



**Bank Spółdzielczy**  
w Radzynie Podlaskim

**Dostosowanie  
środków dostępu użytkowanych  
w systemach bankowości elektronicznej  
Asseco CBP oraz def3000/CEB do  
wymagań SCA (silne uwierzytelnianie).**



## Spis treści:

<b>Spis treści:</b> .....	2
<b>1. Wstęp – dostosowanie środków dostępu użytkowanych w CUI do wymogów silnego uwierzytelniania (SCA)</b> .....	3
<b>2. Asseco CBP – dostosowanie do wymagań SCA</b> .....	4
<b>3. def3000/CEB – dostosowanie do wymagań SCA</b> .....	15

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

Obecnie stosowane środki dostępu do systemów bankowości elektronicznej zostały 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).

W/w zasada (SCA) determinuje zmiany w obecnie użytkowanych schematach środków dostępu, tj.:

- a) Bankowość detaliczna – Asseco CBP
  - autentykacja: hasło maskowane, autoryzacja: kod SMS
  - autentykacja: hasło maskowane, autoryzacja: token mobilny Asseco MAA
  - autentykacja: hasło stałe + token RSA, autoryzacja: hasło stałe + token RSA
  - autentykacja: hasło maskowane, autoryzacja: token RSA
  
- b) Bankowość korporacyjna – def3000/CEB
  - autentykacja: hasło stałe, autoryzacja: karta mikroprocesorowa
  - autentykacja: hasło stałe + token RSA, autoryzacja: karta mikroprocesorowa

## 2. Asseco CBP – dostosowanie do wymagań SCA

Środki dostępu w bankowości detalicznej będą dostosowane do SCA zgodnie ze schematami przedstawionymi w tabeli 1:

Tabela 1		Przed wprowadzeniem SCA		Po wprowadzeniu SCA	
Nr schematu „autentykacja - autoryzacja”	Obecna autentykacja	Obecna autoryzacja	Nowa autentykacja	Nowa autoryzacja	
1	Hasło maskowane	Kod SMS	Hasło maskowane + kod SMS	Kod SMS + PIN <sup>1</sup>	
2	Hasło maskowane	Token mobilny Asseco MAA	Hasło maskowane + token mobilny Asseco MAA + PIN <sup>2</sup>	Token mobilny Asseco MAA + PIN <sup>2</sup>	
3	Hasło stałe + token RSA	Hasło stałe + token RSA	Hasło maskowane + kod SMS	Kod SMS + PIN <sup>1</sup>	
			Hasło maskowane + token mobilny Asseco MAA + PIN <sup>2</sup>	Token mobilny Asseco MAA + PIN <sup>2</sup>	
4	Hasło maskowane	Hasło stałe + token RSA	Hasło maskowane + kod SMS	Kod SMS + PIN <sup>1</sup>	
			Hasło maskowane + token mobilny Asseco MAA + PIN <sup>2</sup>	Token mobilny Asseco MAA + PIN <sup>2</sup>	

Legenda:

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

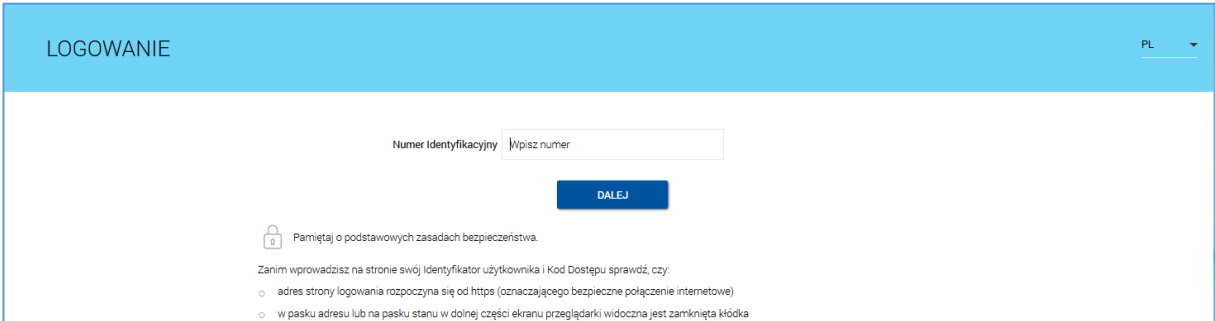
<sup>2</sup> - kod PIN służący do logowania do aplikacji mToken mobilny Asseco MAA

