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

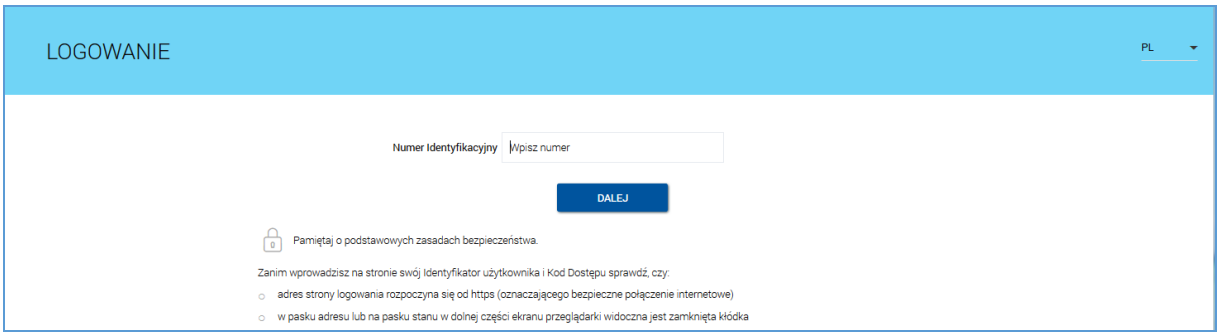
KLIENCI INDYWIDUALNI

SMS

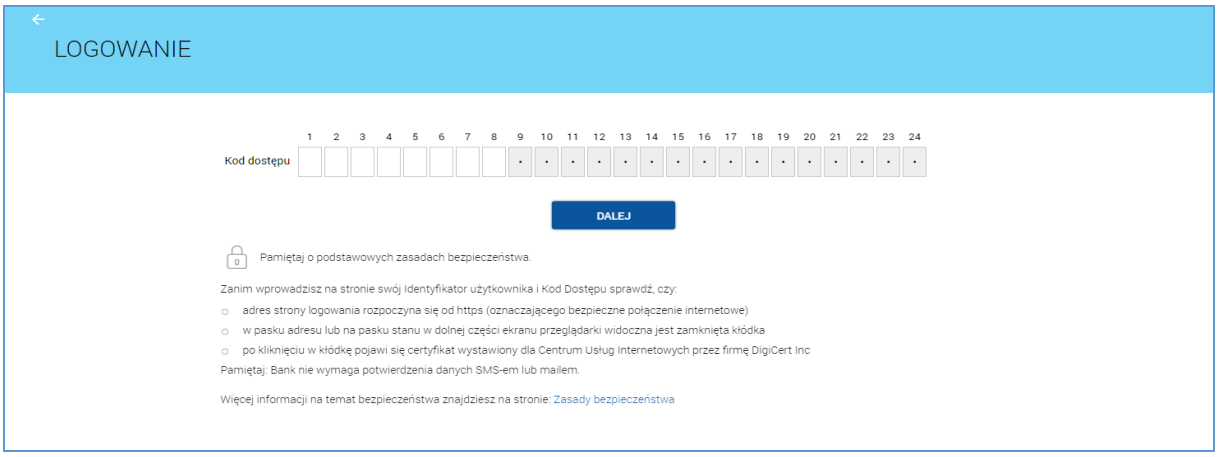
Wygląd formatek dla użytkownika po wprowadzeniu SCA

i) autentykacja:

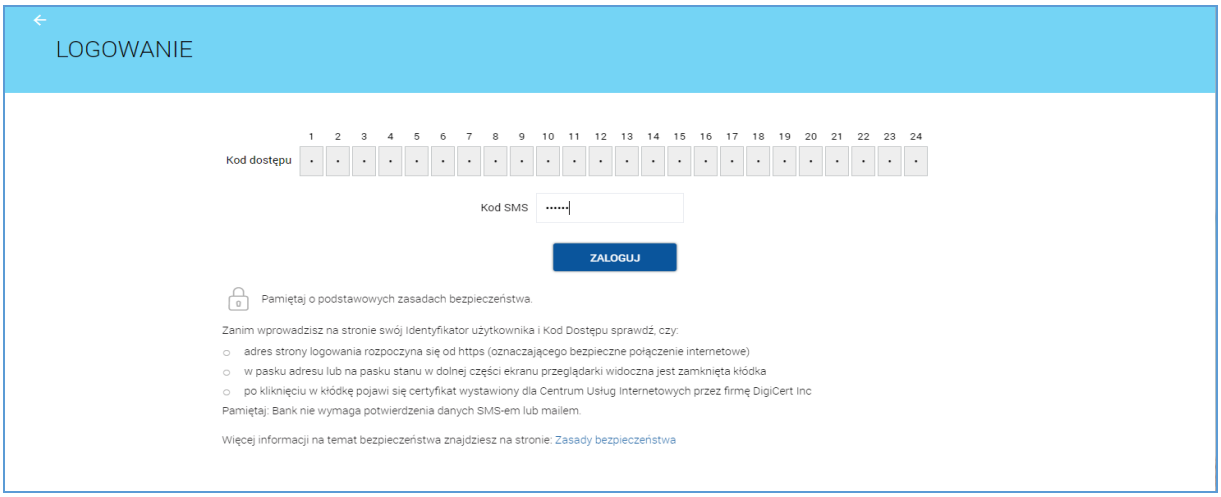
Wprowadzenie identyfikatora użytkownika:



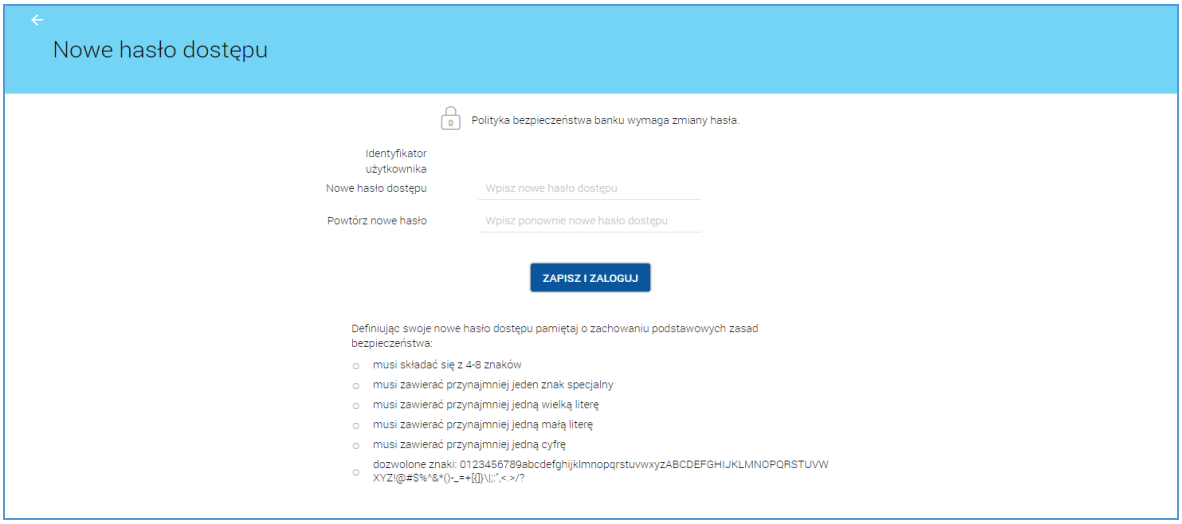
Wprowadzenie tymczasowego hasła, który klient otrzymał w wiadomości SMS:



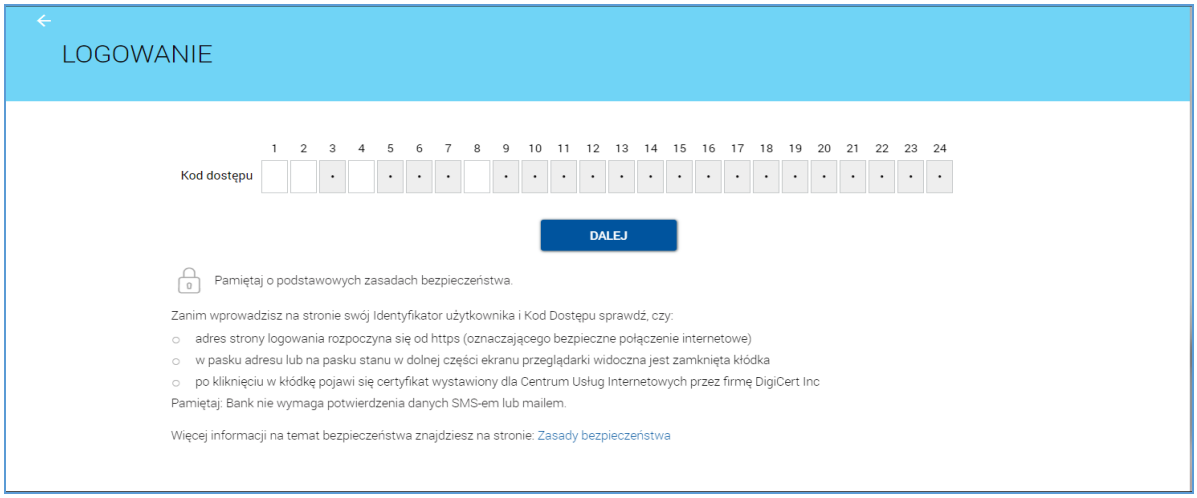
Zatwierdzanie tymczasowego hasła kodem SMS:



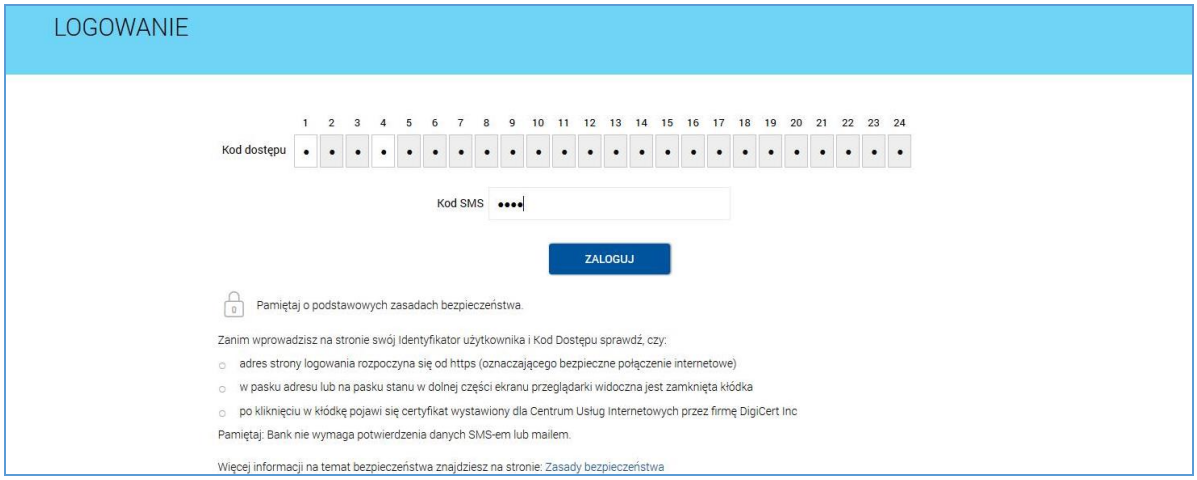
Ustalenie nowego hasła:



Ponowne logowanie do aplikacji z użyciem nowego hasła:

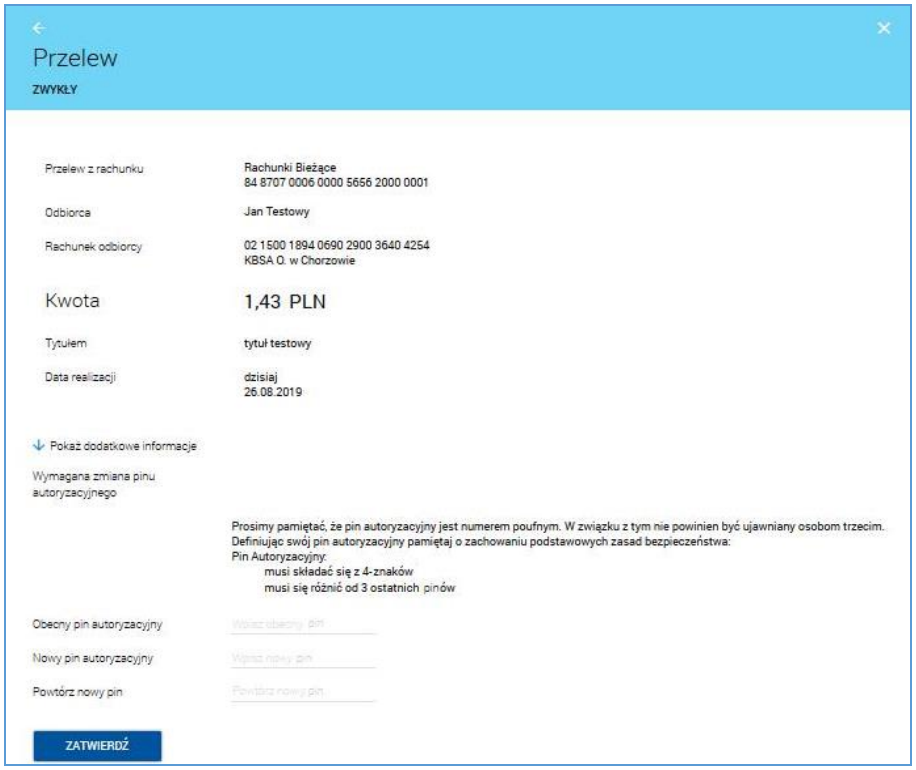


Wprowadzenie kodu SMS:

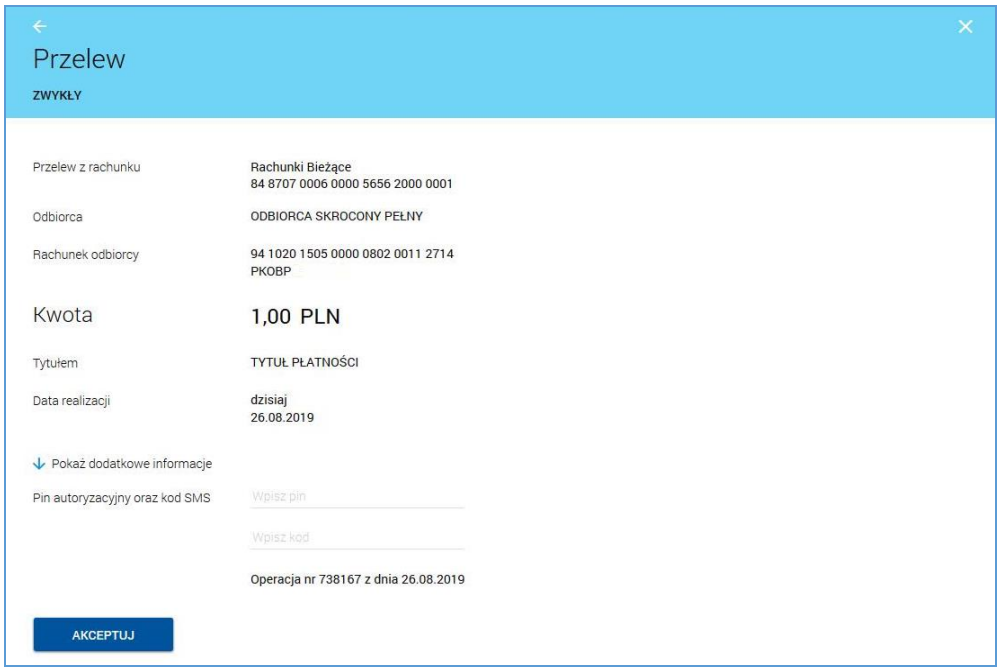


ii) autoryzacja:

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



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

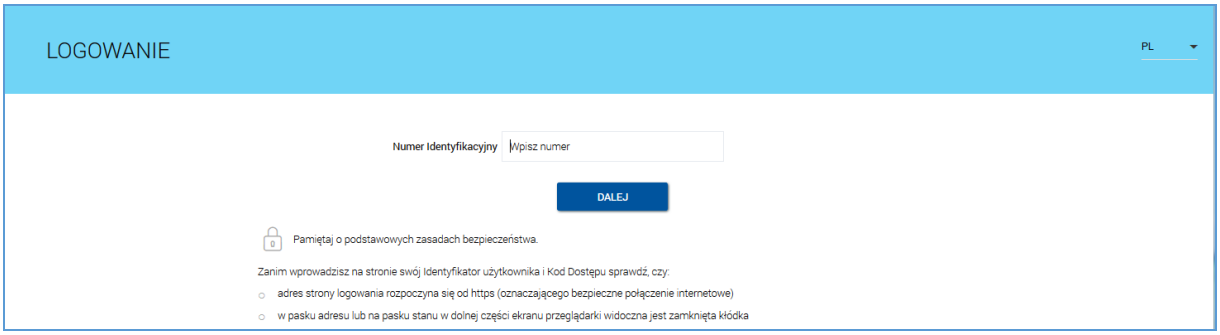


MAA

Wygląd formatek dla użytkownika

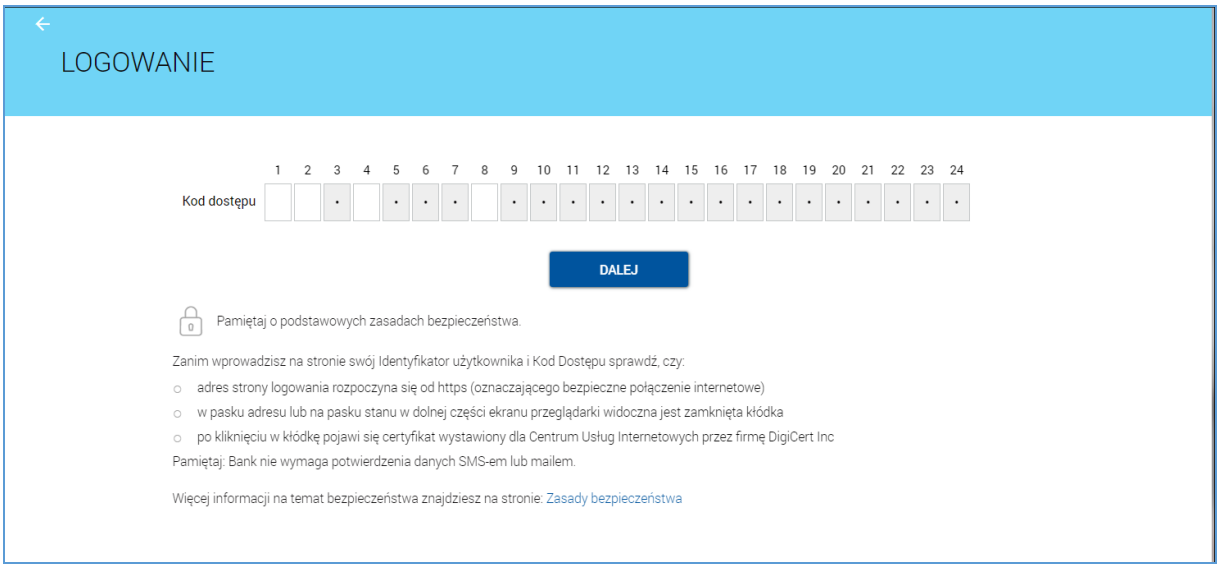
i) autentykacja:

Wprowadzenie identyfikatora użytkownika:



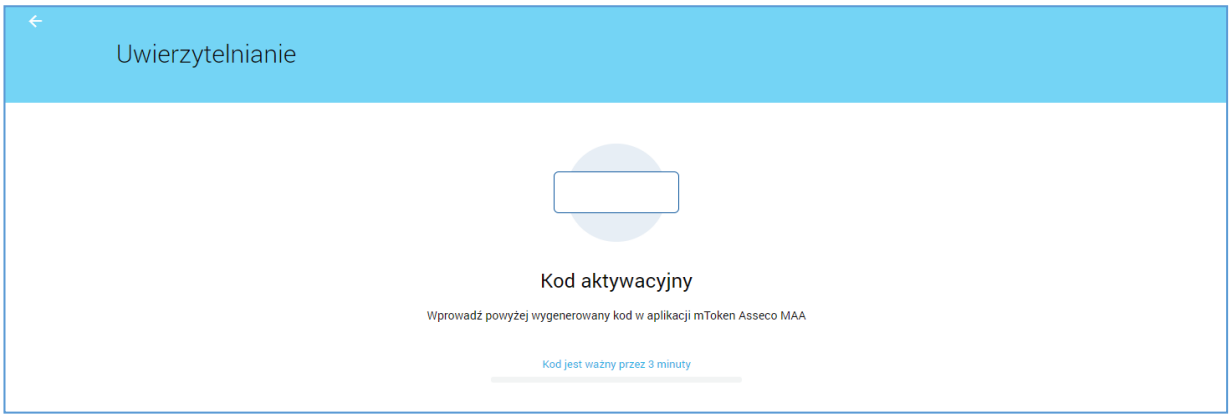
Wprowadzenie hasła maskowanego:

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.

