

ZMIANY W LOGOWANIU I AUTORYZACJI BANKOWOŚCI INTERNETOWEJ

W związku z wdrożeniem Dyrektywy Parlamentu Europejskiego i Rady (UE) nr 2015/2366 z dnia 25 listopada 2015 roku (PSD2) w sprawie usług płatniczych w ramach rynku wewnętrznego nałóżono na banki obowiązek wzmocnienia bezpieczeństwa autoryzacji transakcji. **Zmiany o których mowa dotyczą zarówno procesu autentykacji (logowania) jak i procesu autoryzacji (podpisu).** Aby podnieść standardy bezpieczeństwa banki zobligowane są stosować silne uwierzytelnienie, które wymaga co najmniej 2 niezależnych elementów niezbędnych do logowania/autoryzacji.

Wykonywanie operacji dotychczasowymi metodami nie będzie możliwe po 14 września 2019. **Zapraszamy do kontaktu z pracownikami naszego Banku w celu wprowadzenia zmian w Państwa dostępie do bankowości internetowej.** Sugerujemy jak najszybsze złożenie wniosku o zmianę sposobu autoryzacji na mToken Asseco MAA lub SMS autoryzacyjny. Nadmieniamy, że aktywacja i użytkowanie Tokena Asseco MAA są bezpłatne.

Użytkownicy tokena RSA powinni udać się do najbliższej placówki Banku w celu dokonania formalności związanych ze zmianą formy autoryzacji. Z kolei użytkownicy haseł stałych/maskowanych, kodów SMS, tokena mobilnego Asseco MAA i karty mikroprocesorowej nie muszą podejmować żadnych działań - zmiany w autoryzacji dokonają się automatycznie.

Poniżej prezentujemy tabele zawierającą zestawienie dotychczasowych oraz nowych metod autentykacji (logowania) i autoryzacji (podpisu) z podziałem na klienta indywidualnego. **Poniżej tabeli prezentujemy szczegółowe informacje dotyczące konkretnego wariantu.**

Zmiany dotyczące KLIENTA INDYWIDUALNEGO (system Asseco CBP)

Numer wariantów	Przed zmianami		Po zmianach	
	Obecna autentykacja	Obecna autoryzacja	Nowa autentykacja	Nowa autoryzacja
Wariant nr 1	Hasło maskowane	Kod SMS	Hasło maskowane + Kod SMS	Kod SMS + PIN ¹
Wariant nr 2	Hasło maskowane	Token mobilny Asseco MAA	Hasło maskowane + Token mobilny Asseco MAA + PIN ²	Token mobilny Asseco MAA + PIN ²
Wariant nr 3	Hasło stałe + Token RSA	Hasło stałe + Token RSA	Hasło maskowane + kod SMS	Kod SMS + PIN ¹
			Hasło maskowane + Token mobilny Asseco MAA + PIN ²	Token mobilny Asseco MAA + PIN ²

Legenda:

1 - kod PIN autoryzujący. Klient zostanie poproszony o utworzenie PINu autoryzującego podczas pierwszej autoryzacji zlecenia.

2 - kod PIN służący do logowania do aplikacji mToken mobilny Asseco MAA

Wariant nr 1

Wprowadzenie identyfikatora użytkownika:

LOGOWANIE PL

Numer identyfikacyjny

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

Wprowadzenie hasła maskowanego:

← LOGOWANIE

Kod dostępu

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](#)

Wprowadzenie kodu SMS:

← LOGOWANIE

Kod dostępu

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](#)

Tylko 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
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" value="Wpisz obecny PIN"/>
Nowy pin autoryzacyjny	<input type="text" value="Wpisz nowy pin"/>
Powtórz nowy pin	<input type="text" value="Powtórz nowy pin"/>

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" value="Wpisz pin"/>
<input type="text" value="Wpisz kod"/>

Operacja nr 738167 z dnia 26.08.2019

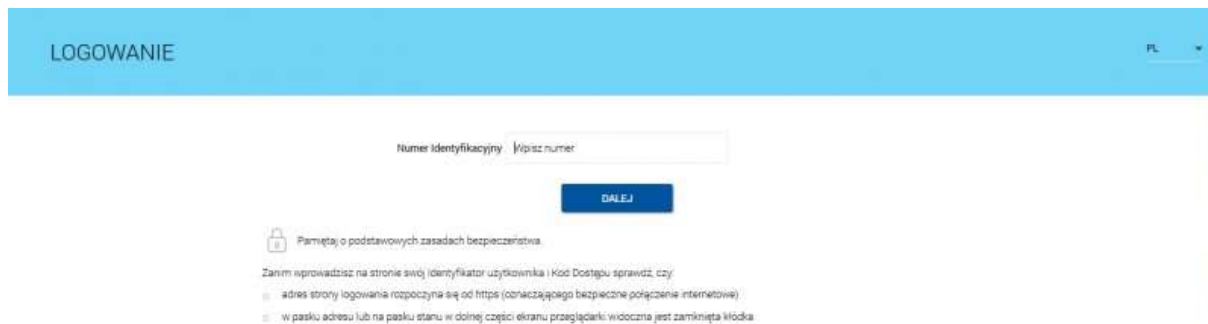
AKCEPTUJ

Wariant nr 2

Użytkownicy korzystający z hasła maskowanego i tokena mobilnego Asseco MAA nie muszą odwiedzać naszych placówek - zmiany w sposobie autoryzacji dokonają się automatycznie.

