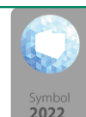




Podręcznik użytkownika aplikacji SCSA (ePodpis)

Wstęp

W bankowości elektronicznej dla Klientów Korporacyjnych wprowadzona została metoda uwierzytelniania i autoryzacji z użyciem karty mikroprocesorowej przez aplikację e-Podpis (SCSA). Aplikacja ePodpis (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.





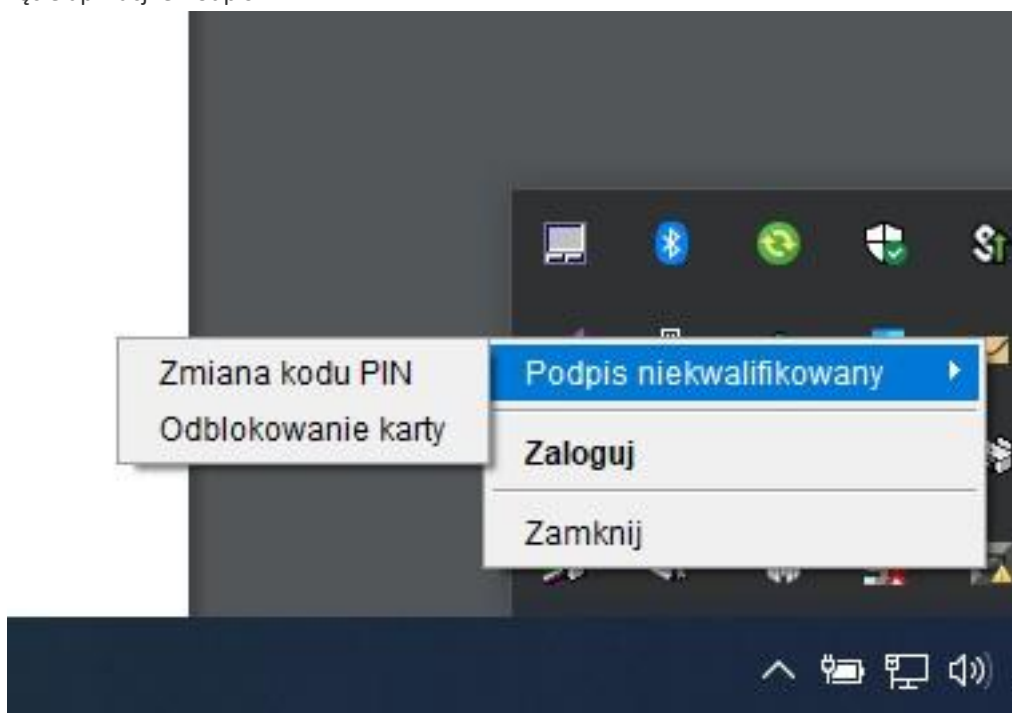
Rozdział 1. Obsługa e-Podpisu

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

1.1. 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:

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

 Odblokowanie karty — □ ×

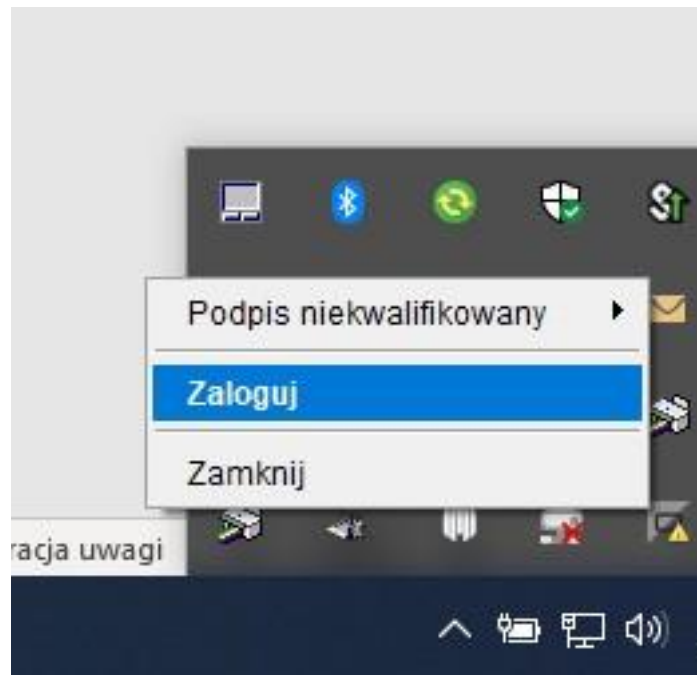
Kod PUK:

Nowy kod PIN:

Powtórz kod PIN:

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





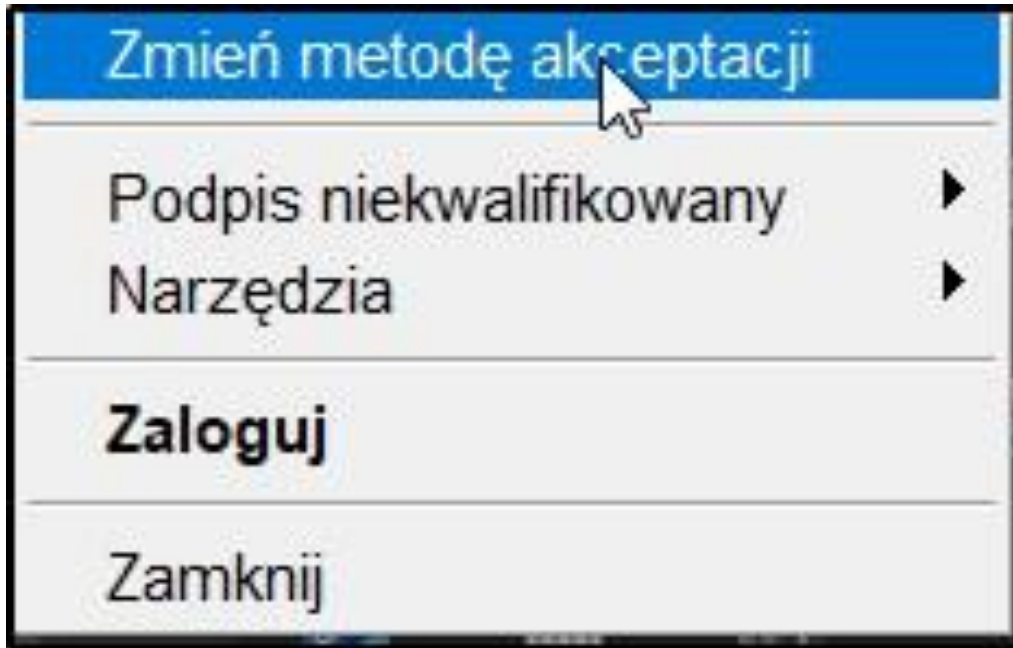
- **Zamknięcie aplikacji - (do podpisywania konieczne będzie ponowne uruchomienie aplikacji)**
- **Wyciągnięcie karty mikroprocesorowej z czytnika kart** powoduje wylogowanie z aplikacji e-Podpis, ale nie powoduje wylogowania z bankowości internetowej, ikona na pasku narzędzi jest w kolorze szarym.
- **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\).