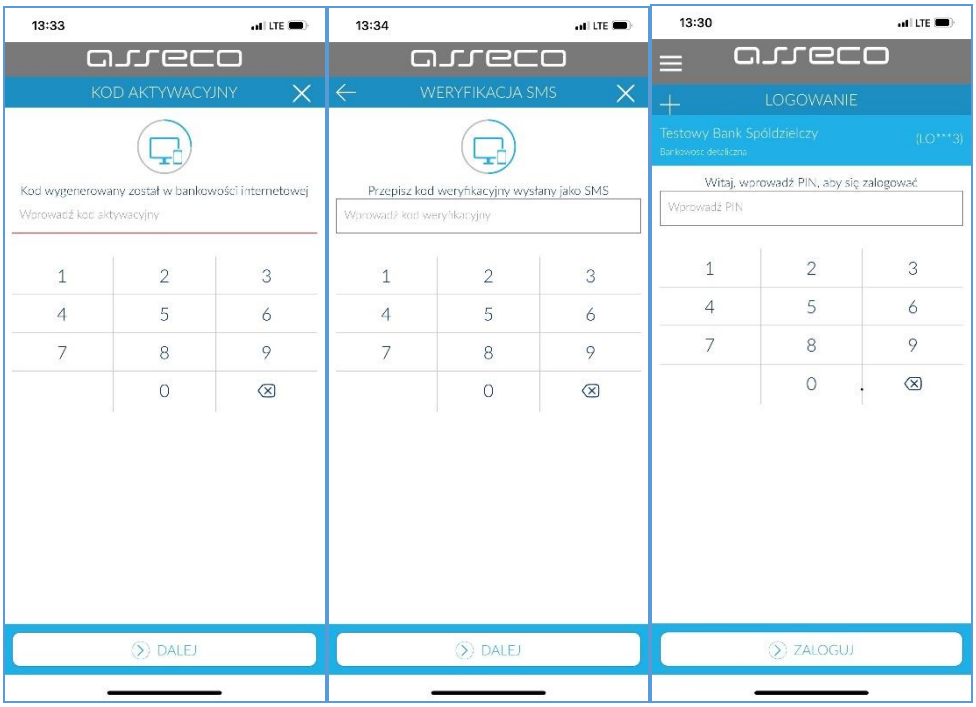


W przypadku braku sparowanego urządzenia, aplikacja wyświetli komunikat o sparowaniu urządzenia.

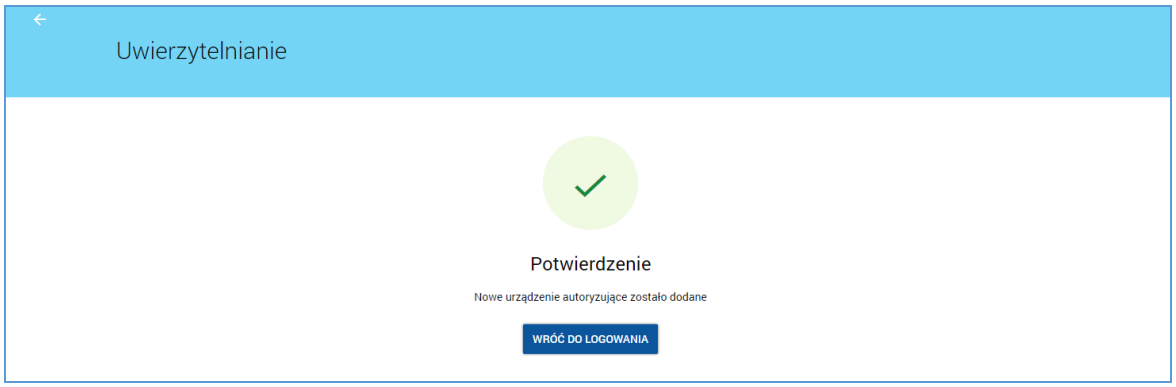
Po tym komunikacie, klient powinien pobrać aplikację na urządzenie mobilne. Po pobraniu aplikacji na urządzenie mobilne, w aplikacji internetowej Asseco CBP należy wybrać opcję „Posiadam aplikację”, gdzie wyświetla się kod aktywacyjny.



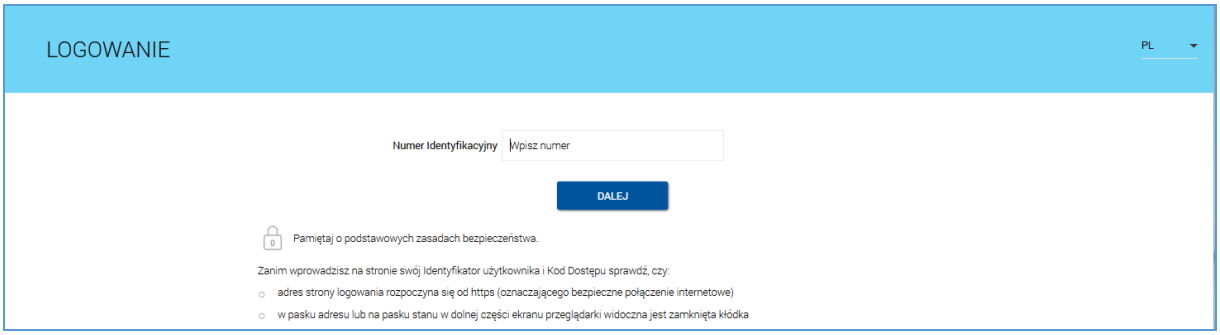
Na urządzeniu mobilnym klient, dodaje nowe urządzenie poprzez znak „+" i wprowadza kod, który wyświetli się w aplikacji internetowej (Kod w aplikacji Asseco CBP pokaże się po wejściu w opcję „Posiadam aplikację" (patrz zrzut powyżej)). W kolejnym kroku należy podać kod SMS, który zostanie przesłany na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



