

Aplikacja SCSA - Instrukcja logowania i autoryzacji w systemie bankowości internetowej

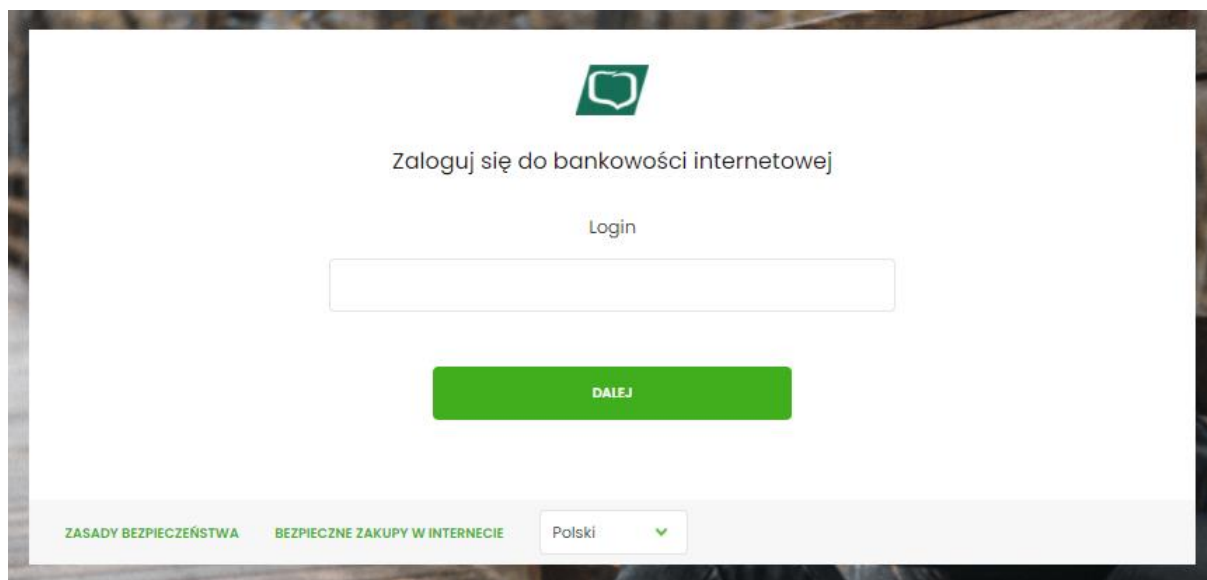
1. Logowanie do systemu bankowości internetowej przy pomocy karty mikroprocesorowej

W celu skorzystania z karty mikroprocesorowej do uwierzytelniania i autoryzacji zleceń system bankowości internetowej pobiera i uruchamia aplikację SCSA (e-Podpis). Do działania aplikacja SCSA wymaga zainstalowanego na komputerze środowiska Java. Może to być zarówno Java pobrana ze strony java.com jak i w wersji otwartej - pobrana np. ze strony: <https://www.bsjaroslaw.pl/bankowosc-korporacyjna>. Aby wykonać zlecenie wymagające akceptacji kartą mikroprocesorową, należy w pierwszej kolejności zalogować się do aplikacji SCSA, wpisując kod PIN. Kod PIN jest to kod wydany razem z kartą mikroprocesorową. Podczas logowania do aplikacji SCSA, bankowości internetowej i podpisywania zleceń cały czas wymagany jest tylko jeden – ten sam kod PIN oraz karta mikroprocesorowa.

A. Pierwsze logowanie do bankowości internetowej za pomocą karty mikroprocesorowej

Proces pierwszego logowania za pomocą karty mikroprocesorowej przebiega w następujący sposób:

- Użytkownik wpisuje następujący adres w przeglądarce: <https://e-bsjaroslaw.cui.pl> lub wybiera z menu „Zaloguj” na stronie www.bsjaroslaw.pl odpowiedni przycisk.
- Użytkownik wprowadza identyfikator oraz naciska przycisk [DALEJ]:



- Pojawia się formatka do potwierdzenia logowania za pomocą aplikacji SCSA, na której widoczny jest m.in. identyfikator użytkownika i kod weryfikacyjny. Kolejny etap logowania wymaga naciśnięcia przycisku [ZALOGUJ SIĘ ZA POMOCĄ E-PODPISU].



