Instrukcja dla klientów indywidualnych opisująca stosowane środki dostępu i autoryzacji w systemie bankowości internetowej w Banku Spółdzielczym Ziemi Łęczyckiej w Łęczycy po 13 września 2019 r. z zastosowaniem tzw. silnego uwierzytelniania

Opracowano na podstawie instrukcji przygotowanej przez Asseco Poland dla bankowości dla klienta indywidualnego – Asseco CBP oraz def3000/CEB do wymagań SCA (silne uwierzytelnianie)

Łęczyca 2019

Szanowni Państwo

W związku z wejściem w życie od 13 września br. zapisów Dyrektywy PSD2 środki dostępu i autoryzacji używane w bankowości internetowej BSZŁ w Łęczycy zostaną dostosowane do wymogów silnego uwierzytelniania (SCA)

Zostaną uzupełnione dodatkowo o wymagania SCA (tzw.: „silne uwierzytelnienie klienta”). **Silne uwierzytelnianie klienta** - uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.

Dostosowanie do wymogów dotyczy zarówno procesu autentykacji (logowania do bankowości internetowej) oraz autoryzacji (zatwierdzania przelewów).

Zarząd Banku dokonał przeglądu stosowanych rozwiązań oraz przygotował dla wszystkich klientów korzystających w bankowości elektronicznej rozwiązania zgodne z opisanymi w Dyrektywie Parlamentu Europejskiego i Rady (UE) (UE) 2015/2366 z dnia 25 listopada 2015 r. zwaną również Dyrektywą PSD2.

W związku z wymaganiami silnego uwierzytelniania uprzejmie informujemy, że w Banku przestaje funkcjonować autoryzacja oparta o Token RSA (nie spełnia powyżej wymienionych kryteriów). Wszystkich klientów użytkujących tego typu środek autentykacji i autoryzacji prosimy o jak najszybsze zgłoszenie się do placówek Banku celem zmiany środka autoryzacji na mToken Asseco MAA lub SMS+PIN

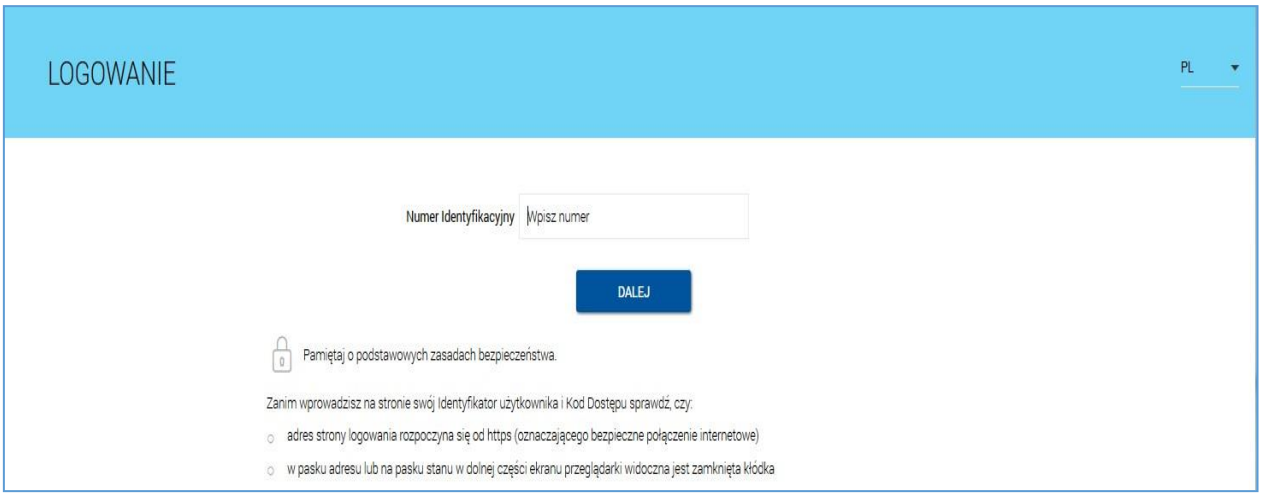
Opis wprowadzanych zmian w procesie autentykacji i autoryzacji w bankowości internetowej Banku