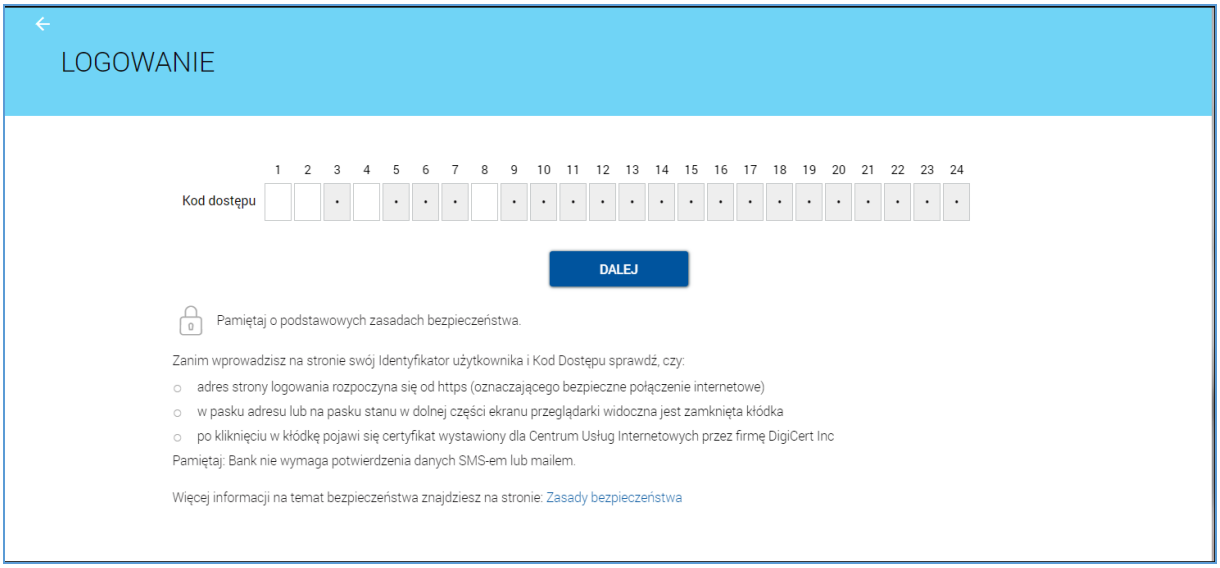
Po wykonaniu w/w czynności, w aplikacji pojawi się komunikat o poprawnym sparowaniu. I system poprosi o ponowne zalogowanie do bankowości.



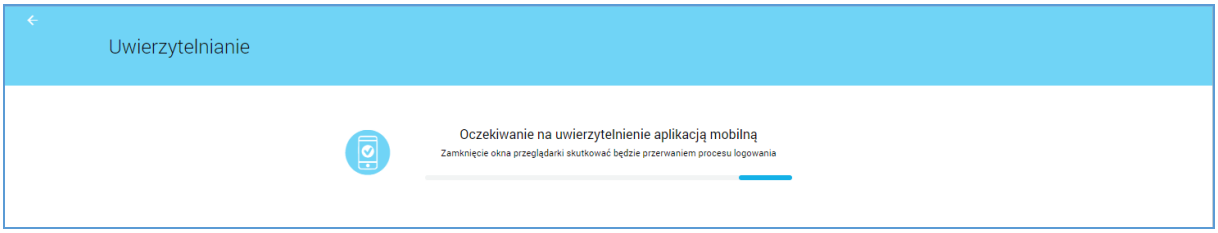
Wówczas ponownie należy wykonać akcję logowania: wprowadzenie identyfikatora użytkownika:



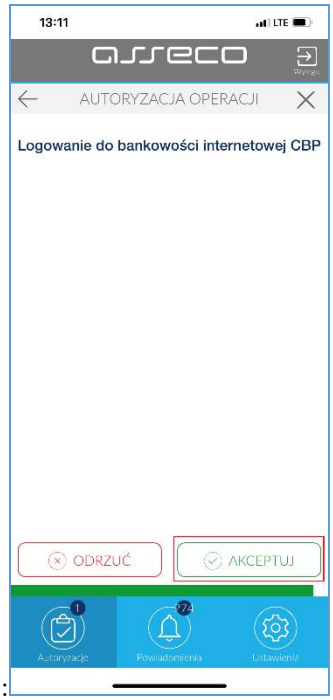
Wprowadzenie hasła maskowanego:

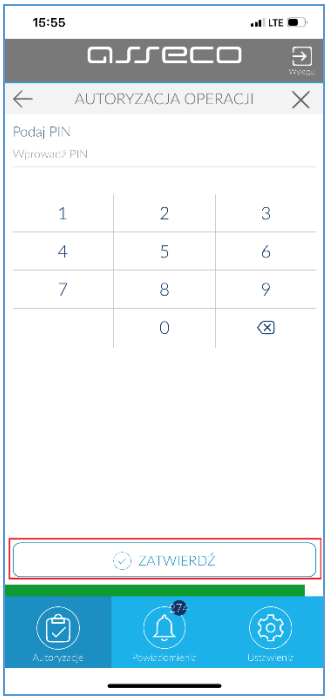


Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:



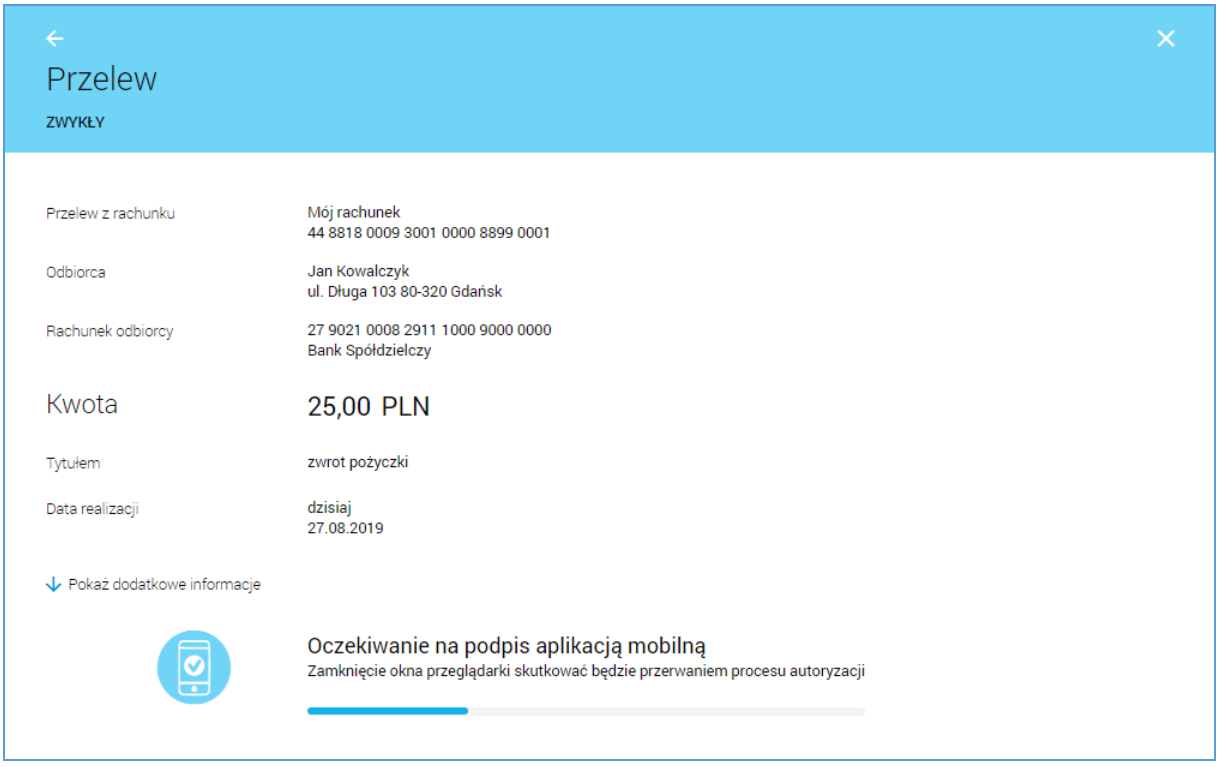
Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem logowania do systemu:



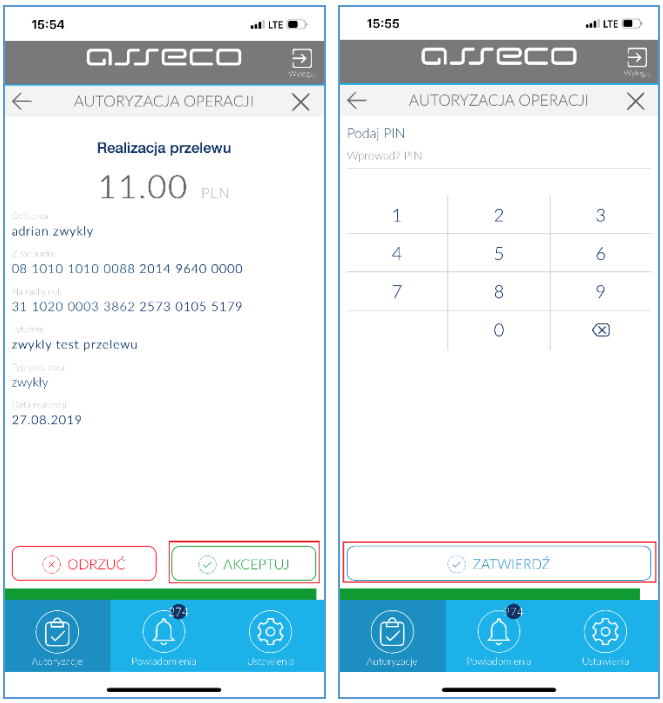


ii) autoryzacja:

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:



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


15:54
LTE
AUTORYZACJA OPERACJI
Realizacja przelewu
11.00 PLN
adrian zwykly
08 1010 1010 0088 2014 9640 0000
31 1020 0003 3862 2573 0105 5179
zwykly test przelewu
zwykły
27.08.2019
ODRZUĆ
AKCEPTUJ
Autoryzacje
Powiadomienia
Ustawienia
15:55
LTE
AUTORYZACJA OPERACJI
Podaj PIN
Wprowadź PIN
1 2 3
4 5 6
7 8 9
0
ZATWIERDŹ
Autoryzacje
Powiadomienia
Ustawienia

KLIENCI KORPORACYJNI

def3000/CEB – dostosowanie do wymagań SCA

KARTA MIKROPROCESOROWA

a) Wygląd formatek dla użytkownika

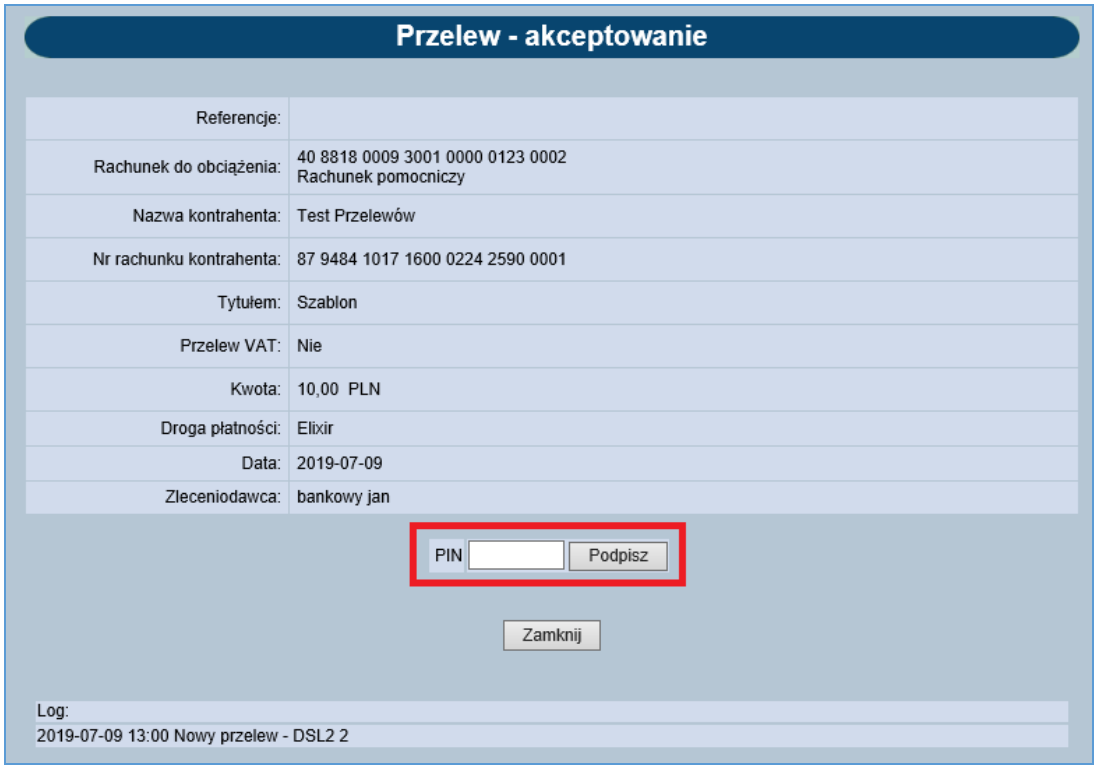
i) autentykacja:

Wybór metody autentykacji – Logowanie karta mikroprocesorową:

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

ii) autoryzacja:

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

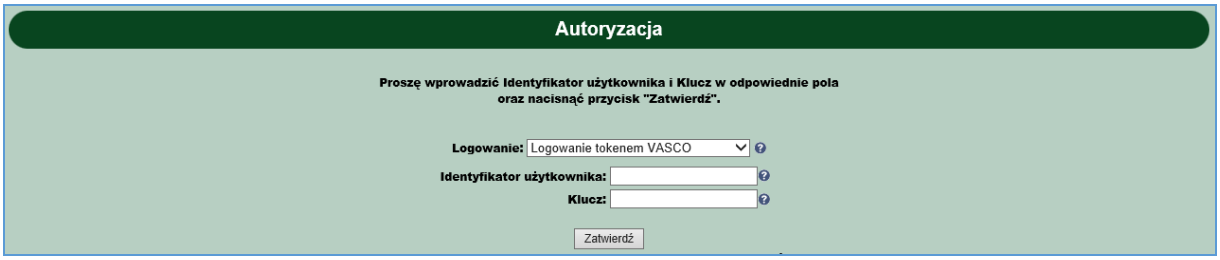


TOKEN VASCO + KARTA MIKROPROCESOROWA

a) Wygląd formatek dla użytkownika

i) autentykacja token VASCO DP260:

Wybór metody autentykacji – Logowanie tokenem VASCO:

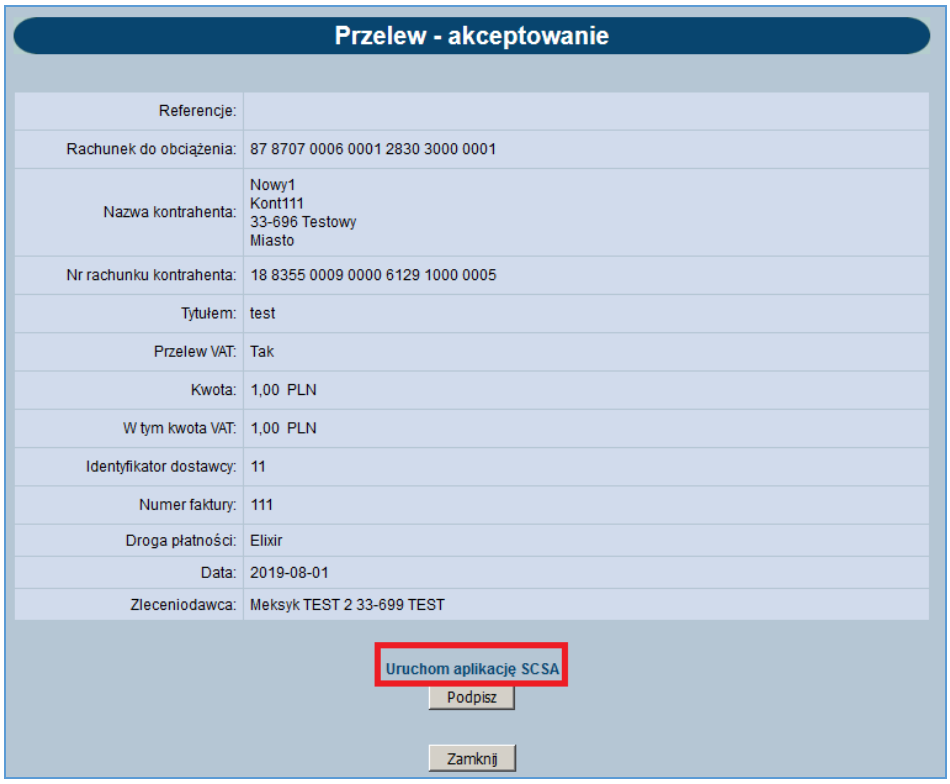


:

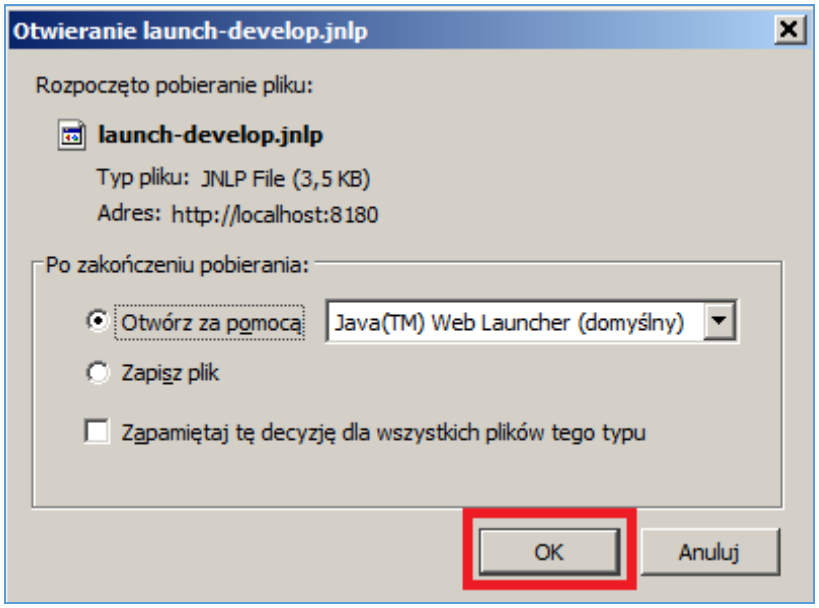
ii) autoryzacja kartą mikroprocesorową z aplikacją SCSA (e-Podpis):

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

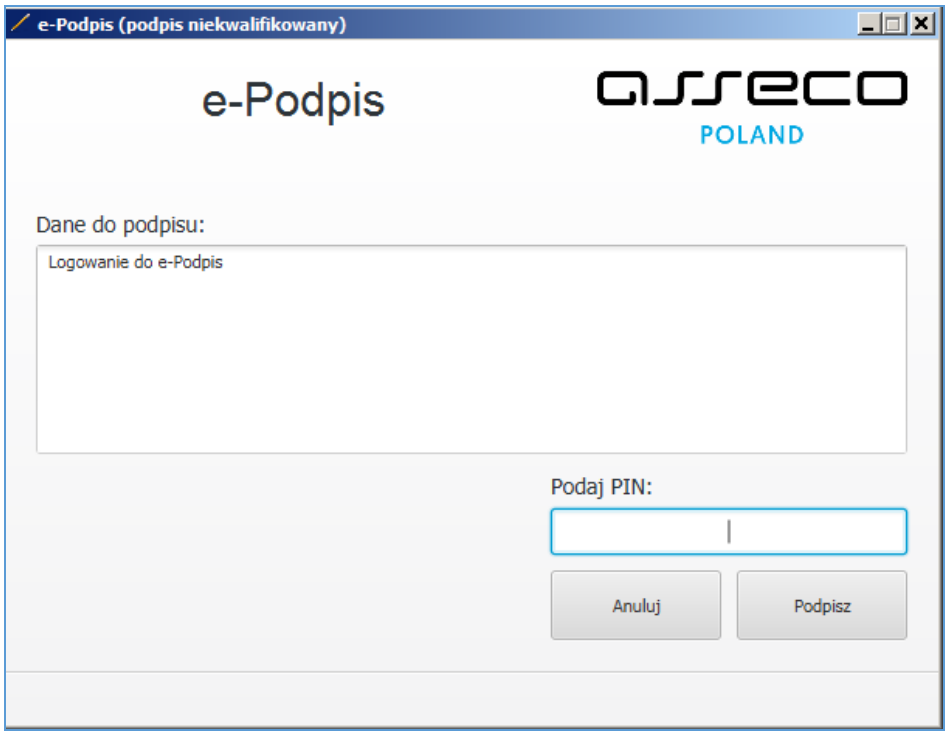
- pobranie (przy pierwszym użyciu dla nowej stacji roboczej), lub
- uruchomienie (przy kolejnym użyciu)



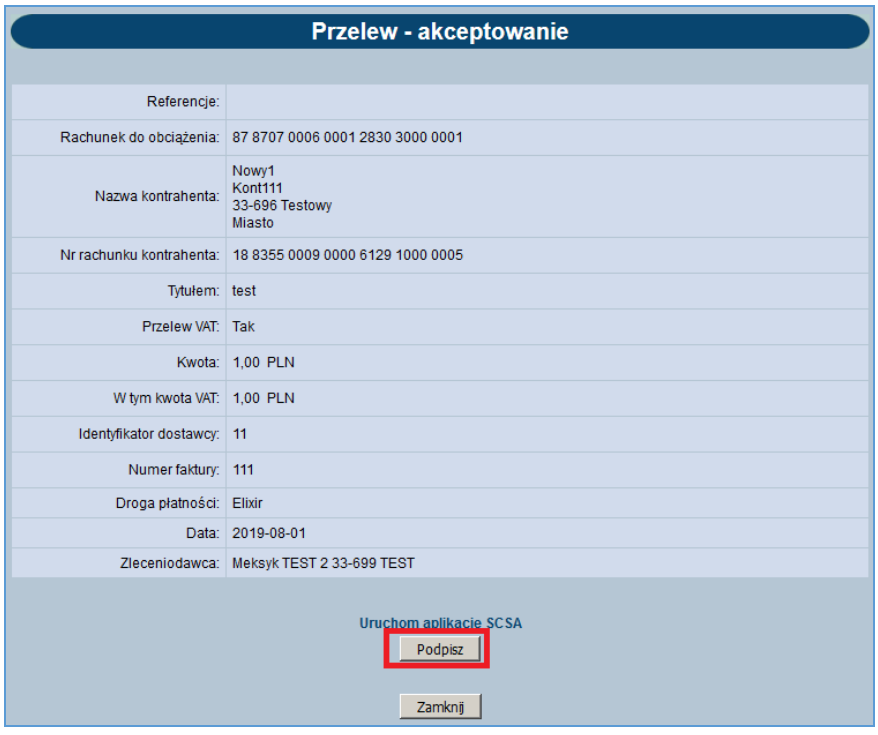
Uruchomienie linku „Uruchom aplikację SCSA" spowoduje, że przeglądarka automatycznie pobierze plik JNLP, który uruchomi (lub pobierze i uruchomi) aplikację SCSA (e-Podpis):



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

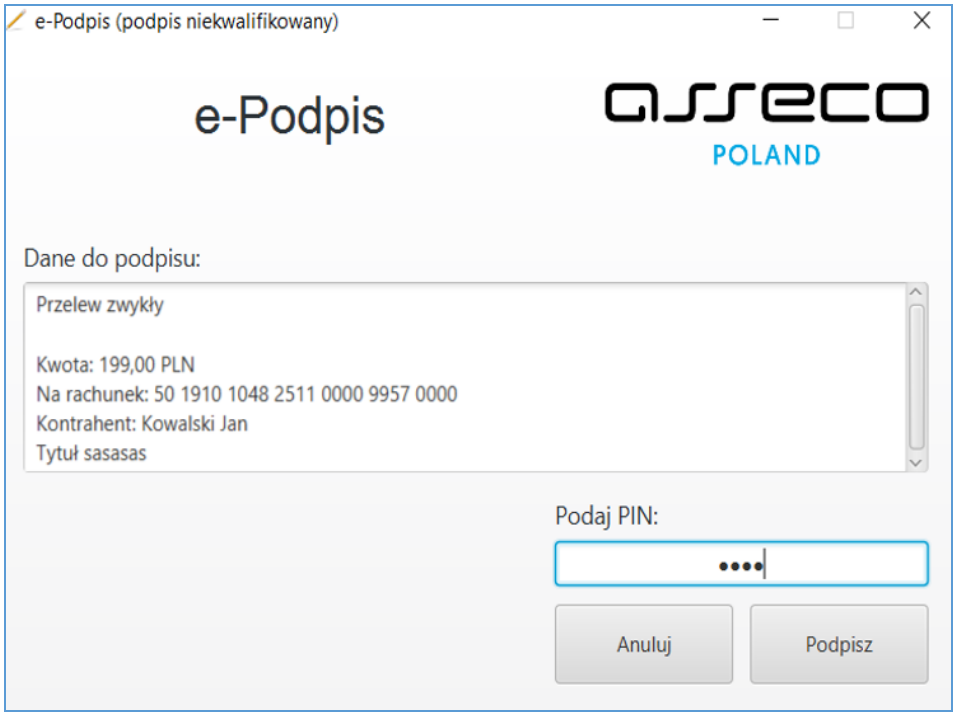


Po uruchomieniu aplikacji SCSA (e-Podpis) i po podaniu PINu (dla logowania do e-Podpis), wybieramy przycisk [Podpisz]:

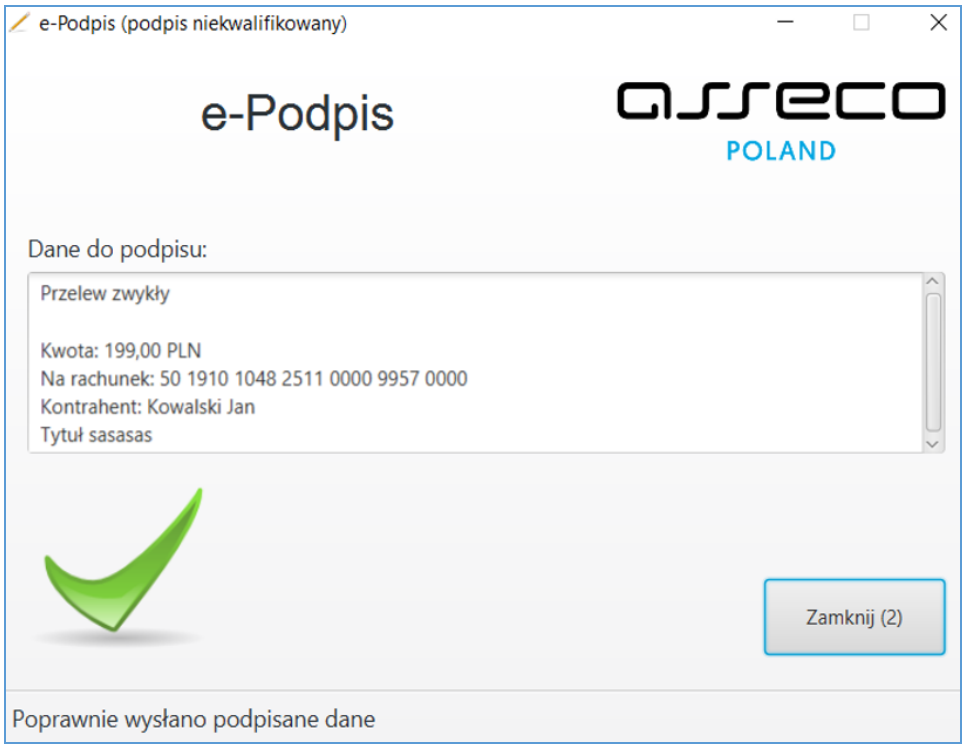


Po użyciu przycisku [Podpisz] formatka „Przelew – akceptowanie” przejdzie w tryb „Oczekiwanie na podpis aplikacją SCSA”:

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:



Po poprawnej autoryzacji zlecenia (podpisie) otrzymujemy potwierdzenie autoryzacji:



Instalacja środowiska JWS Client

Instalator środowiska JWS Clinet[i] 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.