

# **Dostosowanie środków dostępu użytkowanych w systemach bankowości elektronicznej Asseco CBP oraz def3000/CEB do wymagań SCA (silne uwierzytelnianie).**

# KLIENTY INDYWIDUALNI

## SMS

Wygląd formatek dla użytkownika po wprowadzeniu SCA

### i) autentykacja:

Wprowadzenie identyfikatora użytkownika:

The screenshot shows a mobile application interface for logging in. At the top, there is a blue header with the word "LOGOWANIE" on the left and a language selector "PL" on the right. Below the header, the main content area has a white background. In the center, there is a label "Numer Identyfikacyjny" followed by a text input field containing the placeholder text "Wpisz numer". Below the input field is a blue button labeled "DALEJ". Underneath the button, there is a small lock icon and the text "Pamiętaj o podstawowych zasadach bezpieczeństwa." followed by a list of instructions: "Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:" followed by three bullet points: "adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)", "w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka".

Wprowadzenie tymczasowego hasła, który klient otrzymał w wiadomości SMS:

The screenshot shows the same mobile application interface as the previous one, but now for entering a temporary password. The header and the "Numer Identyfikacyjny" section are identical. Below the "DALEJ" button, there is a label "Kod dostępu" followed by a row of 24 input fields. The first 7 fields are empty, and the remaining 17 fields contain a dot "•". Below the input fields is a blue button labeled "DALEJ". Underneath the button, there is a small lock icon and the text "Pamiętaj o podstawowych zasadach bezpieczeństwa." followed by a list of instructions: "Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:" followed by three bullet points: "adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)", "w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka", "po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc". Below this, it says "Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem." and "Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)".

Zatwierdzanie tymczasowego hasła kodem SMS:

← LOGOWANIE

Kod dostępu

Kod SMS

**ZALOGUJ**

Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Ustalenie nowego hasła:

← Nowe hasło dostępu

Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator użytkownika

Nowe hasło dostępu

Powtórz nowe hasło

**ZAPISZ I ZALOGUJ**

Definiując swoje nowe hasło dostępu pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

- o musi składać się z 4-8 znaków
- o musi zawierać przynajmniej jeden znak specjalny
- o musi zawierać przynajmniej jedną wielką literę
- o musi zawierać przynajmniej jedną małą literę
- o musi zawierać przynajmniej jedną cyfrę
- o dozwolone znaki: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ@#\$%&\*()\_-=+{}|~!:"<>/?

Ponowne logowanie do aplikacji z użyciem nowego hasła:

← LOGOWANIE

Kod dostępu

**DALEJ**

Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Wprowadzenie kodu SMS:

LOGOWANIE

Kod dostępu

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

Kod SMS

ZALOGUJ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

**ii) autoryzacja:**

Pierwsza autoryzacja będzie poprzedzona wysłaniem poprzez SMS jednorazowego numeru PIN wraz z wymuszeniem jego zmiany:

←
×
Przelew

ZWYKŁY

Przelew z rachunku	Rachunki Bieżące 84 8707 0006 0000 5656 2000 0001
Odbiorca	Jan Testowy
Rachunek odbiorcy	02 1500 1894 0690 2900 3640 4254 KBSA O. w Chorzowie
<b>Kwota</b>	<b>1,43 PLN</b>
Tytułem	tytuł testowy
Data realizacji	dzisiaj 26.08.2019

[↓ Pokaż dodatkowe informacje](#)

Wymagana zmiana pinu autoryzacyjnego

Prosimy pamiętać, że pin autoryzacyjny jest numerem poufnym. W związku z tym nie powinien być ujawniany osobom trzecim. Definiując swój pin autoryzacyjny pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

**Pin Autoryzacyjny:**  
 musi składać się z 4-znaków  
 musi się różnić od 3 ostatnich pinów

Obecny pin autoryzacyjny	<input style="width: 100%;" type="text" value="Wpisz obecny pin"/>
Nowy pin autoryzacyjny	<input style="width: 100%;" type="text" value="Wpisz nowy pin"/>
Powtórz nowy pin	<input style="width: 100%;" type="text" value="Powtórz nowy pin"/>

