

Internet Banking

Asseco CBP – dostosowanie do wymagań SCA

Dla klientów bankowości internetowej *Internet Banking*, korzystających obecnie z metody autoryzacji **Hasło SMS** oraz aplikacji mobilnej **mToken Asseco MAA**, po uruchomieniu mechanizmów silnego uwierzytelniania klienta (SCA) – **po dniu 13 września 2019**, ulegnie zmianie schemat autentykacji (logowania) oraz autoryzacji.

Po wprowadzeniu silnego uwierzytelniania klienta w bankowości internetowej *Internet Banking* autentykacja (logowanie) oraz autoryzacja z wykorzystaniem **Tokena RSA** zostanie **zablokowana**.

Środki dostępu w *Internet Banking* będą dostosowane do SCA zgodnie z poniższymi schematami:

Metoda autoryzacji	Obecnie		Po wprowadzeniu SCA	
	autentykacja	autoryzacja	NOWA AUTENTYKACJA	NOWA AUTORYZACJA
Hasło SMS	Hasło maskowane	Kod SMS	Hasło maskowane + kod SMS	Kod SMS + PIN
mToken Asseco MAA	Hasło maskowane	Token mobilny Asseco MAA	Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN

Opis szczegółowy schematów autentykacji oraz autoryzacji po dostosowaniu do SCA środków dostępu do IB – wygląd formatek dla użytkownika (kolorystyka może być inna) został przedstawiony na kolejnych stronach.

1. Hasło SMS


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


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](#)

AUTORYZACJA

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

2. mToken Asseco MAA


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

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="text"/>	<input type="text"/>	<input type="text" value="•"/>	<input type="text"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>	<input type="text" value="•"/>

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](#)

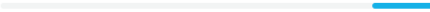
Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:

← Uwierzytelnianie

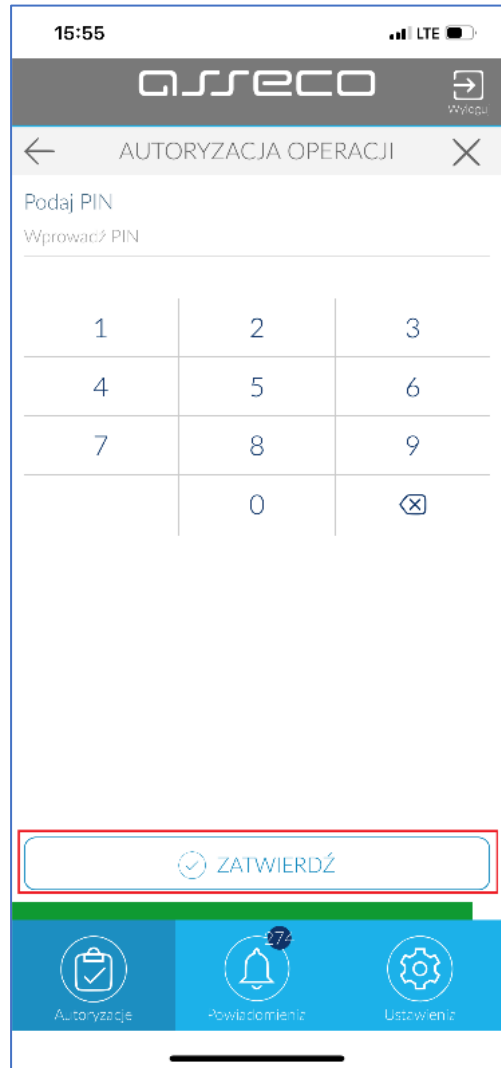


Oczekiwanie na uwierzytelnienie aplikacją mobilną

Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu logowania



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



AUTORYZACJA

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:

← Przelew ×

ZWYKŁY

Przelew z rachunku	Mój rachunek 44 8818 0009 3001 0000 8899 0001
Odbiorca	Jan Kowalczyk ul. Długa 103 80-320 Gdańsk
Rachunek odbiorcy	27 9021 0008 2911 1000 9000 0000 Bank Spółdzielczy
Kwota	25,00 PLN
Tytułem	zwrot pożyczki
Data realizacji	dzisiaj 27.08.2019

↓ Pokaż dodatkowe informacje



Oczekiwanie na podpis aplikacją mobilną
Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu autoryzacji

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