Zaloguj się do bankowości internetowej

Powiadomienie autoryzujące logowanie dla **XXXXXXXX** zostało wysłane do aplikacji SCSA.

Kod weryfikacyjny: **YYYY**

Zweryfikuj zgodność powyższego kodu z kodem widocznym w aplikacji SCSA.

Pozostań na tej stronie i potwierdź operację w aplikacji SCSA.

ZALOGUJ SIĘ ZA POMOCĄ E-PODPISU

COFNIJ

- System pobiera aplikację SCSA służącą do obsługi podpisu za pomocą karty mikroprocesorowej.
- Po uruchomieniu aplikacja SCSA prezentuje użytkownikowi ekran logowania do e-Podpis, czyli do samej aplikacji.

e-Podpis (podpis niekwalifikowany)

e-Podpis

Dane do podpisu:

Logowanie do e-Podpis

Podaj PIN:

....

Anuluj Podpisz

- Użytkownik wpisuje PIN, następnie naciska przycisk [PODPISZ], aplikacja sprawdza poprawność wprowadzonych danych.
- Po poprawnej weryfikacji wprowadzonego PIN-u aplikacja SCSA ponownie prosi o podanie kodu PIN, ale tym razem w celu potwierdzenia logowania do bankowości internetowej.



Zaloguj się do bankowości internetowej

Powiadomienie autoryzujące logowanie dla **XXXXXXXX** zostało wysłane do aplikacji SCSA.

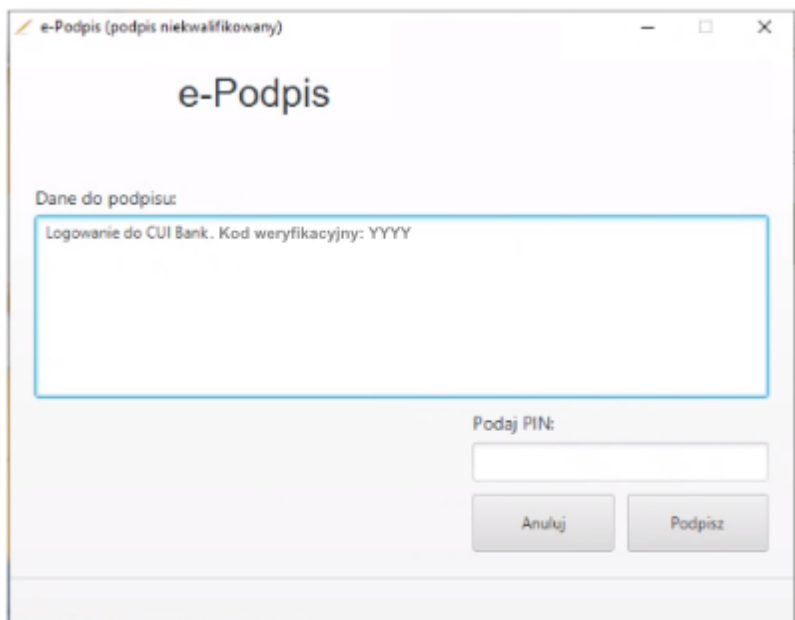
Kod weryfikacyjny: **YYYY**

Zweryfikuj zgodność powyższego kodu z kodem widocznym w aplikacji SCSA.

Pozostań na tej stronie i potwierdź operację w aplikacji SCSA.