1. Klient indywidualny autoryzujący przelewy kodem SMS

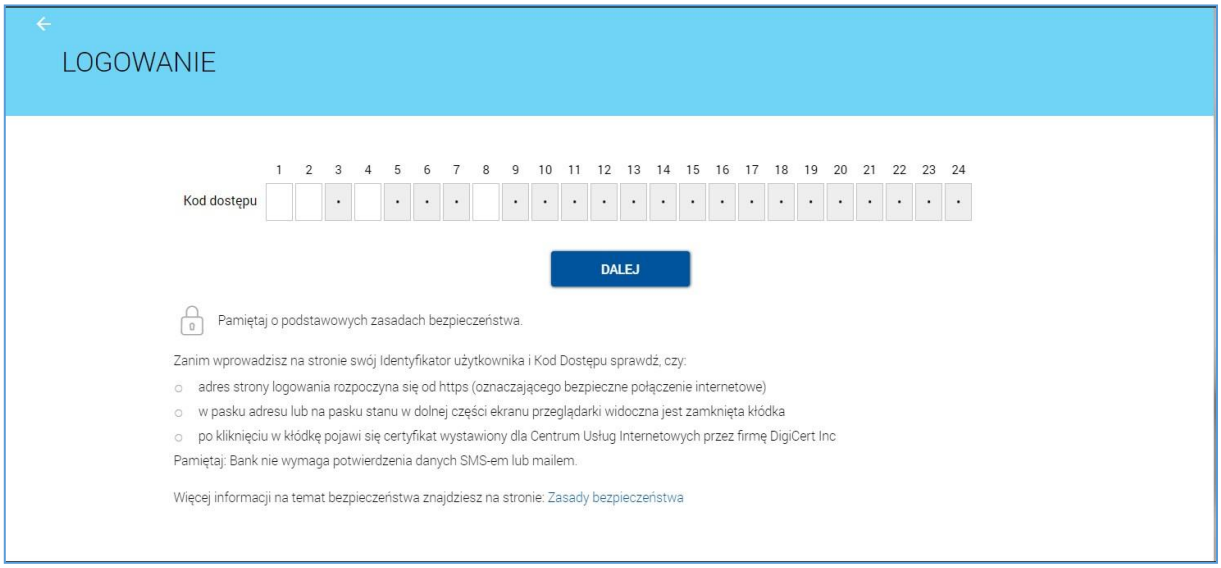
1.1 Logowanie do systemu bankowości internetowej zostanie uzupełnione o podanie dodatkowego numeru PIN. Numer PIN zostanie przysłany do użytkownika podczas pierwszej autoryzacji przelewu

1.2 Ekrany „nowego" logowania:

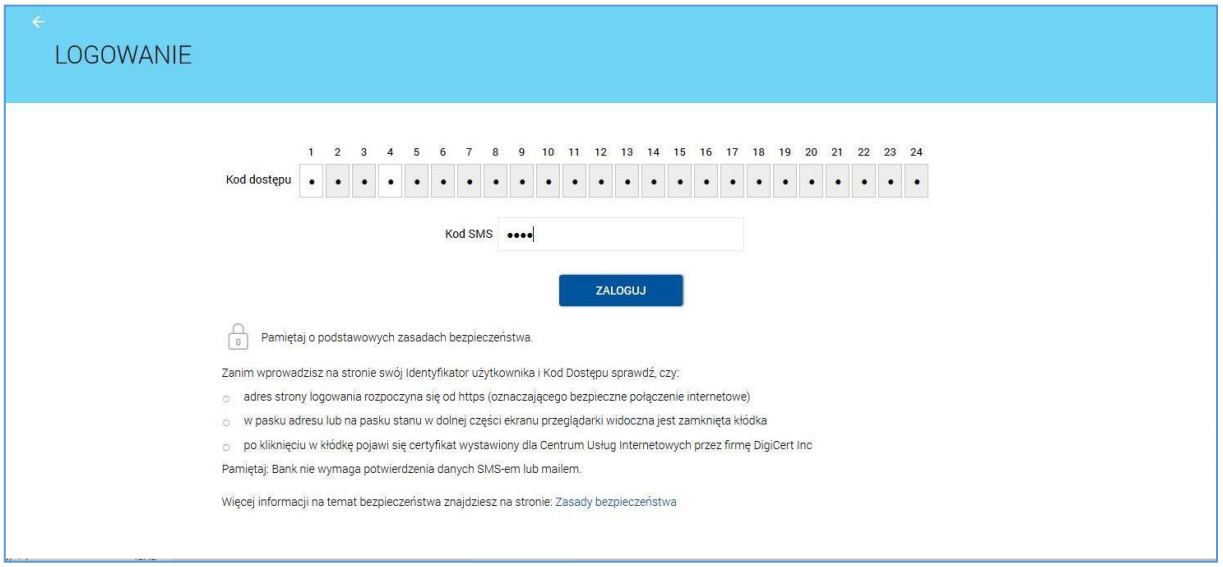
1.3 Wprowadzenie identyfikatora użytkownika (jak dotychczas):



