

**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)

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

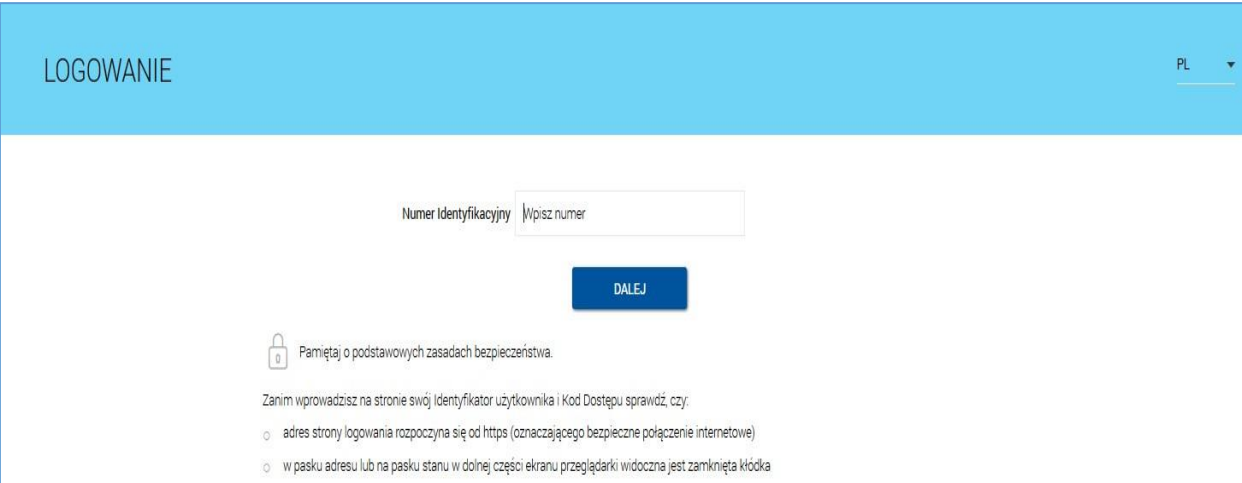
Opis wprowadzanych zmian w procesie autentykacji i autoryzacji w bankowości internetowej Banku

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 Ekran „nowego” logowania:


1.3 Wprowadzenie identyfikatora użytkownika (jak dotychczas):



LOGOWANIE PL ▼

Numer Identyfikacyjny

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


1.4 Wprowadzenie hasła maskowanego (jak dotychczas):

← 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:

- 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](#)

1.5 Wprowadzenie kodu SMS (nowy element logowania):


← 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:

- 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](#)

2. Autoryzacja (zatwierdzanie przelewu):

Pierwsza autoryzacja będzie poprzedzona wysłaniem poprzez SMS jednorazowego numeru PIN wraz z wymuszeniem jego zmiany na **PIN znany tylko użytkownikowi**

← 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
Kwota	1,43 PLN
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 type="text"/>
Nowy pin autoryzacyjny	<input type="text"/>
Powtórz nowy pin	<input type="text"/>

ZATWIERDŹ

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

← Przelew
ZWYKŁY

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

<input type="text"/>
<input type="text"/>

Operacja nr 738167 z dnia 26.08.2019

AKCEPTUJ


3. Klient indywidualny korzystający z mToken Asseco MMA

3.1 Logowanie -wprowadzenie identyfikatora użytkownika (jak dotychczas):

LOGOWANIE PL

Numer Identyfikacyjny

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


3.2 Wprowadzenie hasła maskowanego (jak dotychczas):

← 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:


- 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](#)

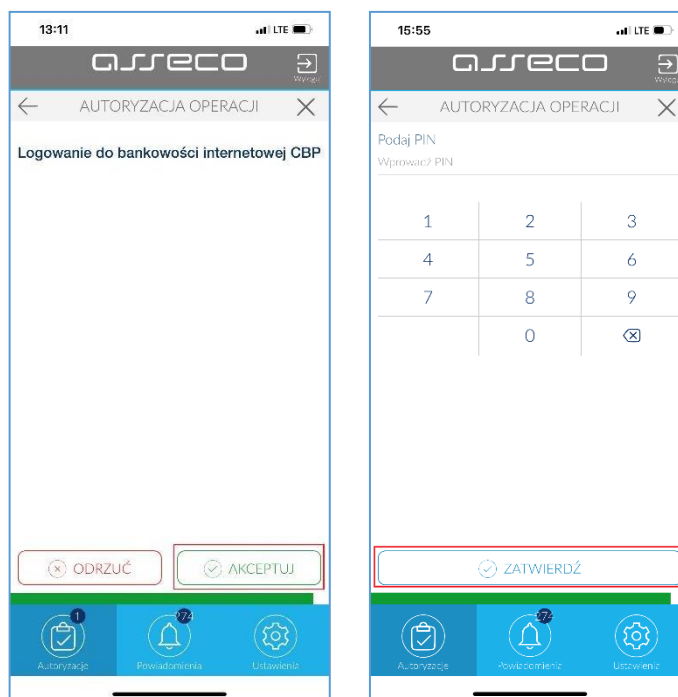
3.3 Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA (nowy element logowania):

← Uwierzytelnianie

 **Oczekiwanie na uwierzytelnienie aplikacją mobilną**
Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu logowania

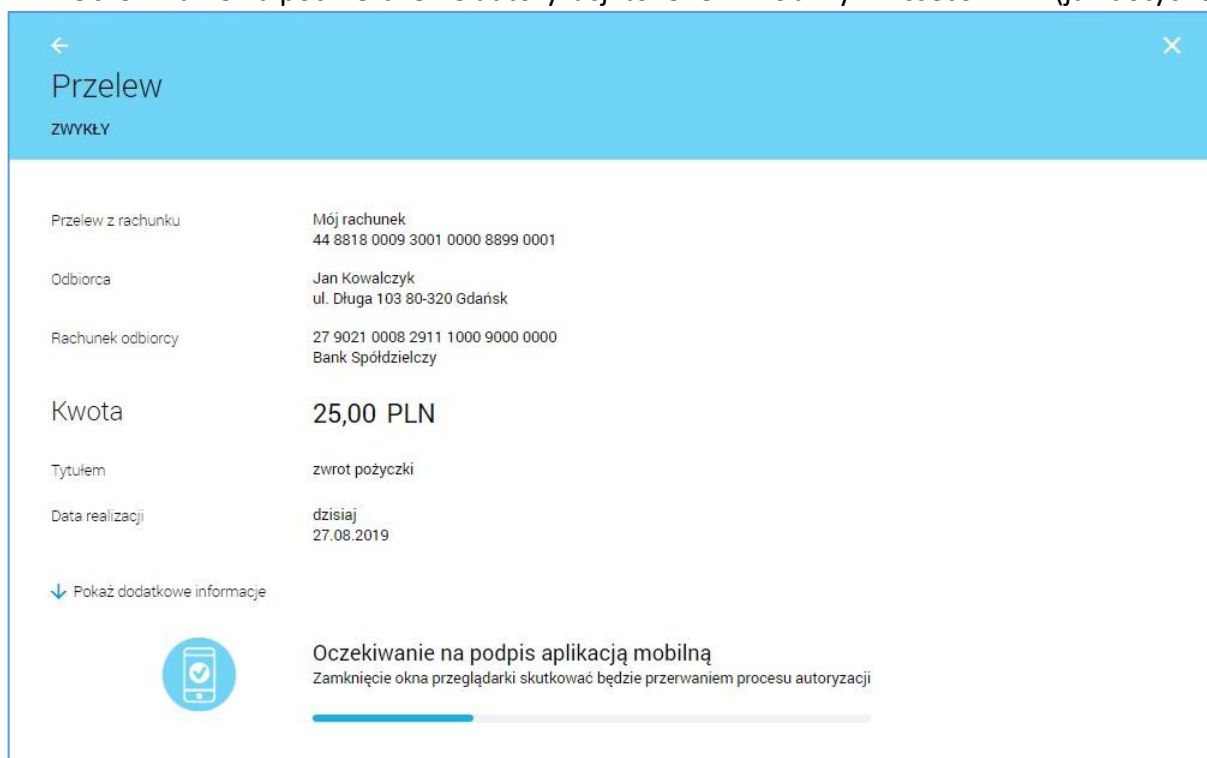
Progress bar: [-----|-----]

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):