ZATWIERDŹ

Kolejne autoryzacje będą wymagały wprowadzenia zdefiniowanego wcześniej PIN-u do podpisu oraz kodu SMS:

← Przelew ×

ZWYKLY

Przelew z rachunku Rachunki Bieżące  
84 8707 0006 0000 5656 2000 0001

Odbiorca ODBIORCA SKROCONY PEŁNY

Rachunek odbiorcy 94 1020 1505 0000 0802 0011 2714  
PKOBP

Kwota 1,00 PLN

Tytułem TYTUŁ PŁATNOŚCI

Data realizacji dzisiaj  
26.08.2019

↓ Pokaż dodatkowe informacje

Pin autoryzacyjny oraz kod SMS Wpisz pin

Wpisz kod

Operacja nr 738167 z dnia 26.08.2019

AKCEPTUJ

## MAA

Wygląd formatek dla użytkownika

### i) autentykacja:

Wprowadzenie identyfikatora użytkownika:

LOGOWANIE PL

Numer Identyfikacyjny Wpisz numer

DALEJ

🔒 Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka

Wprowadzenie hasła maskowanego:

**UWAGA! W przypadku pierwszego logowania, dla klienta, system w pierwszym kroku poprosi o podanie hasła startowego. Wówczas system najpierw poprosi o ustalenie nowego hasła a po ustaleniu nowego hasła, aplikacja wymusi ponowne logowanie już z nowym hasłem.**

←
LOGOWANIE

Kod dostępu

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

DALEJ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

W przypadku braku sparowanego urządzenia, aplikacja wyświetli komunikat o sparowaniu urządzenia.

←
Urządzenie autoryzujące

**Do autoryzacji urządzenia wymagana jest aplikacja mToken Asseco MAA**

Jeśli nie posiadasz aplikacji, znajdziesz ją w Google Play lub App Store

POSIADAM APLIKACJĘ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

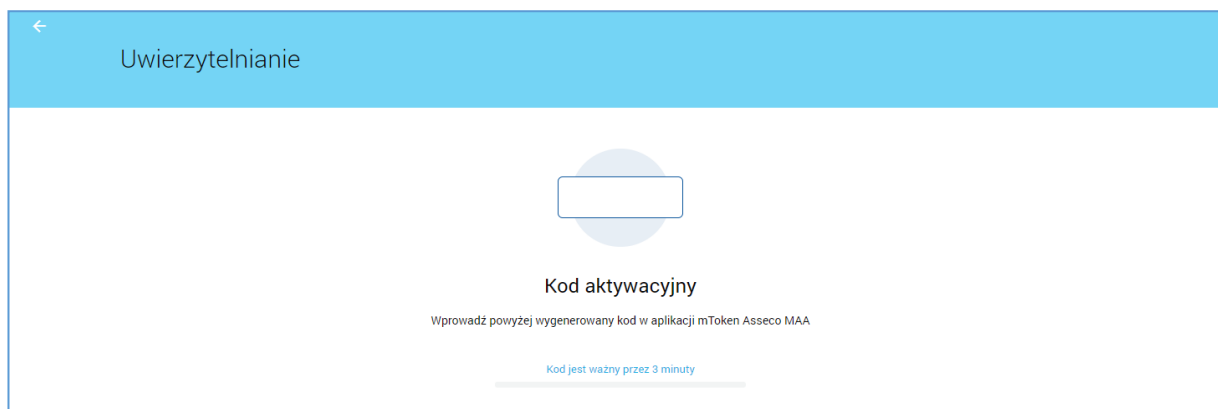
Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