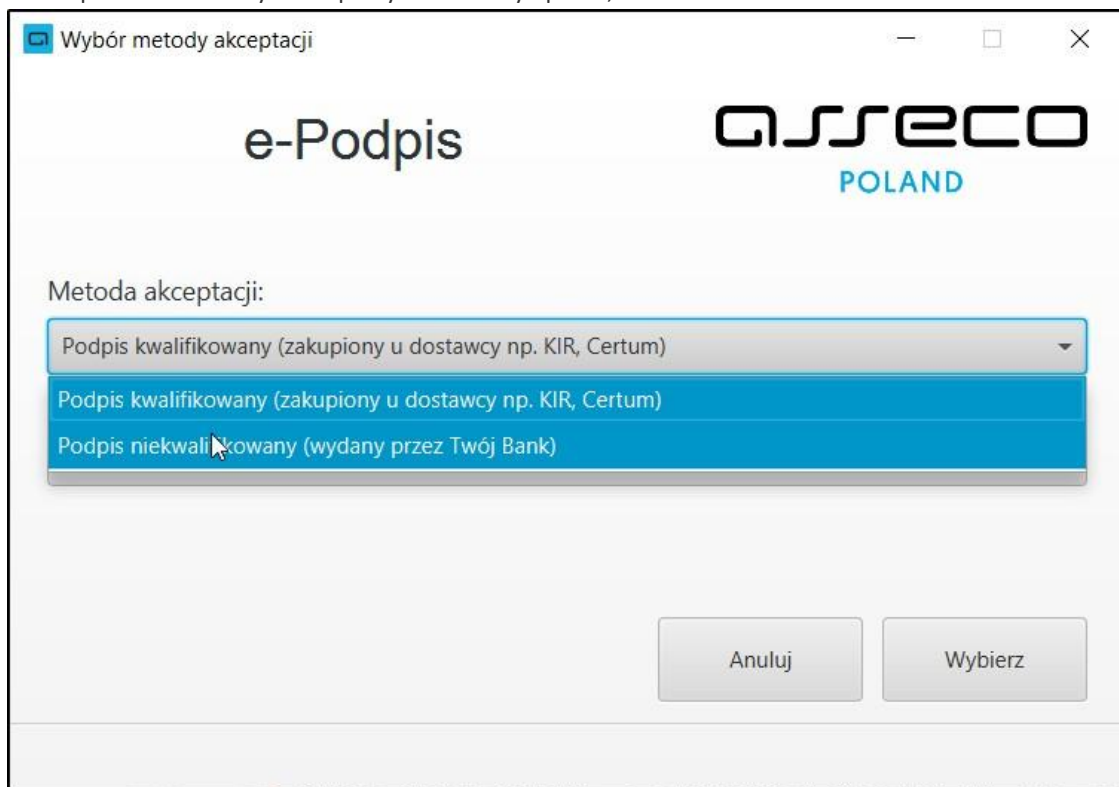
1.2. Podpis kwalifikowany

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.





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

- 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:

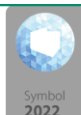
Logowanie do e-Podpis

[Zmień metodę akceptacji](#)

Certyfikat:

Podaj PIN:

Anuluj Podpisz



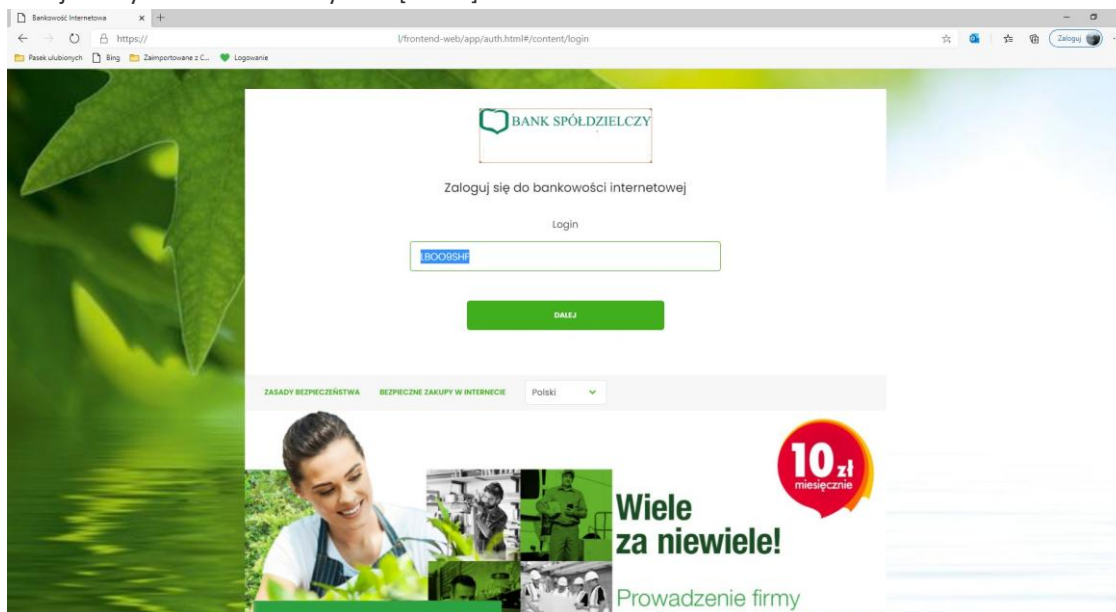


Rozdział 2. Logowanie do systemu bankowości internetowej def3000/EBP – uruchamianie aplikacji e-Podpis

