

Jakie zmiany w logowaniu od 14 września 2019 r

Token RSA

Do 14 września 2019 r

Obecna autentykacja	Obecna autoryzacja
Hasło stałe + token RSA	Kod SMS Hasło stałe + token RSA

Od 14 września 2019

Nowa autentykacja	Nowa autoryzacja
Hasło maskowane + kod SMS	Kod SMS + PIN
Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN

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:

- 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:

← 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

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](#)

Autoryzacja transakcji :

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 KB SA 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 tak jak dotychczas 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

lub alternatywnie

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:

- 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:

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](#)

Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:

Uwierzytelnianie

Oczekiwanie na uwierzytelnienie aplikacją mobilną

Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu logowania

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

13:11 LTE

assecO Wycieczki

AUTORYZACJA OPERACJI

Logowanie do bankowości internetowej CBP

ODRZUĆ **AKCEPTUJ**

1 2 3

Autoryzacja Powiadomienia Ustawienia

15:55 LTE

assecO Wycieczki

AUTORYZACJA OPERACJI

Podaj PIN

Wprowadź PIN

1	2	3
4	5	6
7	8	9
	0	

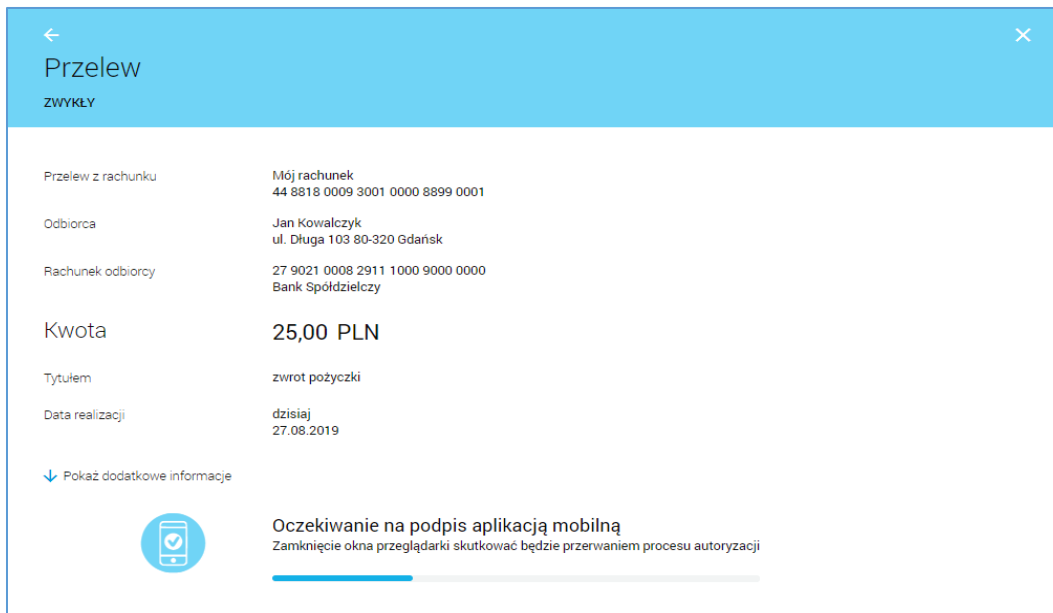
ZATWIERDŹ

1 2 3

Autoryzacja Powiadomienia Ustawienia

autoryzacja:

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:



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