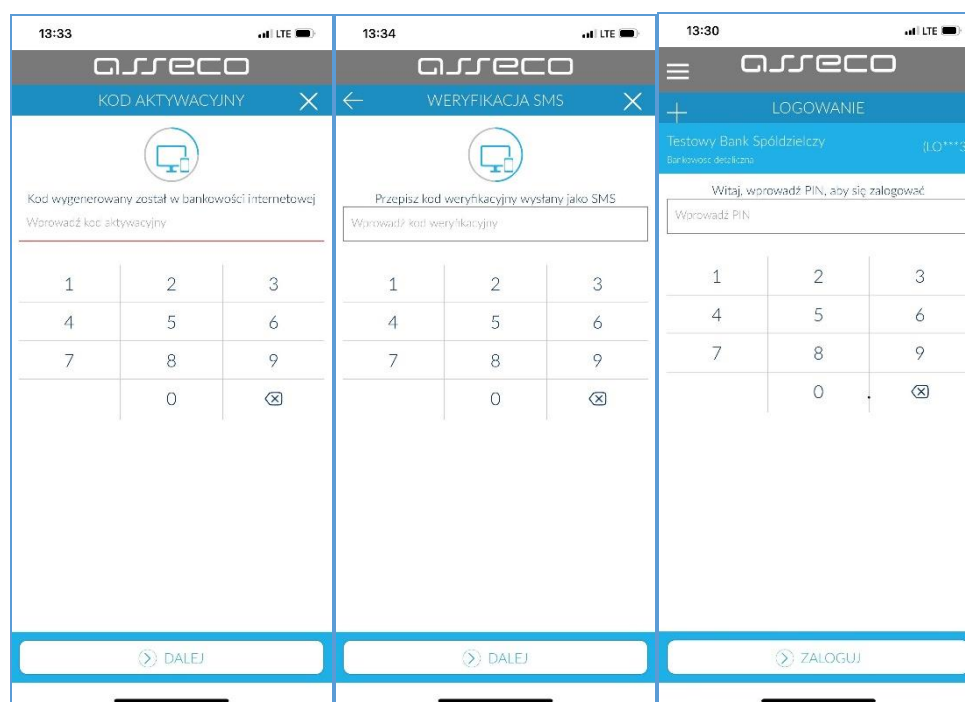
Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

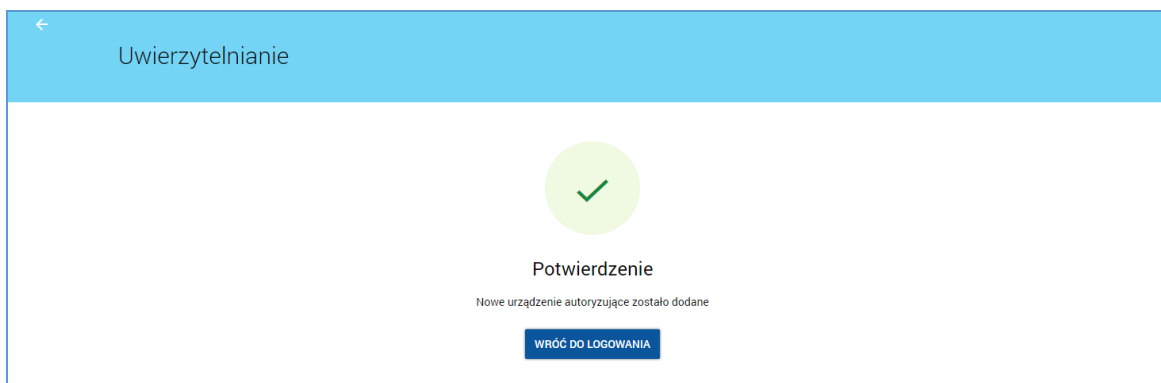
Po tym komunikacie, klient powinien pobrać aplikację na urządzenie mobilne. Po pobraniu aplikacji na urządzenie mobilne, w aplikacji internetowej Asseco CBP należy wybrać opcję „Posiadam aplikację”, gdzie wyświetla się kod aktywacyjny.