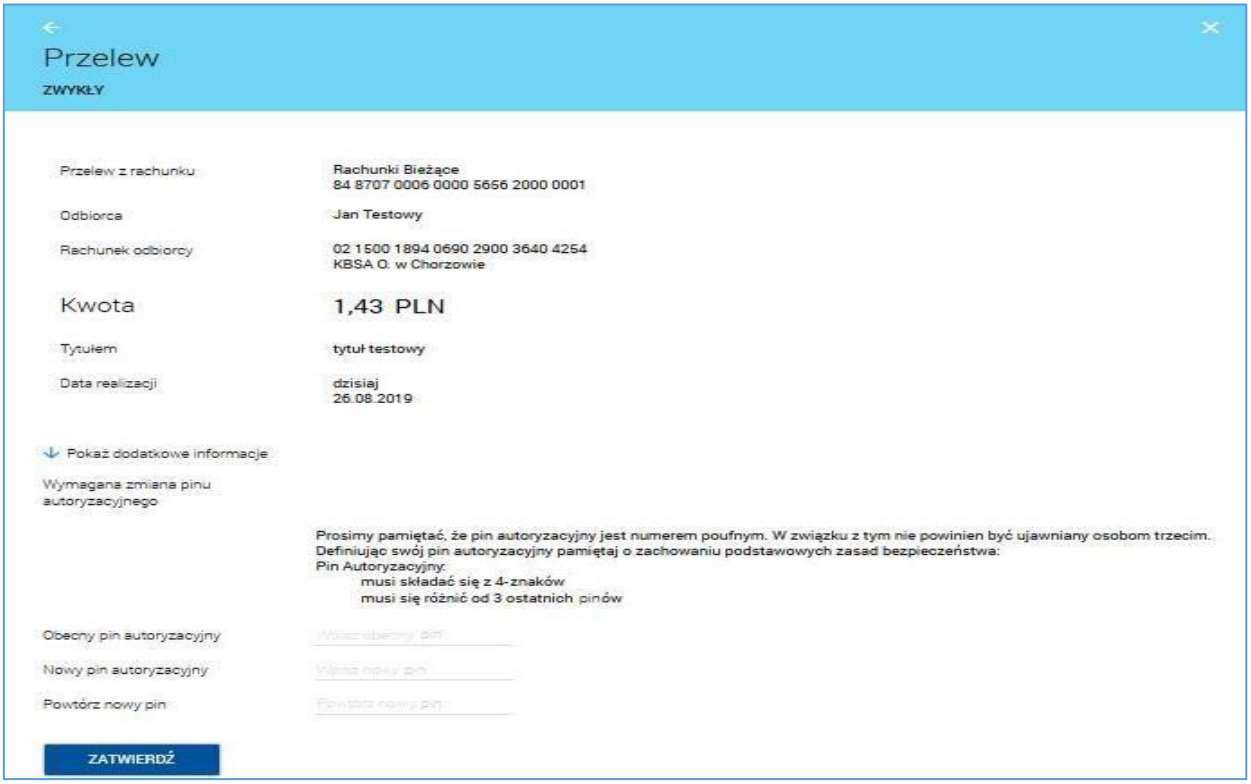
1.4 Wprowadzenie hasła maskowanego (jak dotychczas):



1.5 Wprowadzenie kodu SMS (nowy element logowania):



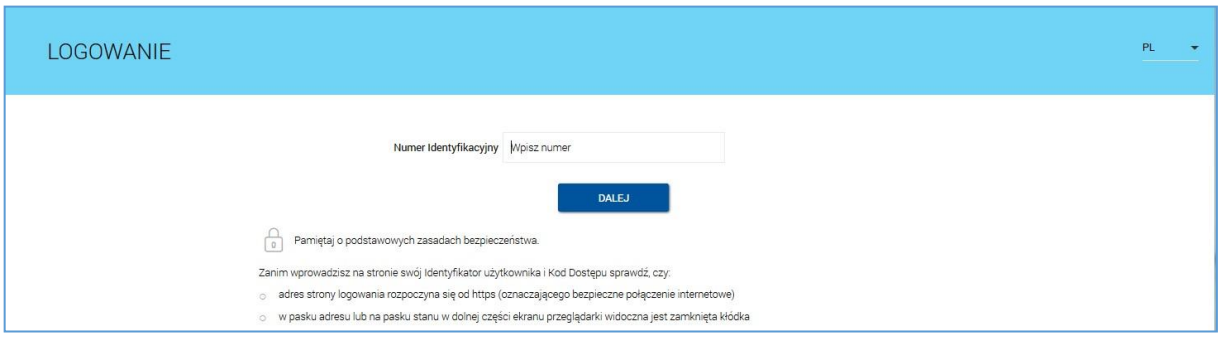
2. Autoryzacja (zatwierdzanie przelewu)**:**
Pierwsza autoryzacja będzie poprzedzona wysłaniem poprzez SMS jednorazowego numeru PIN wraz z wymuszeniem jego zmiany na **PIN znany tylko użytkownikowi**



