

Zmiany w bankowości CBP (ebank.bsszczytno.pl)

1. Wstęp – dostosowanie środków dostępu użytkowanych w CUI do wymogów silnego uwierzytelniania (SCA)

Obecnie stosowane środki dostępu do systemów bankowości elektronicznej zostaną uzupełnione o dodatkowe wymagania SCA (tzw.: „silne uwierzytelnienie klienta”). „Silne uwierzytelnianie klienta” oznacza 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 SCA dotyczy procesu autentykacji (logowania) oraz autoryzacji (podpisu).

Planowanie termin wprowadzenia zmian to 11.09.2019 r, lecz nie później niż 14.09.2019r.

2. CBP – dostosowanie do wymagań SCA

Środki dostępu w bankowości detalicznej będą dostosowane do SCA zgodnie ze schematami przedstawionymi w poniższej tabeli:

Nr schematu „autentykacja - autoryzacja”	Przed wprowadzeniem SCA		Po wprowadzeniu SCA	
	Obecna autentykacja	Obecna autoryzacja	Nowa autentykacja	Nowa autoryzacja
1	Hasło maskowane	Kod SMS	Hasło maskowane + kod SMS	Kod SMS + PIN
2	Hasło maskowane	Token mobilny Asseco MAA	Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN

2.1. Opis szczegółowy – Hasło maskowane, Kod SMS

Wygląd formatek dla użytkownika po wprowadzeniu SCA

i) **Autentykacja (logowanie):**

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](#)

ii) Autoryzacja (podpisywanie):

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="Wstaw 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

Operacja nr 738167 z dnia 26.08.2019

AKCEPTUJ

2.2. Opis szczegółowy - Hasło maskowane, mToken

Wygląd formatek dla użytkownika po wprowadzeniu SCA

i) **Autentykacja (logowanie):**

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

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](#)

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

ASSECO

← AUTORYZACJA OPERACJI

Logowanie do bankowości internetowej CBP

ODRZUĆ AKCEPTUJ

15:55

ASSECO

← AUTORYZACJA OPERACJI

Podaj PIN

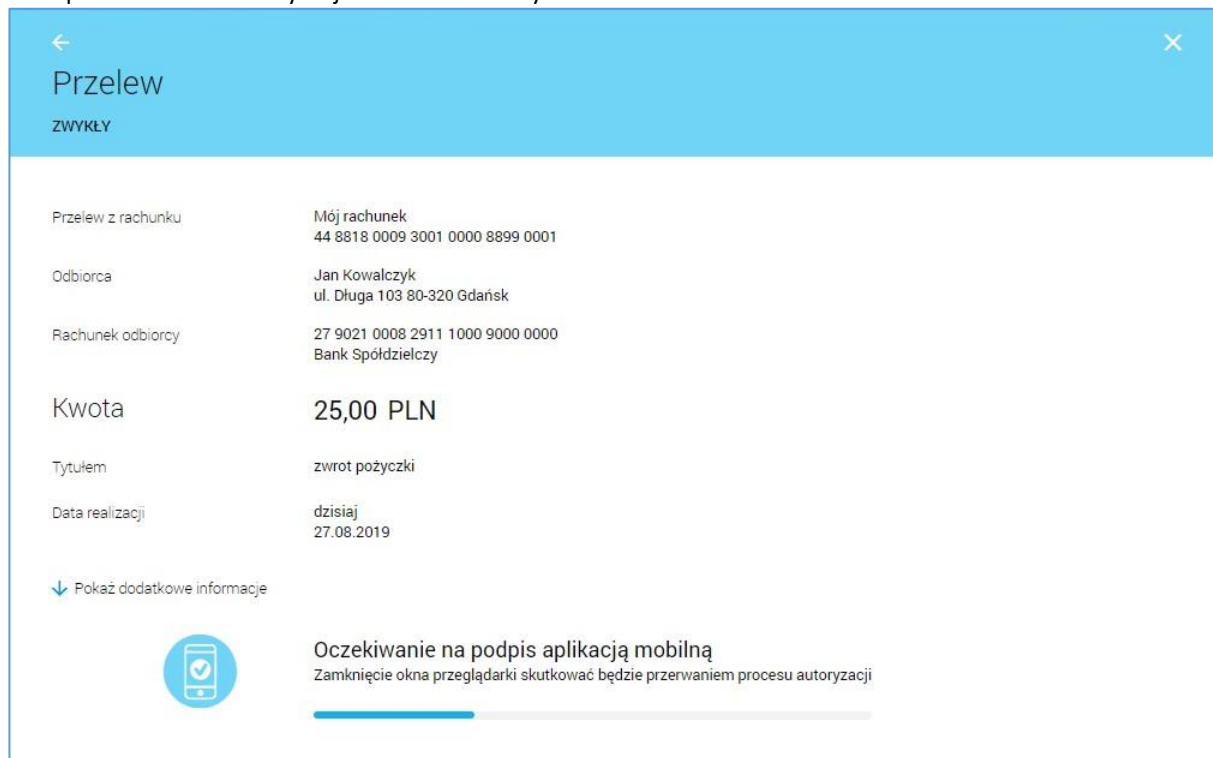
Wprowadź PIN

1	2	3
4	5	6
7	8	9
	0	⊗

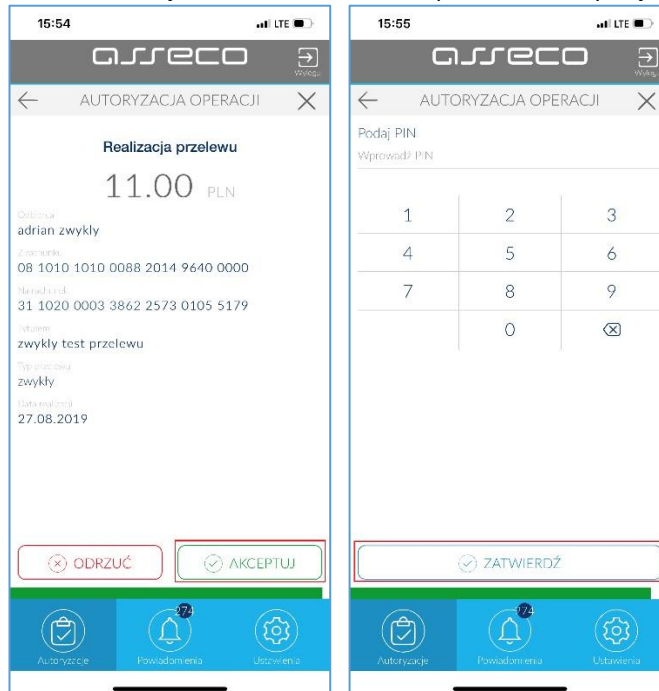
ZATWIERDŹ

ii) **Autoryzacja (podpisywanie):**

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:



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



Pozostałe funkcjonalności bankowości nie ulegają zmianom.