W procesie uwierzytelniania i autoryzacji zleceń przy pomocy karty mikroprocesorowej, system bankowości internetowej pobiera i uruchamia aplikację e-Podpis SCSA. W procesie uruchomienia wykorzystane będące oprogramowanie: OpenWebStart lub Java.

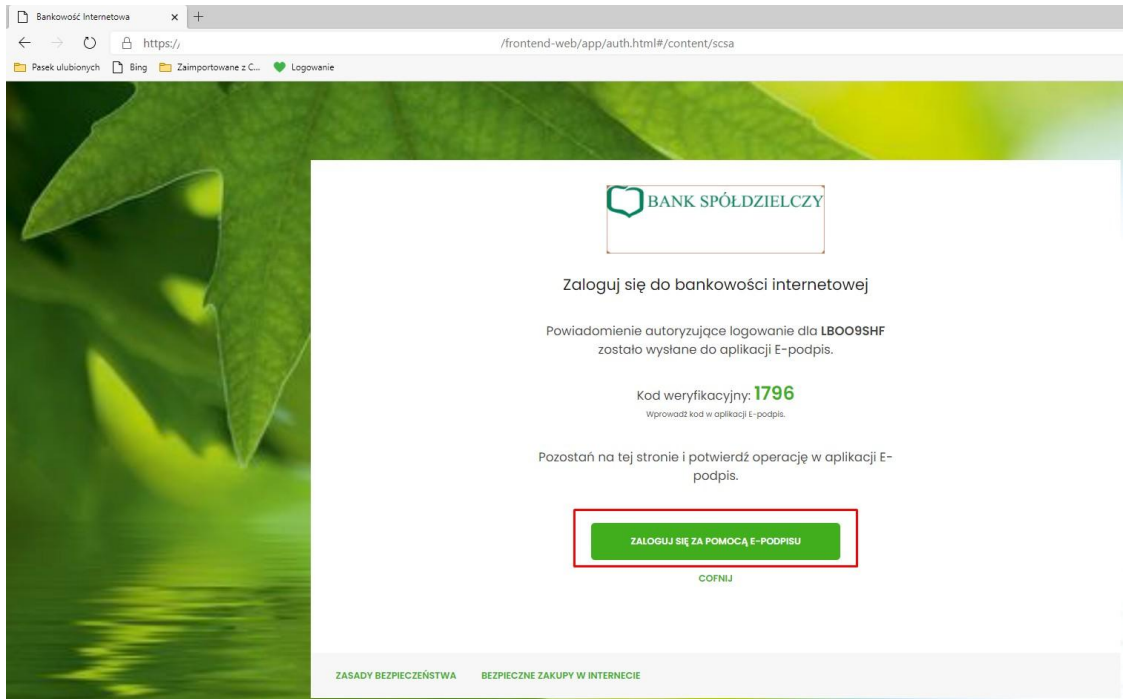
Proces pierwszego logowania przy użyciu karty mikroprocesorowej do aplikacji, będzie przebiegał następująco:

- Podaj identyfikator klienta i wybierz [DALEJ].