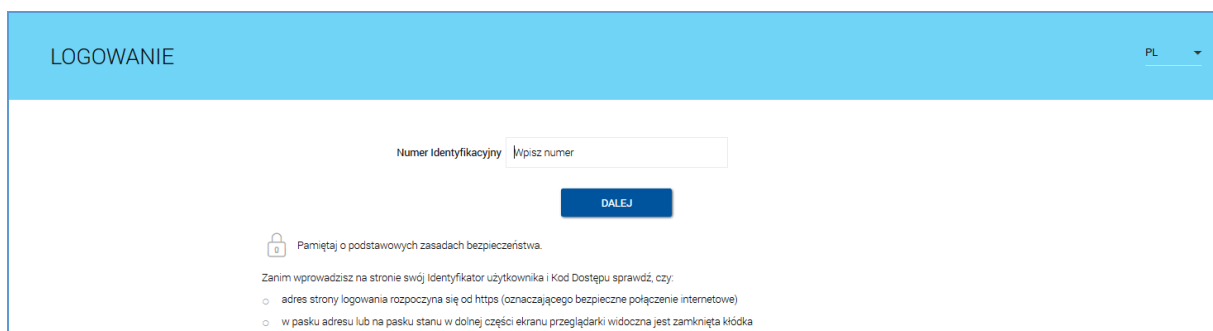
Na urządzeniu mobilnym klient, dodaje nowe urządzenie poprzez znak „+” i wprowadza kod, który wyświetli się w aplikacji internetowej (Kod w aplikacji Asseco CBP pokaże się po wejściu w opcję „Posiadam aplikację” (patrz zrzut powyżej)). W kolejnym kroku należy podać kod SMS, który zostanie przesłany na wskazany w Bank Admin numer telefonu i ustawić pin do aplikacji



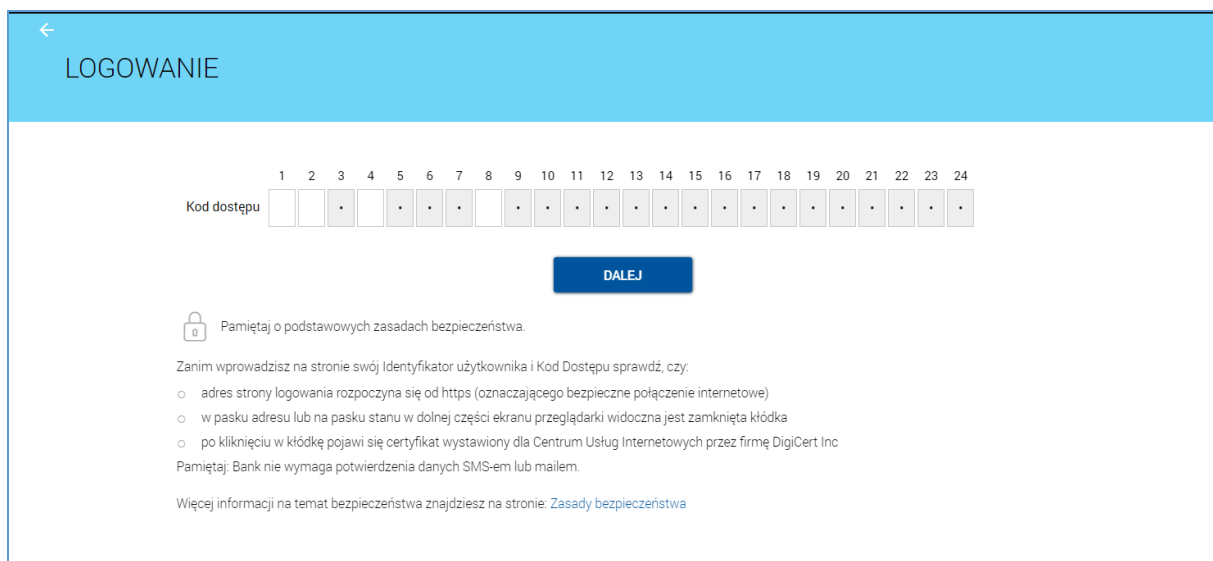
Po wykonaniu w/w czynności, w aplikacji pojawi się komunikat o poprawnym sparowaniu. I system poprosi o ponowne zalogowanie do bankowości.