AUTENTYKACJA:


Wprowadzenie identyfikatora użytkownika:



LOGOWANIE PL

Numer identyfikacyjny

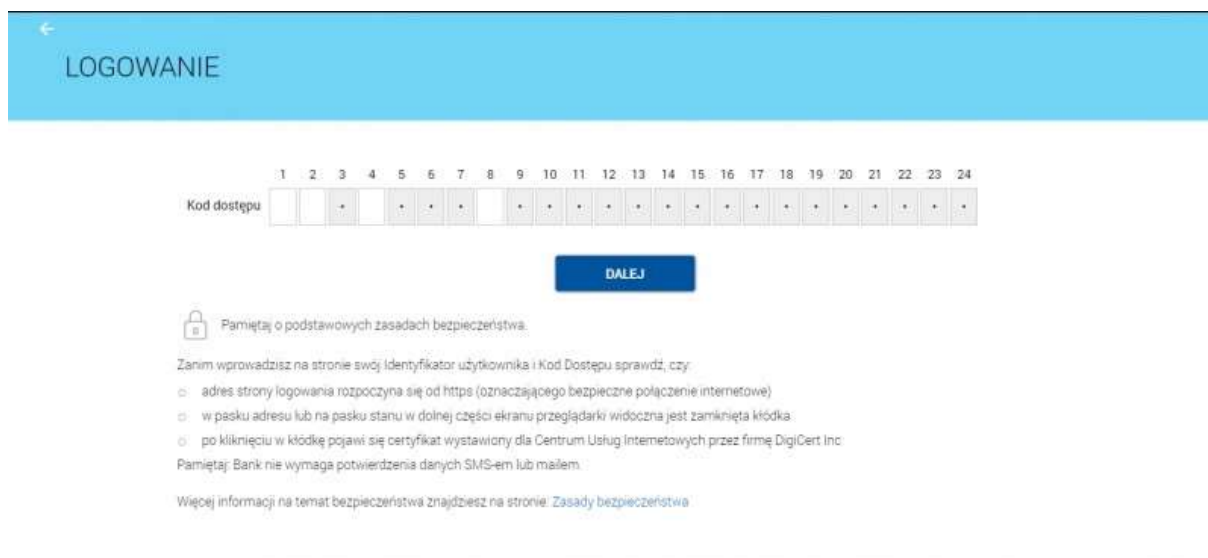
DALEJ

 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


Wprowadzenie hasła maskowanego:



LOGOWANIE

Kod dostępu

DALEJ

 Pamiętaj o podstawowych zasadach bezpieczeństwa.

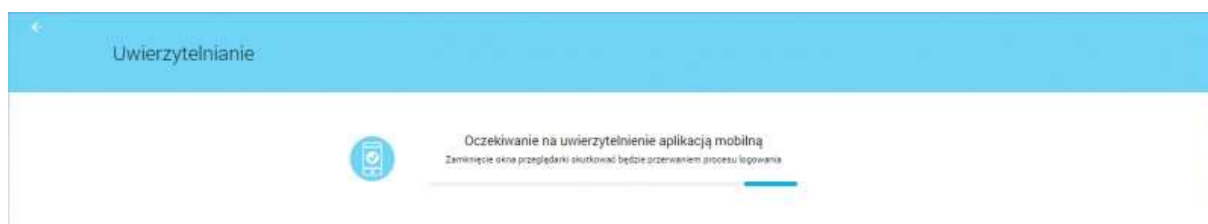
Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- 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](#)

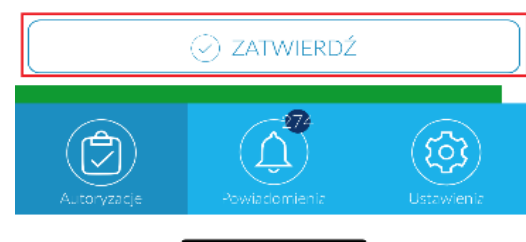
Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:



Uwierzytelnianie

 **Oczekiwanie na uwierzytelnienie aplikacją mobilną**
Zamknij okno przeglądarki skutkować będzie przerwaniem procesu logowania

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

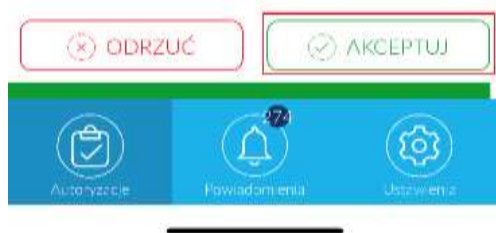


AUTORYZACJA:

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:



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



Wariant nr 3

W przypadku użytkowników tokena RSA konieczna jest wizyta w najbliższej placówce Banku w celu zmiany metody autoryzacji - WARIANT 1 lub WARIANT 2.