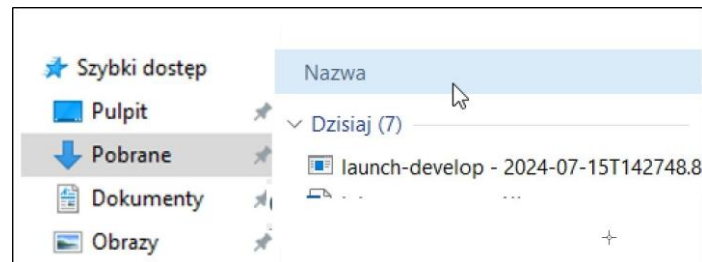


- Po wpisaniu identyfikatora zostaniemy przeniesieni do kolejnej strony, na której będziemy mieć możliwość pobrania i uruchamiania e-Podpisu (SCSA) poprzez wybranie opcji:” Zaloguj się za pomocą E-Podpisu”. Na formatce zostanie zaprezentowany: Identyfikator osoby logującej się i kod weryfikacyjny.





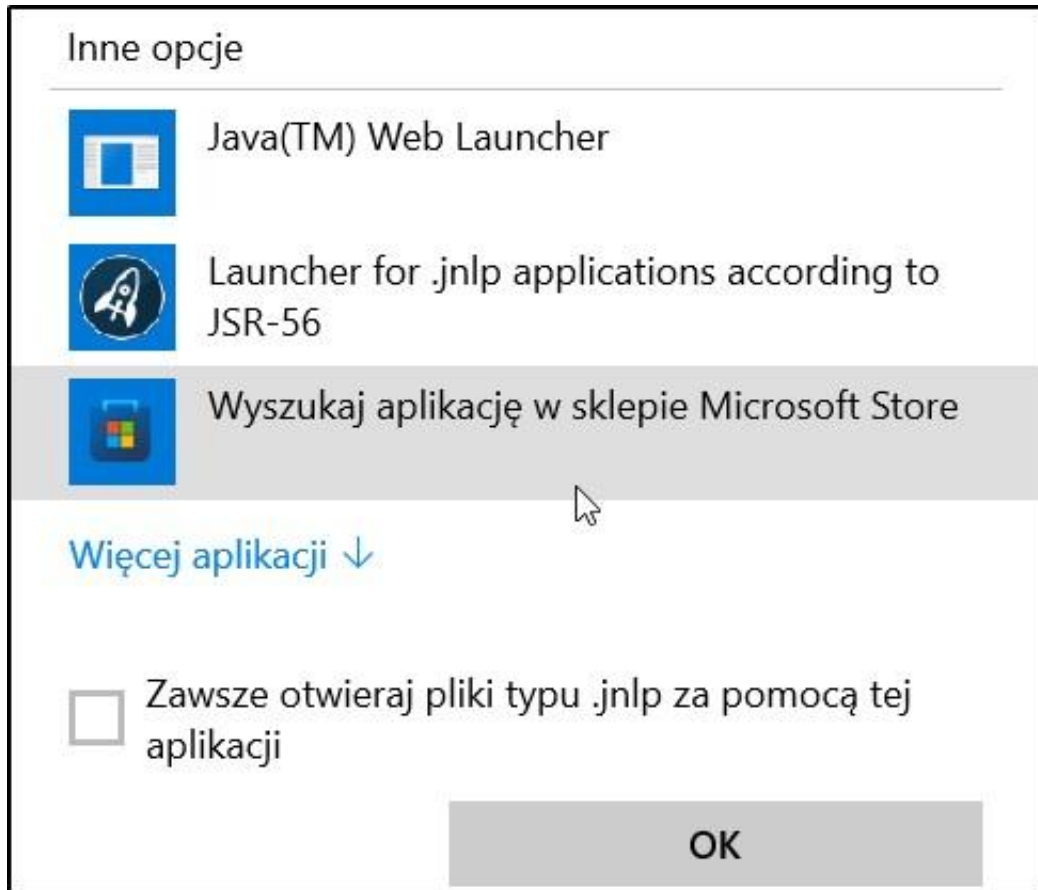
- Po wybraniu opcji [ZALOGUJ SIĘ ZA POMOCĄ E-PODPISU]” zostanie pobrany plik „launch-develop.jnlp”. W zależności od przeglądarki plik „launch.jnlp” może zostać bezpośrednio uruchomiony – przycisk „Otwórz” lub jest zapisywany (domyślnie w folderze „Pobrane”) i wtedy należy uruchomić pobrany plik z folderu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