ZALOGUJ SIĘ ZA POMOCĄ E-PODPISU

COFNIJ

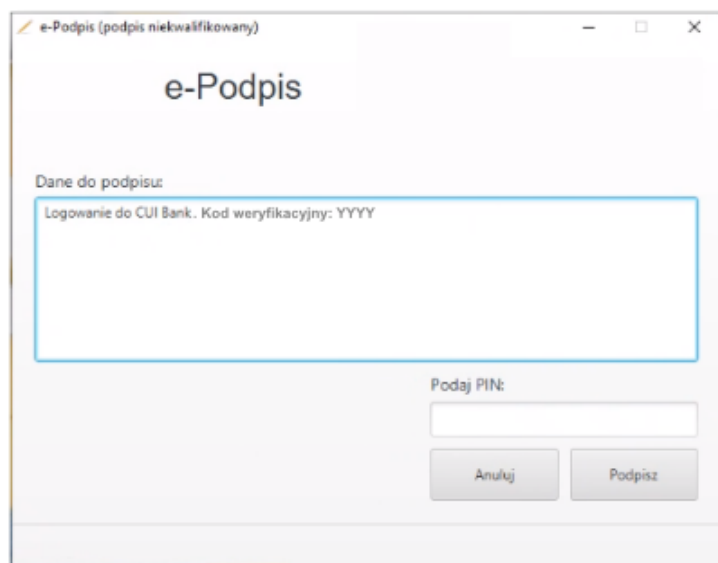


- Należy sprawdzić, czy kod weryfikacyjny podany na stronie logowania jest identyczny z kodem wyświetlanym w aplikacji SCSA.
 - Po poprawnym wprowadzeniu kodu PIN system loguje użytkownika do bankowości internetowej.
- B. Kolejne logowanie do bankowości internetowej przy pomocy karty mikroprocesorowej Przed zalogowaniem do aplikacji SCSA jej ikona znajdująca się w zasobniku jest szara (na zrzucie ekranu oznaczona czerwonym okręgiem):

Po zalogowaniu ikona staje się niebieska:



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



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

2. Autoryzacja zleceń za pomocą karty mikroprocesorowej

Po wprowadzeniu danych dyspozycji przelewu i naciśnięciu [DALEJ] system prezentuje formularz potwierdzenia wprowadzonych danych wraz z oknem do prowadzenia kodu PIN.

The image shows two overlapping windows from a banking application. The background window is titled 'Przelew' (Transfer) and displays the following details:

- Nadawca: JAN TESTOWY, TESTOWA II-III MIASTO
- Odbiorca: Odbiorca Testowy
- Rachunek odbiorcy: 84 2190 0002 4086 8249 8284 2288, ONB Centrala
- Kwota: 1,00 PLN
- Tytułem: tytuł testowy
- Data realizacji: Dzisiaj, 27.02.2020
- Rodzaj przelewu: Elixir i wewnętrzny

Below the details, there is a green link 'POKAŻ DODATKOWE INFORMACJE' and a confirmation instruction: 'Pozostań na tej stronie i potwierdź operację w aplikacji e-Podpis.' A loading spinner is visible at the bottom with the text 'Oczekiwanie na podpis aplikacją e-Podpis. URUCHOM APLIKACJĘ E-PODPIS'.

The foreground window is titled 'e-Podpis (podpis niekwalifikowany)' and contains the following information:

- Dane do podpisu: Dodanie przelewu
- Kwota: 1,00 PLN
- Odbiorca: Odbiorca Testowy
- Z rachunku: 92 8707 0006 0001 4036 3000 0001
- Na rachunek: 84 2190 0002 4086 8249 8284 2288
- Tytułem: tytuł
- Typ przelewu: Przelew krajowy

At the bottom of this window, there is a field for 'Podaj PIN:' with a masked input (****) and two buttons: 'Anuluj' and 'Podpisz'.

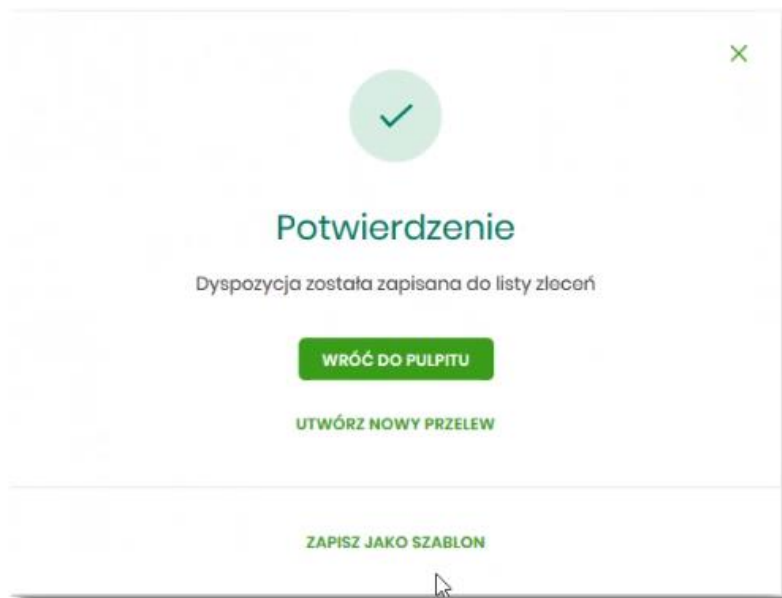
Na formularzu E-PODPIS dostępne są akcje:

- [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.