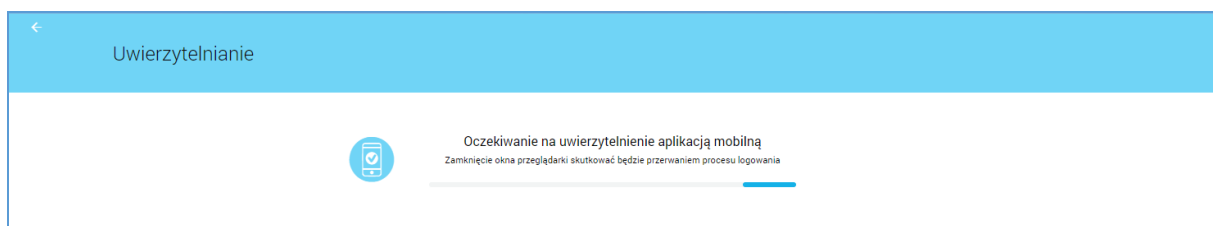
Wówczas ponownie należy wykonać akcję logowania: wprowadzenie identyfikatora użytkownika:



Wprowadzenie hasła maskowanego:

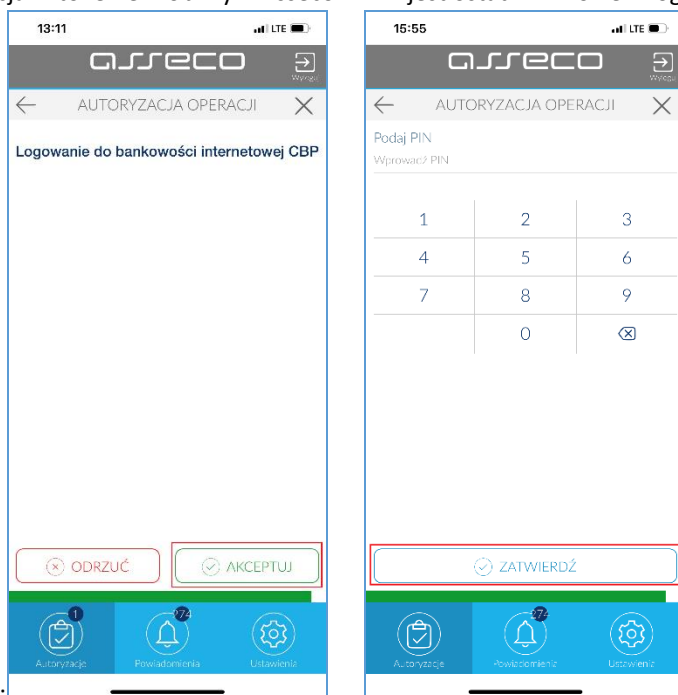


Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:





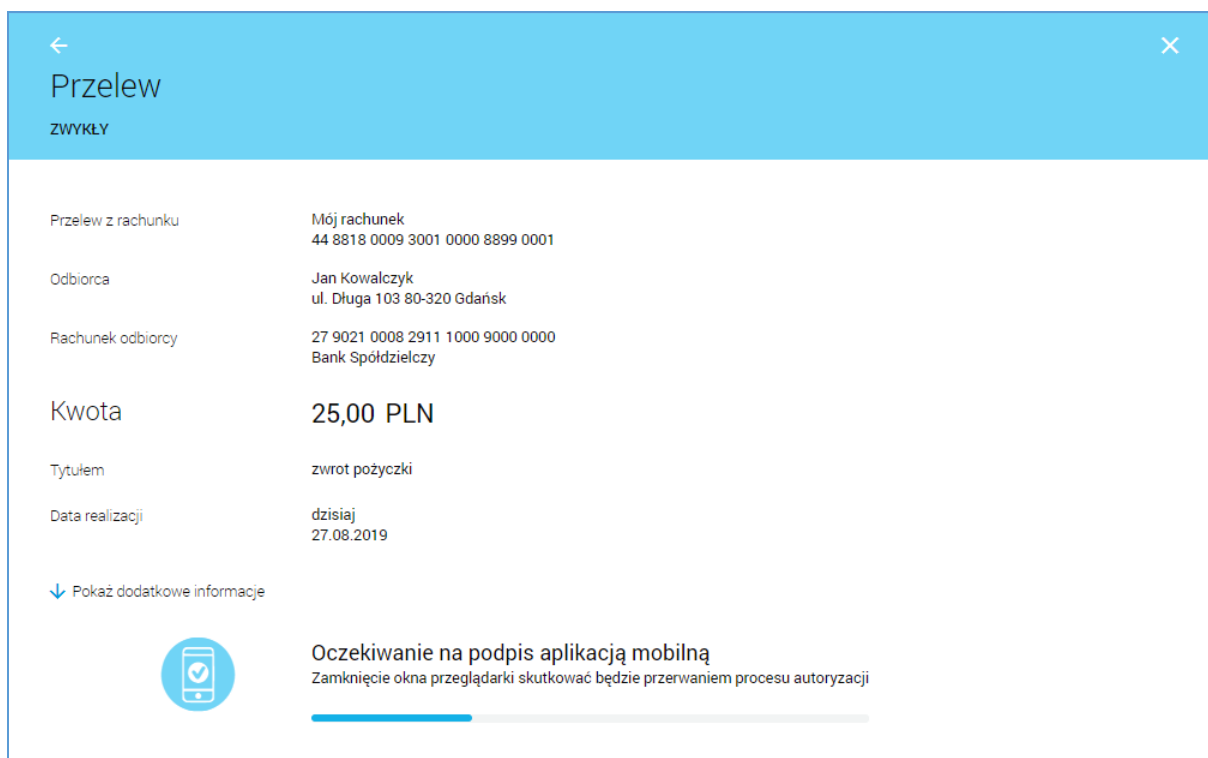
Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem logowania do