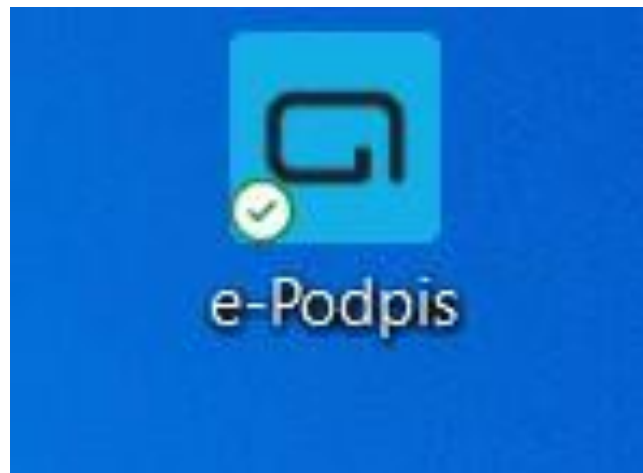
lub jeśli jest taka możliwość to uruchomić go z poziomu przeglądarki jako OpenWebStart.

Dla uruchomienia poprzez OpenWebStart będziemy mieć:

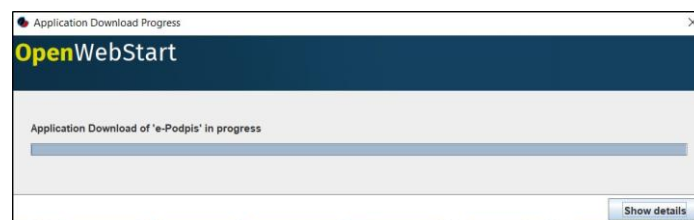




lub skrótu na pulpicie

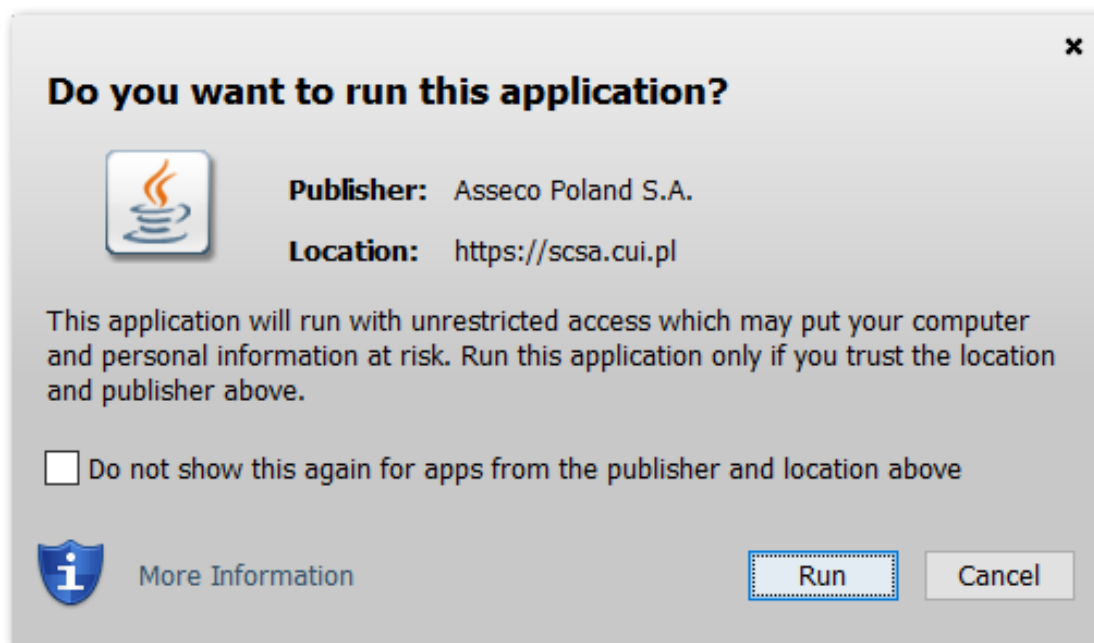
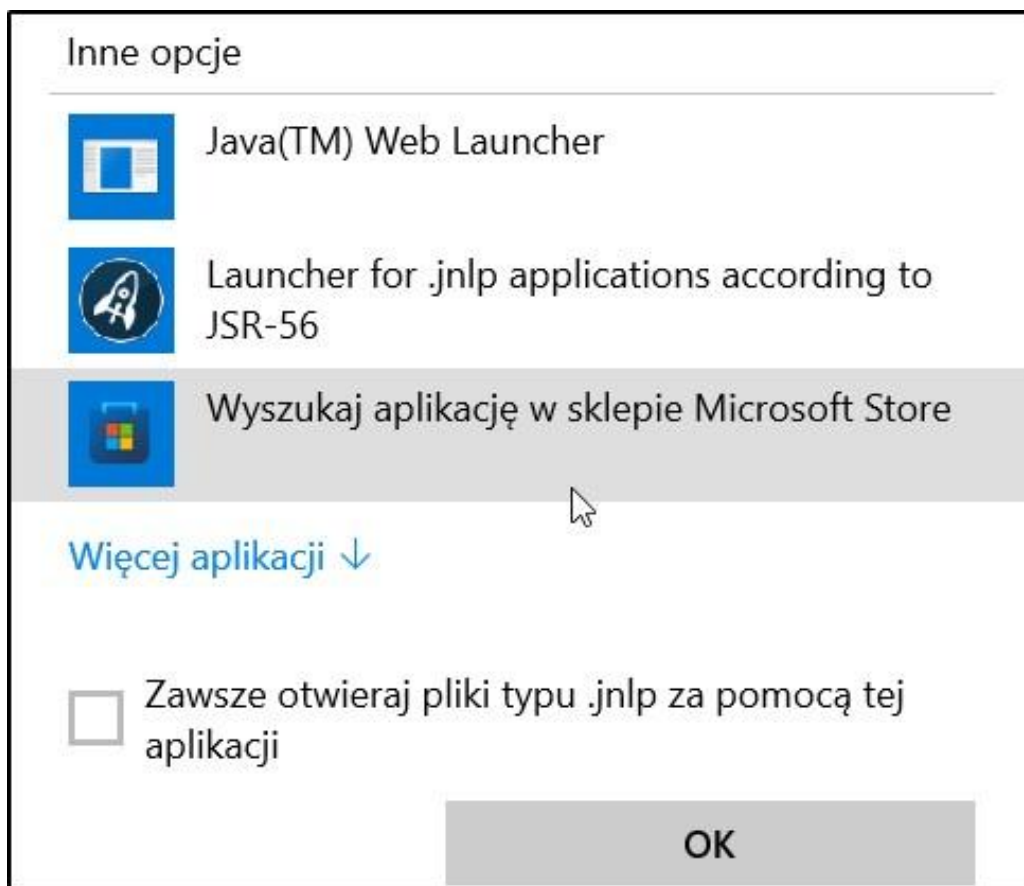


W kolejnym oknie wyświetlana jest informacja o pobieraniu przez e-Podpis danych z <https://scsa.cui.pl/webstart>.



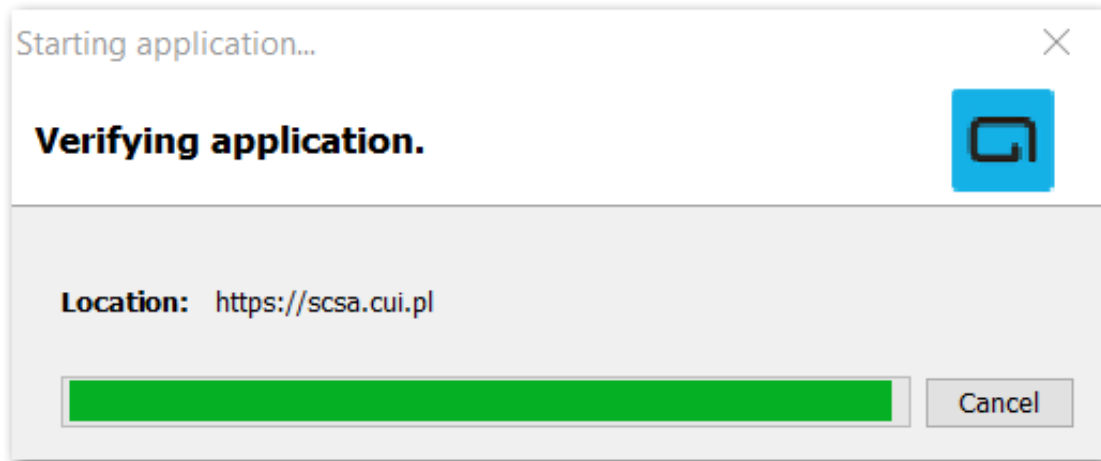
Dla uruchomienia z pomocą **Java** będziemy mieć:





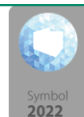
Po uruchomieniu aplikacji przy pomocy Java, system wyświetlił okno, w którym będzie zaprezentowane okno do weryfikacji danych.





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.

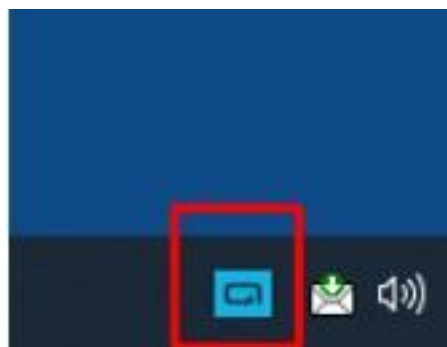




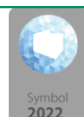
W oknie dialogowym „Dane do podpisu” pojawia się komunikat „Logowanie do e-Podpis”. Prawidłowe podanie kodu PIN powoduje zalogowanie do e-Podpisu i pojawienie się komunikatu „Poprawnie wysłano podpisane dane”.



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)

e-Podpis (podpis niekwalifikowany)

e-Podpis

ASSECO
POLAND

Dane do podpisu:

Logowanie BS

Kod weryfikacyjny:

Podaj PIN:

Anuluj Podpisz

Dla e-Podpis(podpis kwalifikowany)





e-Podpis (podpis kwalifikowany)

e-Podpis **ASSECO**
POLAND

Dane do podpisu:

Logowanie BS

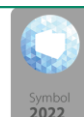
Kod weryfikacyjny:

Certyfikat:

Podaj PIN:

Anuluj Podpisz

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






Dla e-Podpis(podpis niekwalifikowany)

e-Podpis (podpis niekwalifikowany)

e-Podpis **ASSECO**
POLAND

Dane do podpisu:

Logowanie BS



Zamknij (2)

Poprawnie wysłano podpisane dane

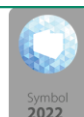




Dla e-Podpis (podpis kwalifikowany)

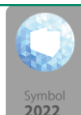


W przypadku gdy użytkownik wprowadzi błędny kod PIN i błędny kod weryfikacyjny, system zaprezentuje komunikat:





Dla e-Podpis(podpis niekwalifikowany)

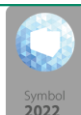




Dla e-Podpis(podpis kwalifikowany)

The screenshot shows a web application window titled "e-Podpis (podpis kwalifikowany)". The header includes the text "e-Podpis" and the logo for "assecO POLAND". Below the header, there is a section "Dane do podpisu:" containing a text input field with the placeholder "Logowanie do e-Podpis". A link "Zmień metodę akceptacji" is located below the input field. To the right, there is a "Certyfikat:" section with a dropdown menu showing "CN=" and a red box around the selection. Below that is a "Podaj PIN:" section with an empty input field. At the bottom of this section are two buttons: "Anuluj" and "Podpisz". On the left side of the form, there is a large red circular icon with a white 'X' inside. At the very bottom of the window, a grey bar contains the error message: "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:
3576

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:

Logowanie BS

Kod weryfikacyjny:
9480

Certyfikat:
CN= [REDACTED]

Podaj PIN:
[REDACTED]

Anuluj Podpisz

Wystąpił błąd podczas podpisywania danych