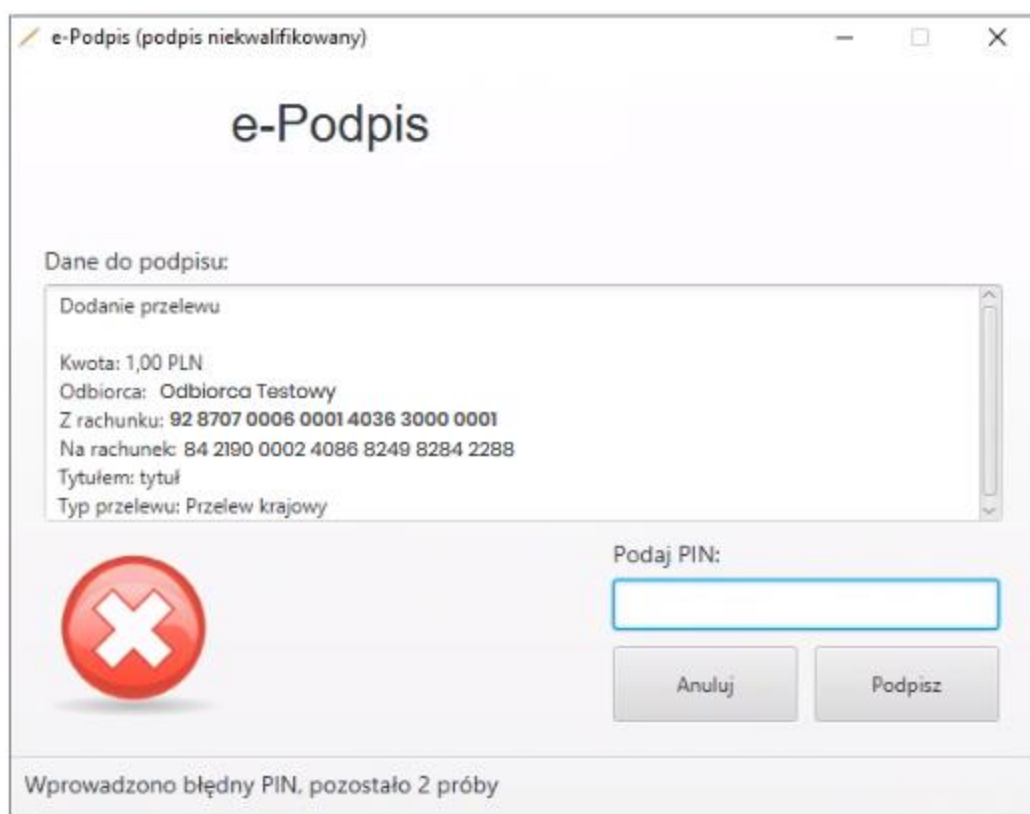
The image shows the 'e-Podpis (podpis niekwalifikowany)' window after a successful transaction. It displays the same transfer details as the previous window, but with a large green checkmark icon on the left and a 'Zamknij' (Close) button on the right. At the bottom, a status message reads: 'Poprawnie wysłano podpisane dane'.

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



Na formularzu POTWIERDZENIE dostępne są akcje:

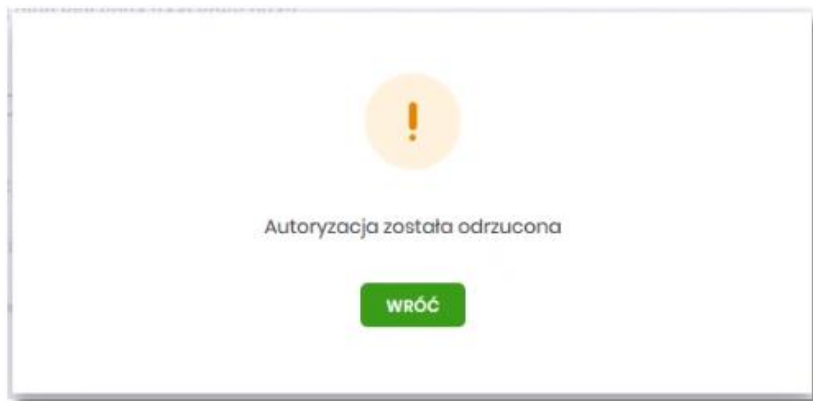
- [WRÓĆ DO PULPITU] – umożliwia powrót do pulpitu.
- [UTWÓRZ NOWY PRZELEW] – umożliwia utworzenie nowej dyspozycji.
- [ZAPISZ JAKO SZABLON] – umożliwia zapisanie dyspozycji jako szablon. W przypadku gdy użytkownik wprowadzi błędny kod PIN, system zaprezentuje komunikat:



Na formularzu E-PODPIS dostępne są akcje:

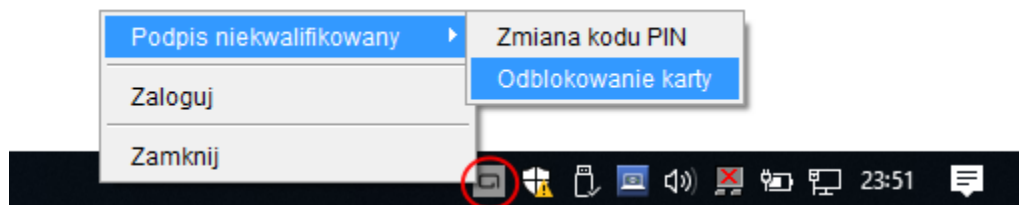
- [ANULUJ] – umożliwia rezygnację z podpisania dyspozycji,
- [PODPISZ] – umożliwia wprowadzenie poprawnego kodu i podpisanie dyspozycji.

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



3. Odblokowanie kodu PIN W celu odblokowania kodu PIN należy:

1. Umieścić kartę mikroprocesorową w czytniku.
2. Uruchomić aplikację SCSA wpisując identyfikator w bankowości internetowej.
3. Kliknąć prawym przyciskiem myszy na ikonę aplikacji w zasobniku systemowym i wybrać z menu: Podpis niekwalifikowany → Odblokowanie karty:



4. W oknie Odblokowanie karty wpisać kod PUK oraz dwukrotnie nowy kod PIN, a następnie zatwierdzić przyciskiem [ODBLOKUJ]:

Odblokowanie karty

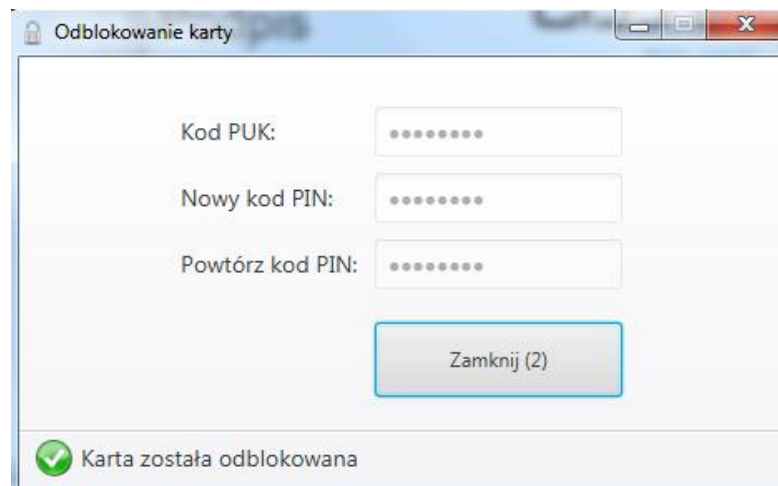
Kod PUK:

Nowy kod PIN:

Powtórz kod PIN:

Odblokuj

5. Karta zostanie odblokowana:



4. Korzystanie z przeglądarek internetowych

Z uwagi na kompatybilność systemu bankowości internetowej z przeglądarkami mobilnymi zapewniona jest zgodność interfejsu użytkownika systemu z niżej wymienionymi wersjami bazowymi przeglądarek oraz wyższymi:

Platformy stacjonarne (desktop/laptop) :

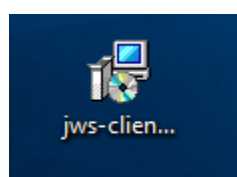
- Chrome 50.x lub przeglądarki oparte na Chrome (np. Opera).
- Firefox 46.0
- Safari

Do korzystania z karty mikroprocesorowej konieczne jest zainstalowanie programu Java Web Start, który służy do uruchomienia aplikacji SCSA obsługującej uwierzytelnianie i autoryzację zleceń. 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.