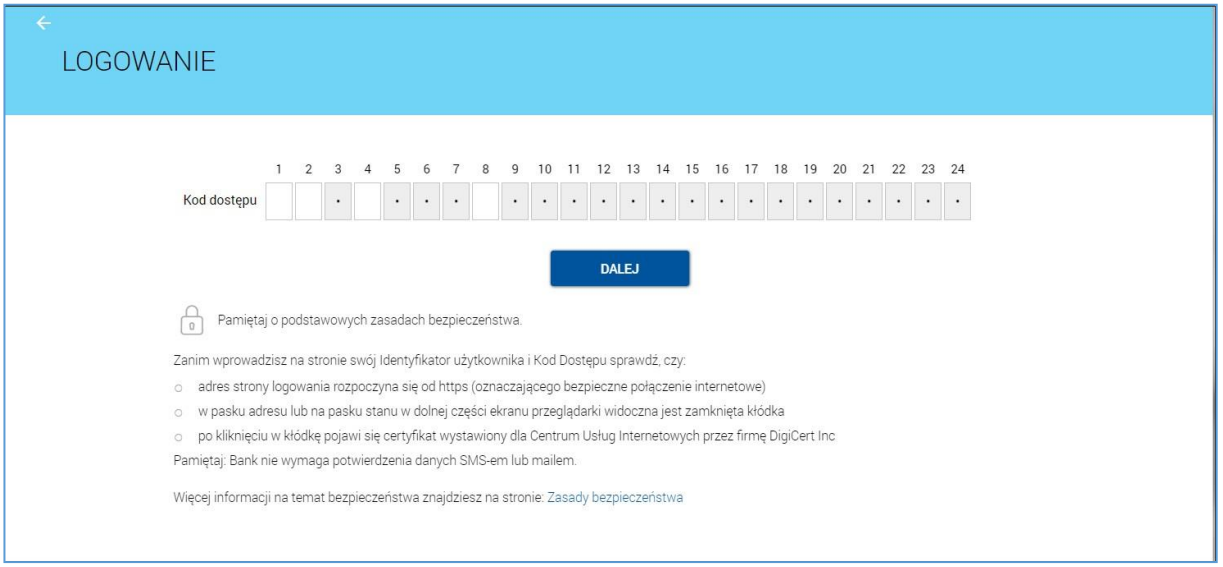
Kolejne autoryzacje będą wymagały wprowadzenia zdefiniowanego wcześniej PIN-u do podpisu oraz kodu SMS:

3. Klient indywidualny korzystający z mToken Asseco MMA

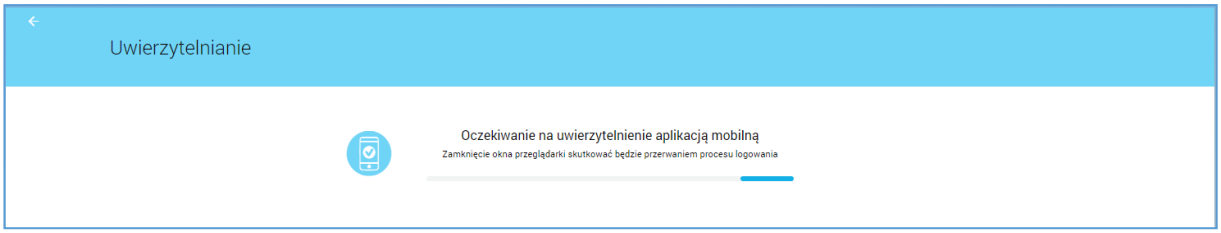
3.1 Logowanie -wprowadzenie identyfikatora użytkownika (jak dotychczas):



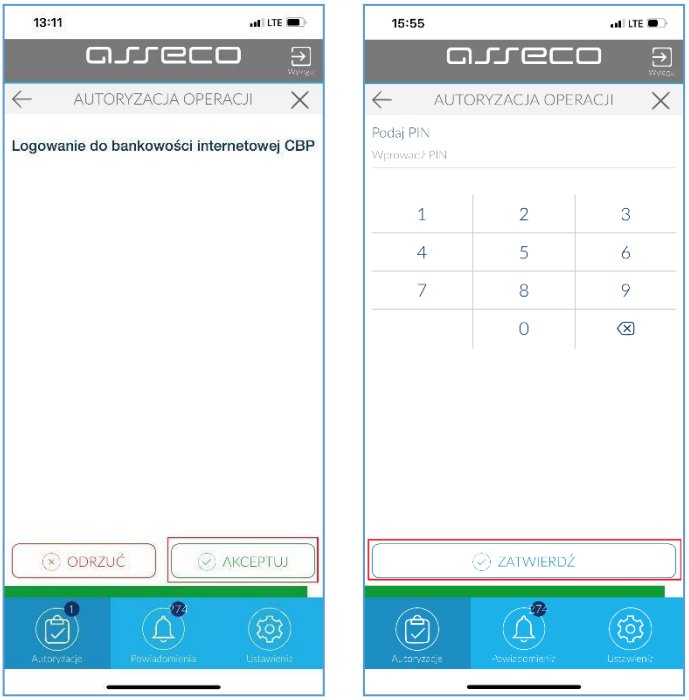
3.2 Wprowadzenie hasła maskowanego (jak dotychczas):



3.3 Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA (nowy element logowania):

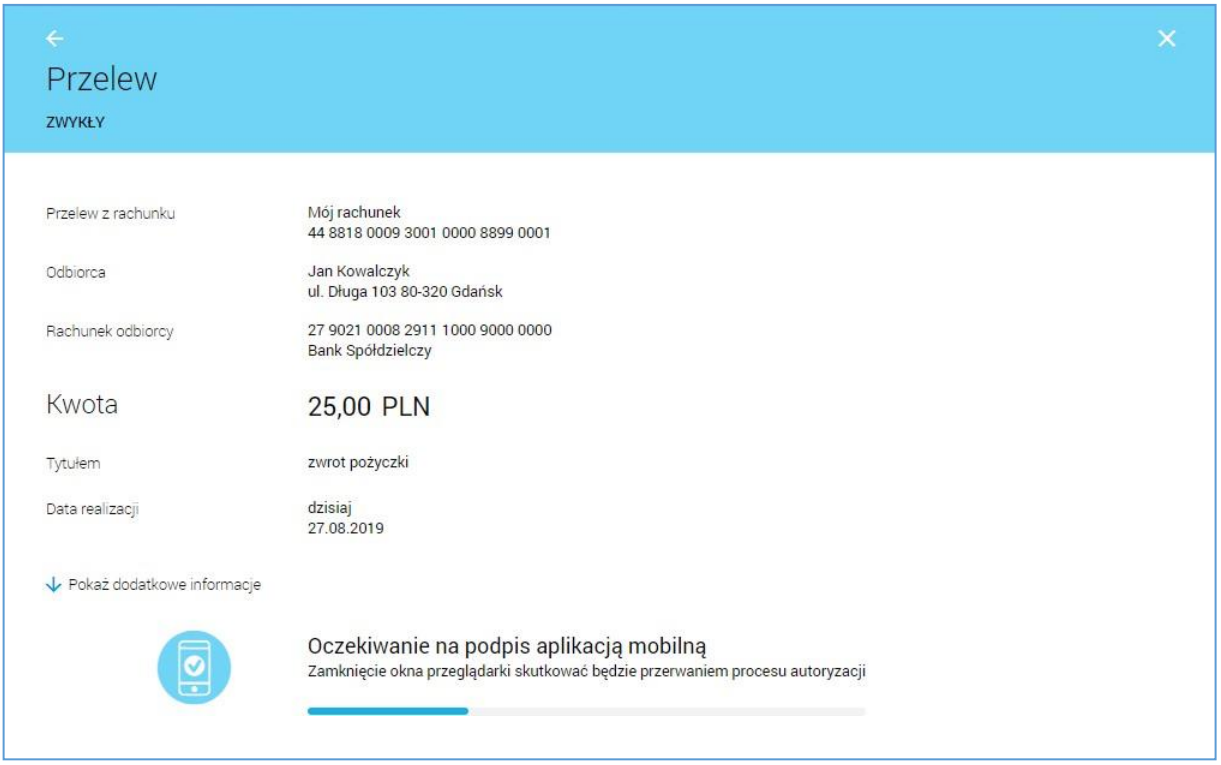


3.4 Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem logowania do systemu:



4. Autoryzacja (zatwierdzanie przelewu)**:**

4.1 Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA (jak dotychczas) :



4.2 Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem w procesie autoryzacji (jak dotychczas):