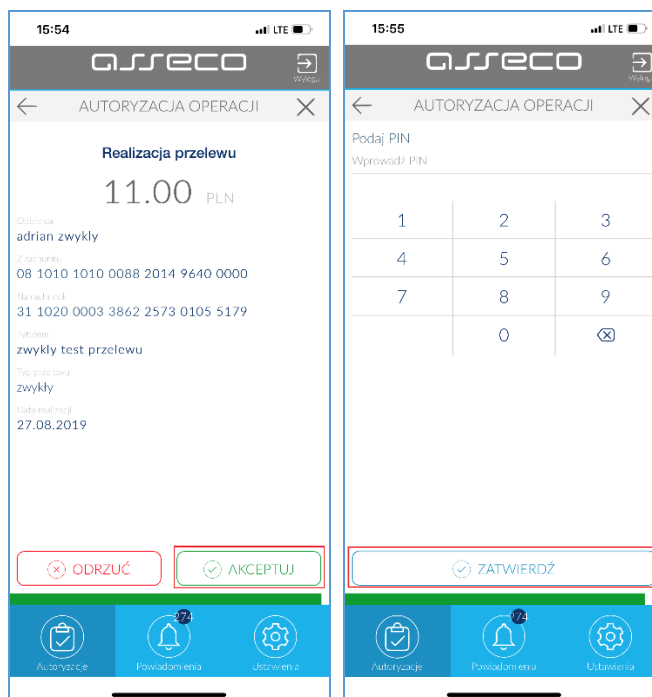
systemu:

**ii) autoryzacja:**

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:



Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem w procesie autoryzacji:



## KLIENCI KORPORACYJNI

### def3000/CEB – dostosowanie do wymagań SCA

#### KARTA MIKROPROCESOROWA

- a) Wygląd formatek dla użytkownika  
 i) **autentykacja:**

Wybór metody autentykacji – Logowanie karta mikroprocesorową:

The screenshot shows a web interface titled "Autoryzacja". At the top, it says "Proszę wprowadzić PIN oraz nacisnąć przycisk 'Zatwierdź'". Below this, there is a "Logowanie:" label followed by a dropdown menu where "Logowanie kartą mikroprocesorową" is selected. Underneath is a "PIN:" label followed by an empty input field. At the bottom, there is a "Zatwierdź" button.

Umieszczenie karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenie numeru PIN karty mikroprocesorowej:

This screenshot is identical to the previous one, but the "PIN:" input field now contains four asterisks (\*\*\*\*), indicating that the PIN has been entered.

- ii) **autoryzacja:**

Umieszczenie karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenie numeru PIN karty mikroprocesorowej:

**Przelew - akceptowanie**

Referencje:	
Rachunek do obciążenia:	40 8818 0009 3001 0000 0123 0002 Rachunek pomocniczy
Nazwa kontrahenta:	Test Przelewów
Nr rachunku kontrahenta:	87 9484 1017 1600 0224 2590 0001
Tytułem:	Szablon
Przelew VAT:	Nie
Kwota:	10,00 PLN
Droga płatności:	Elixir
Data:	2019-07-09
Zleceniodawca:	bankowy jan

**Log:**  
2019-07-09 13:00 Nowy przelew - DSL 2

## TOKEN VASCO + KARTA MIKROPROCESOROWA

- a) Wygląd formatek dla użytkownika  
 i) **autentykacja token VASCO DP260:**

Wybór metody autentykacji – Logowanie tokenem VASCO:

**Autoryzacja**

Proszę wprowadzić Identyfikator użytkownika i Klucz w odpowiednie pola oraz nacisnąć przycisk "Zatwierdź".

Logowanie: Logowanie tokenem VASCO ⓘ

Identyfikator użytkownika:  ⓘ

Klucz:  ⓘ

:

- ii) **autoryzacja kartą mikroprocesorową z aplikacją SCSA (e-Podpis):**

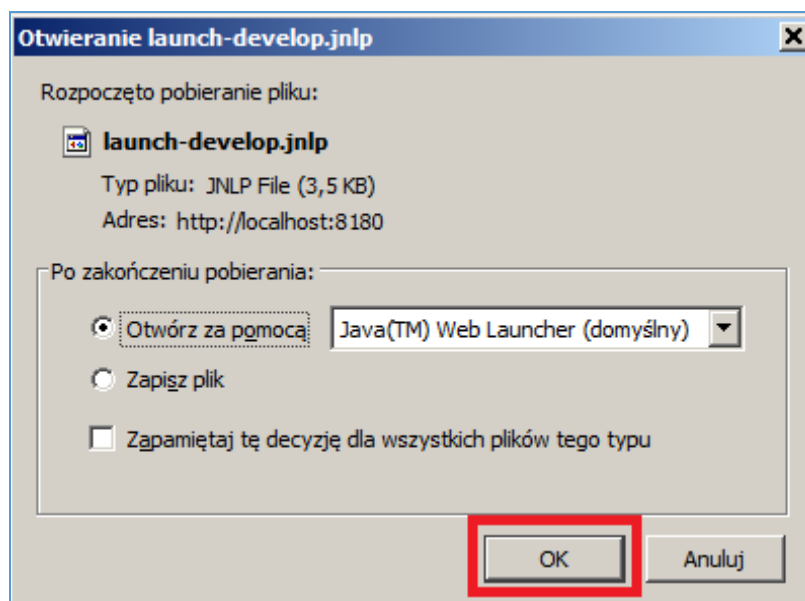
Przed podpisem należy uruchomić link „Uruchom aplikację SCSA”. Spowoduje to:

- pobranie (przy pierwszym użyciu dla nowej stacji roboczej), lub
- uruchomienie (przy kolejnym użyciu)

Przelew - akceptowanie	
Referencje:	
Rachunek do obciążenia:	87 8707 0006 0001 2830 3000 0001
Nazwa kontrahenta:	Nowy1 Kont111 33-696 Testowy Miasto
Nr rachunku kontrahenta:	18 8355 0009 0000 6129 1000 0005
Tytułem:	test
Przelew VAT:	Tak
Kwota:	1,00 PLN
W tym kwota VAT:	1,00 PLN
Identyfikator dostawcy:	11
Numer faktury:	111
Droga płatności:	Elixir
Data:	2019-08-01
Zleceniodawca:	Meksyk TEST 2 33-699 TEST

Uruchom aplikację SCOSA  
 Podpisz  
 Zamknij

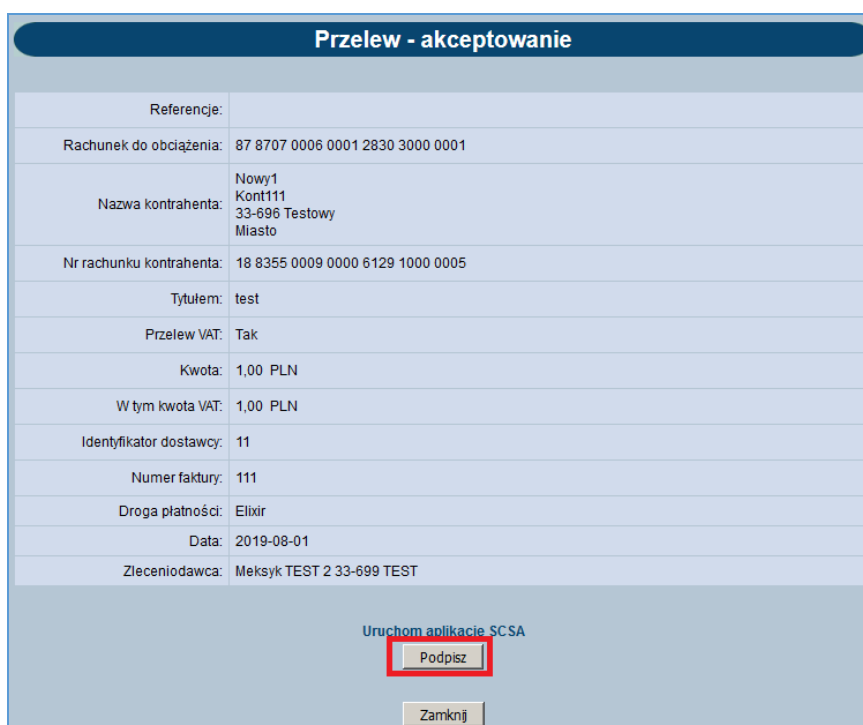
Uruchomienie linku „Uruchom aplikację SCOSA” spowoduje, że przeglądarka automatycznie pobierze plik JNLP, który uruchomi (lub pobierze i uruchomi) aplikację SCOSA (e-Podpis):



Po uruchomieniu pliku JNLP Użytkownikowi automatycznie pojawi się okno aplikacji SCOSA (e-Podpis). Zalogowanie do aplikacji SCOSA wymaga umieszczenia karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenia numeru PIN karty mikroprocesorowej:



Po uruchomieniu aplikacji SCSA (e-Podpis) i po podaniu PINu (dla logowania do e-Podpis), wybieramy przycisk [Podpisz]:



Po użyciu przycisku [Podpisz] formatka „Przelew – akceptowanie” przejdzie w tryb „Oczekiwanie na podpis aplikacją SCSA”:

Przelew - akceptowanie	
Referencje:	
Rachunek do obciążenia:	87 8707 0006 0001 2830 3000 0001
Nazwa kontrahenta:	Nowy1 Kont111 33-696 Testowy Miasto
Nr rachunku kontrahenta:	18 8355 0009 0000 6129 1000 0005
Tytułem:	test
Przelew VAT:	Tak
Kwota:	1,00 PLN
W tym kwota VAT:	1,00 PLN
Identyfikator dostawcy:	11
Numer faktury:	111
Droga płatności:	Elixir
Data:	2019-08-01
Zleceniodawca:	Meksyk TEST 2 33-699 TEST

Powiadomienie autoryzacyjne zostało wysłane na aplikację SCSA.  
Pozostań na stronie i potwierdź operację w aplikacji SCSA.



Oczekiwanie na podpis aplikacją SCSA

Następnie należy wykonać autoryzację zlecenia (podpis) w aplikacji SCSA. W tym celu wymagane jest umieszczenie karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenie numeru PIN karty mikroprocesorowej:

e-Podpis (podpis niekwalifikowany)

e-Podpis



Dane do podpisu:

Przelew zwykły

Kwota: 199,00 PLN

Na rachunek: 50 1910 1048 2511 0000 9957 0000

Kontrahent: Kowalski Jan

Tytuł sasasas

Podaj PIN:

••••

Po poprawnej autoryzacji zlecenia (podpisie ) otrzymujemy potwierdzenie autoryzacji:



## Instalacja środowiska JWS Client

Instalator środowiska JWS Clinet<sup>i</sup> został udostępniony w lokalizacji :

<https://www.bsklodzko.pl/pliki-do-pobrania>

Powyższy instalator jest niezbędny do poprawnego uruchomienia aplikacji SCSA podczas podpisu przelewu w bankowości korporacyjnej.