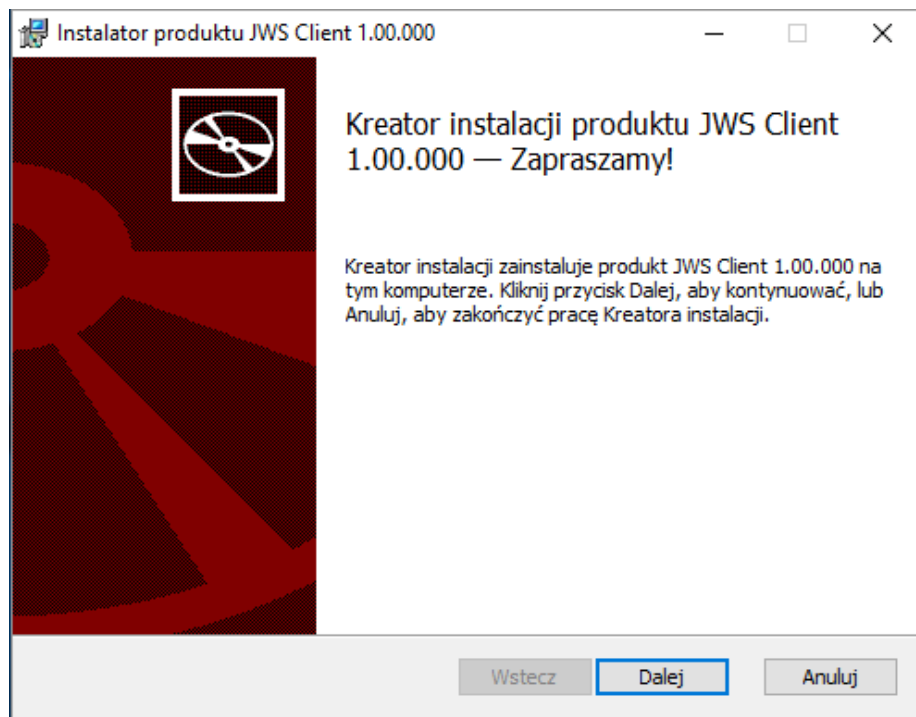
5. Instalacja oprogramowanie Java (Open JDK) oraz komponentu IcedTea

Ze względu na fakt, że licencja środowiska JAVA firmy Oracle stała się płatna, zalecamy instalację oprogramowanie JAVA Web Start Client, zawierające darmowe otwarte środowisko Java (Open JDK) oraz komponent IcedTea do obsługi technologii JAVA Web Start. Wymagania techniczne System operacyjny: Windows 7 lub nowszy. W celu zainstalowania aplikacji JAVA Web Start Client należy:

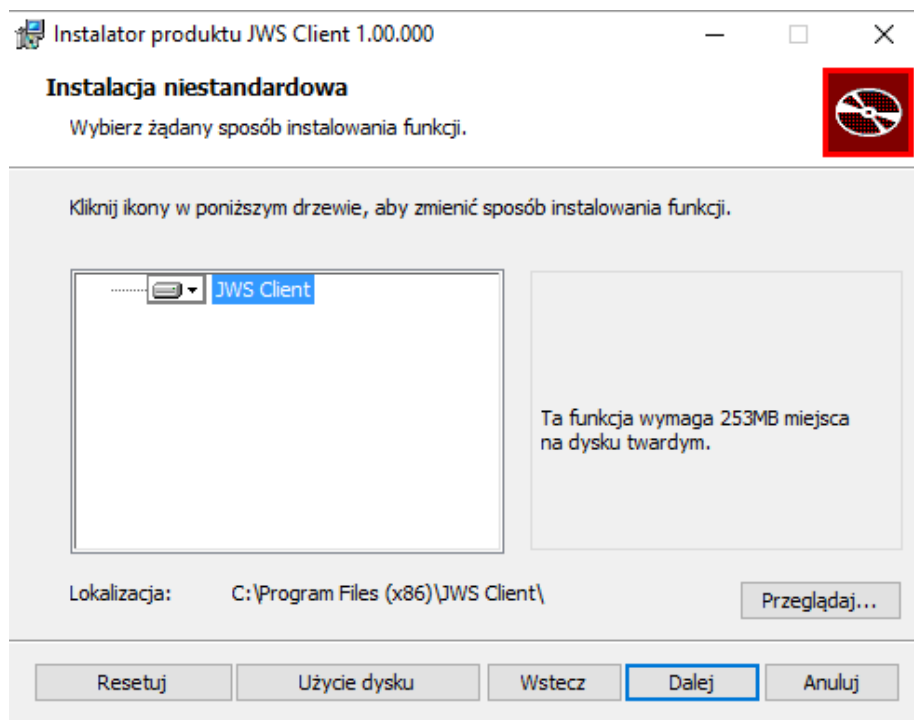
1. Pobrać z lokalizacji: <https://www.bsjaroslaw.pl/public-files/jws-client-windows-1.00.000-x86-pl.msi> plik instalatora oprogramowania JAVA Web Start Client, zawierające otwarte środowisko Java (Open JDK) oraz komponent IcedTea do obsługi technologii JAVA Web Start.
2. Uruchomić instalator:



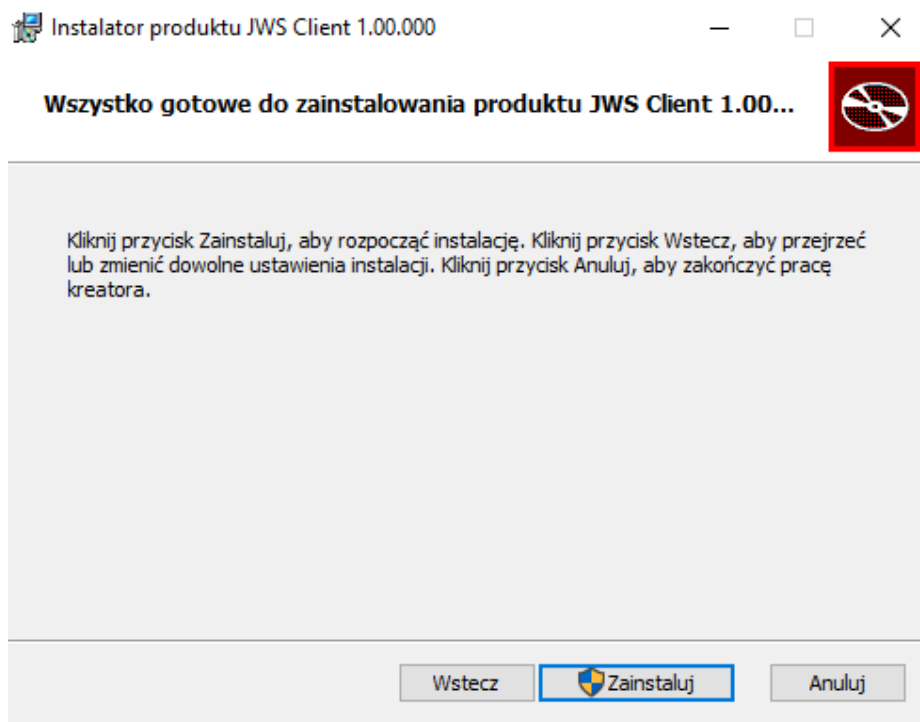
3. Nacisnąć [DALEJ]:



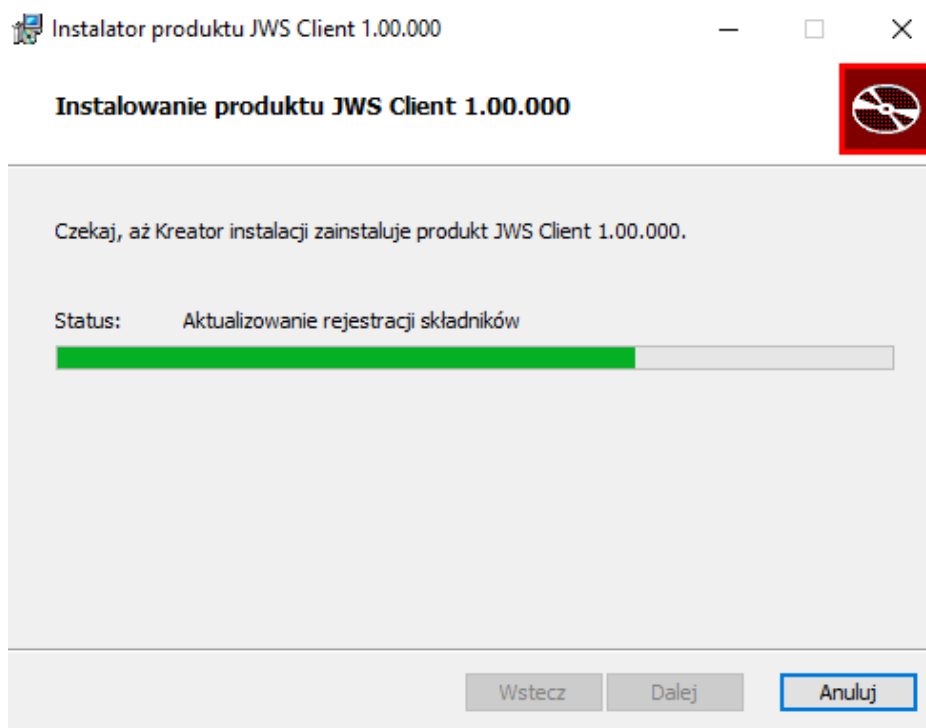
4. Nacisnąć [DALEJ]:



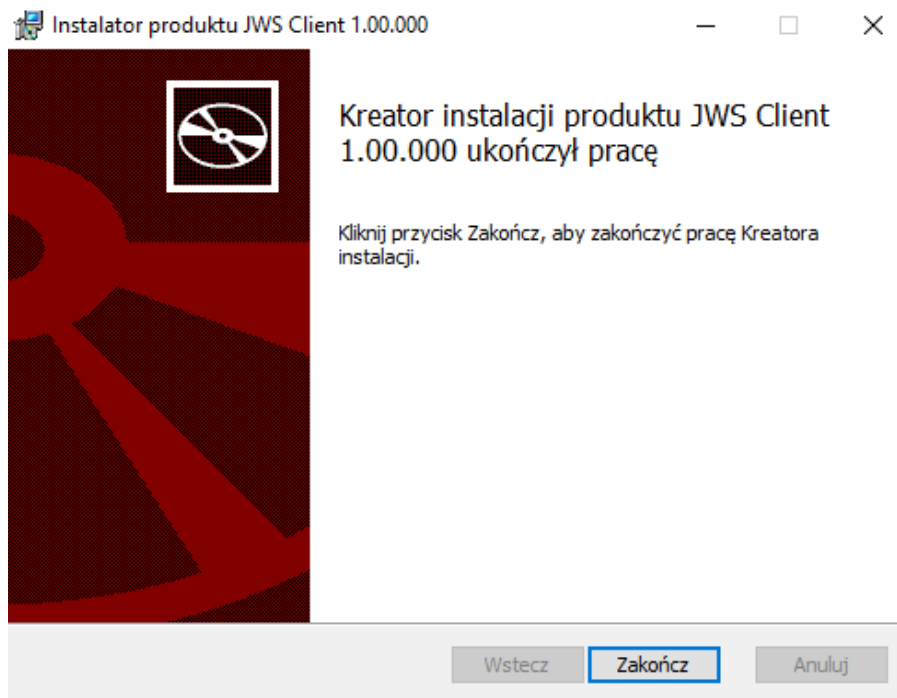
5. Uruchomić instalację przyciskiem [ZAINSTALUJ]:



6. Zezwolić na instalację oprogramowania w okienkach wyświetlanych przez system operacyjny lub oprogramowanie zabezpieczające (programy antywirusowe, zapory sieciowe itp.).
7. Poczekać na zakończenie instalacji:



8. Potwierdzić zakończenie instalacji przyciskiem [ZAKOŃCZ].



9. Zrestartować komputer:

