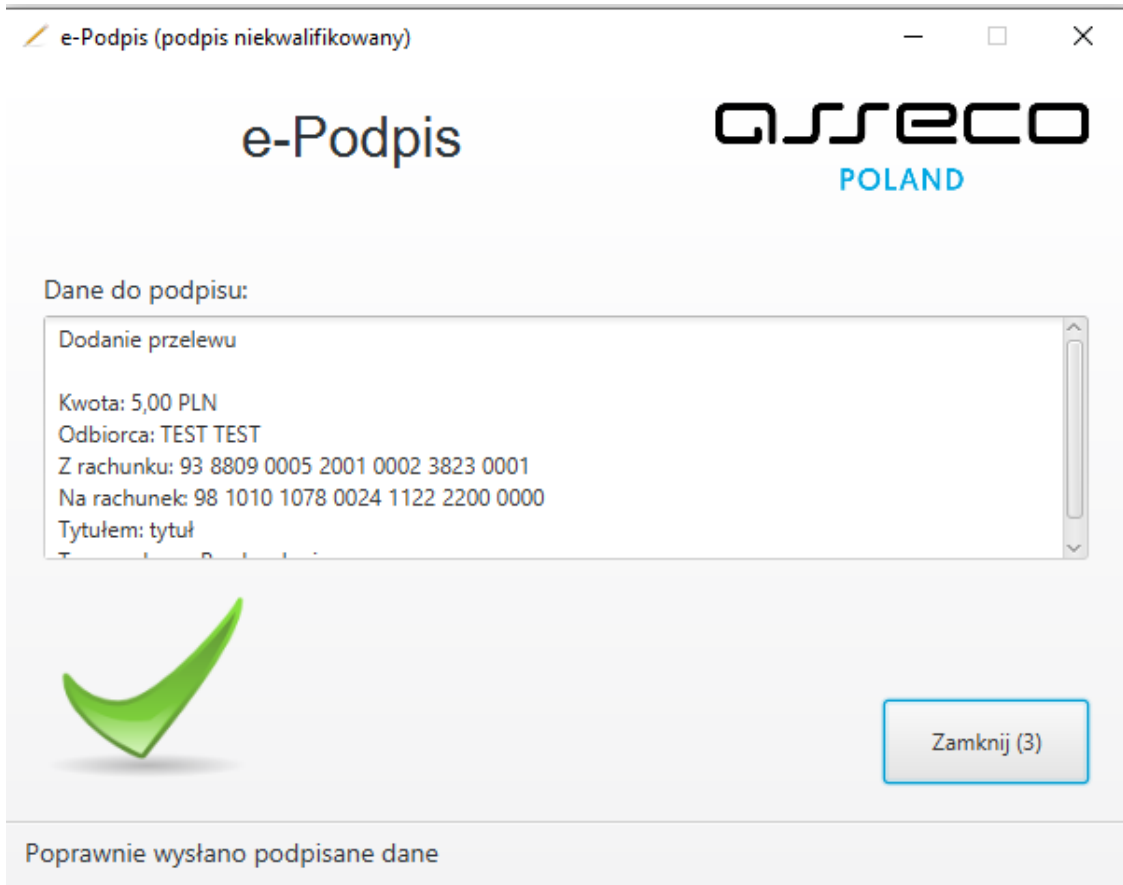
Na formatce dyspozycji dodania przelewu, w systemie def3000/EBP, po wprowadzeniu danych wybieramy [dalej]. System prezentuje formularz potwierdzenia wprowadzonych danych wraz z oknem do wprowadzenia kodu PIN.



Na formularzu E-PODPIS dostępne są akcje:

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

Dla e-Podpis(podpis niekwalifikowany)



Dla e-Podpis(podpis kwalifikowany)



e-Podpis

**ASSECO**  
POLAND

Dane do podpisu:

Dodanie przelewu

Kwota: 12,01 PLN

Odbiorca: Tomasz Wilk ul. Zimna 12 34-098 Warszawa

Z rachunku: 18 9101 0003 2003 0001 1336 0001

Na rachunek: 20 1140 2017 0000 4302 0510 6903

Tytułem: Aktualzacja danych adresu danych:

Certyfikat:

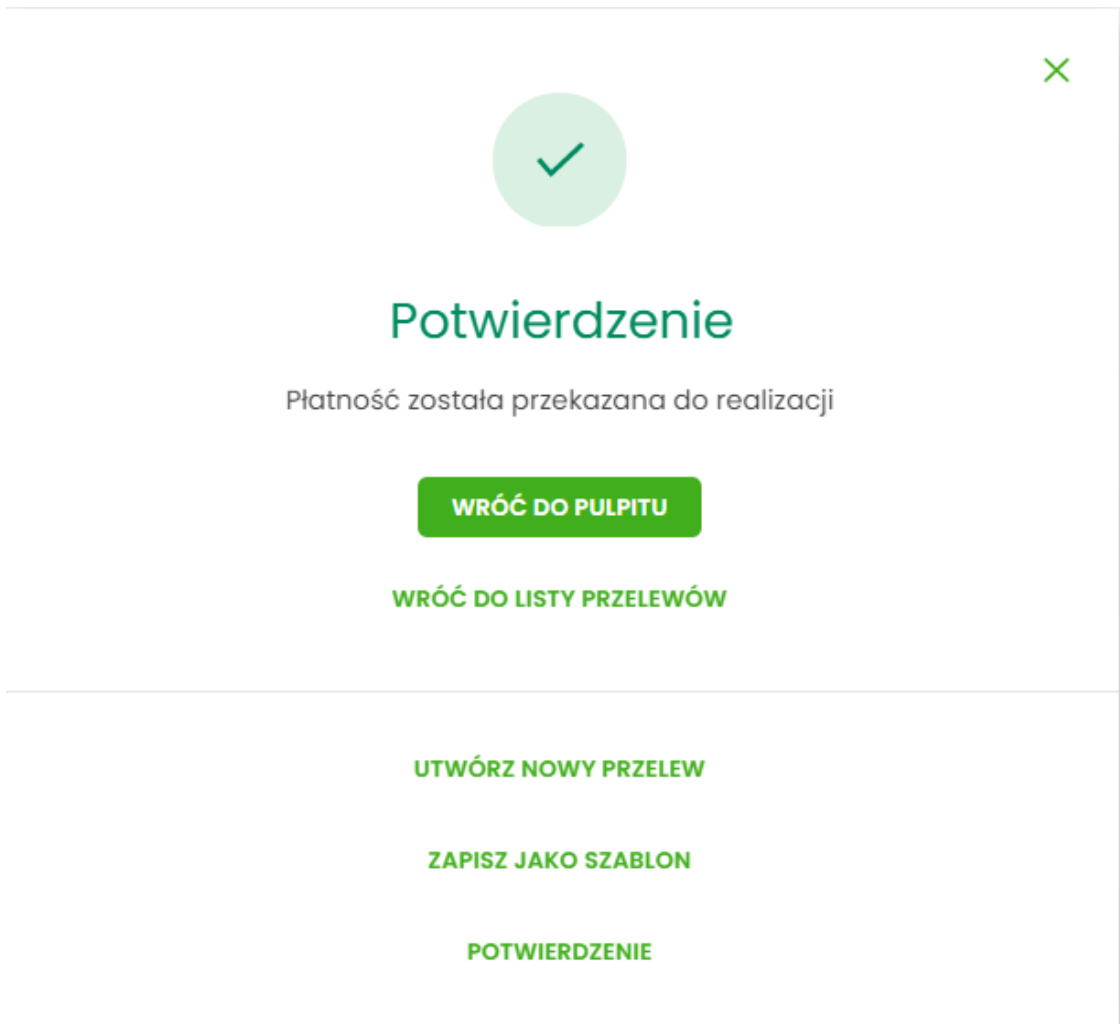
CN=...,serial...

Podaj PIN:

Anuluj

Podpisz

Po naciśnięciu [ZAMKNIJ] system def3000/EBP, 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:

Dla e-Podpis(podpis niekwalifikowany)

e-Podpis (podpis niekwalifikowany)

e-Podpis **ASSECO**  
POLAND

Dane do podpisu:

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  
Tytułem: tytuł

Podaj PIN:

Anuluj Podpisz

Wystąpił błąd podczas podpisywania danych

Dla e-Podpis(podpis kwalifikowany)

e-Podpis (podpis kwalifikowany)

e-Podpis **ASSECO**  
POLAND


Dane do podpisu:

Dodanie przelewu

Kwota: 12,01 PLN  
Odbiorca: Tomasz Wilk ul. Zimna 12 34-098 Warszawa  
Z rachunku: 18 9101 0003 2003 0001 1336 0001  
Na rachunek: 20 1140 2017 0000 4302 0510 6903  
Tytułem: Aktualzacja danych adresu danych:

Certyfikat:  
CN= [redacted]

Podaj PIN:

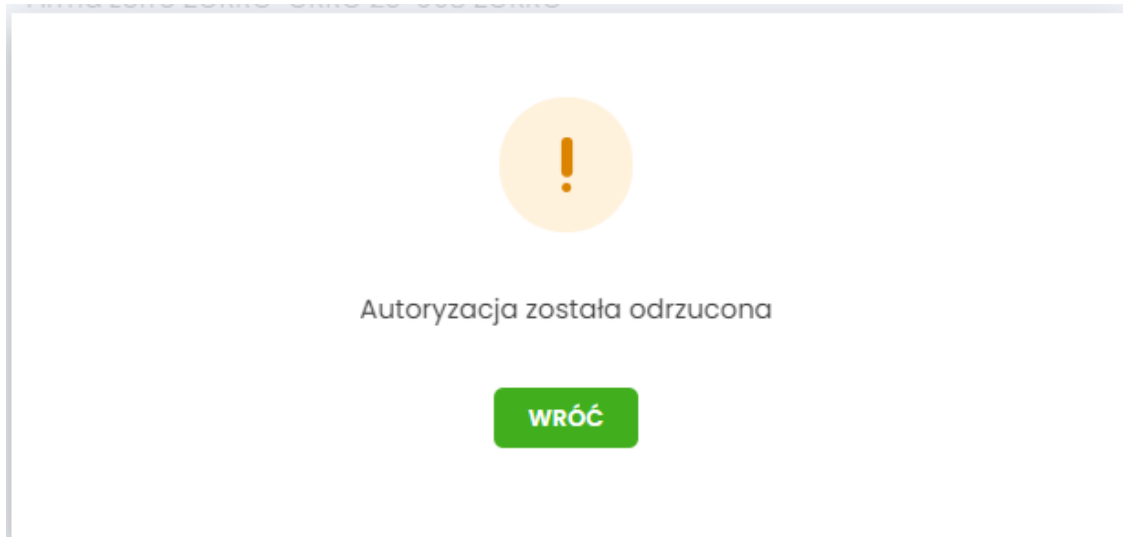


Wystąpił błąd podczas podpisywania danych

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 def3000/EBP prezentuje następujący komunikat:



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.