### 2.1. Opis szczegółowy – schemat nr 1 (dostosowanie do SCA środka dostępu – autentykacja: Hasło maskowane, autoryzacja: Kod SMS)

Wygląd formatek dla użytkownika po wprowadzeniu SCA

#### i) autentykacja:

Wprowadzenie identyfikatora użytkownika:



Wprowadzenie tymczasowego hasła, który klient otrzymał w wiadomości SMS:

← 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](#)

### Zatwierdzenie tymczasowego hasła kodem 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](#)

### Ustalenie nowego hasła:

← Nowe hasło dostępu

Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator użytkownika

Nowe hasło dostępu

Powtórz nowe hasło

**ZAPISZ I ZALOGUJ**

Definiując swoje nowe hasło dostępu pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

- o musi składać się z 4-8 znaków
- o musi zawierać przynajmniej jeden znak specjalny
- o musi zawierać przynajmniej jedną wielką literę
- o musi zawierać przynajmniej jedną małą literę
- o musi zawierać przynajmniej jedną cyfrę
- o dozwolone znaki: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ@#%&\*()\_+=!@!";<.>/?

### Ponowne logowanie do aplikacji z użyciem nowego hasła:

← 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](#)

### Wprowadzenie kodu SMS:

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](#)

ii) **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
<b>Kwota</b>	<b>1,43 PLN</b>
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="Wprowadź obecny pin"/>
Nowy pin autoryzacyjny	<input type="text" value="Wprowadź 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
<b>Kwota</b>	<b>1,00 PLN</b>
Tytułem	TYTUŁ PŁATNOŚCI
Data realizacji	dzisiaj 26.08.2019

↓ Pokaż dodatkowe informacje

Pin autoryzacyjny oraz kod SMS

Wpisz pin

Wpisz kod

Operacja nr 738167 z dnia 26.08.2019

**AKCEPTUJ**

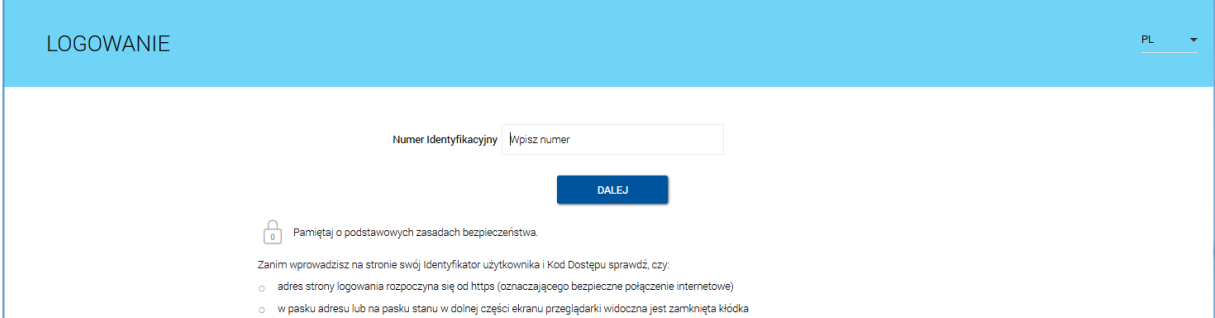


2.2. Opis szczegółowy - schemat nr 2 (dostosowanie do SCA środka dostępu – autentykacja: Hasło maskowane, autoryzacja: Token mobilny Asseco MAA)

Wygląd formatek dla użytkownika

**i) autentykacja:**


Wprowadzenie identyfikatora użytkownika:



LOGOWANIE PL ▾

Numer Identyfikacyjny

**DALEJ**

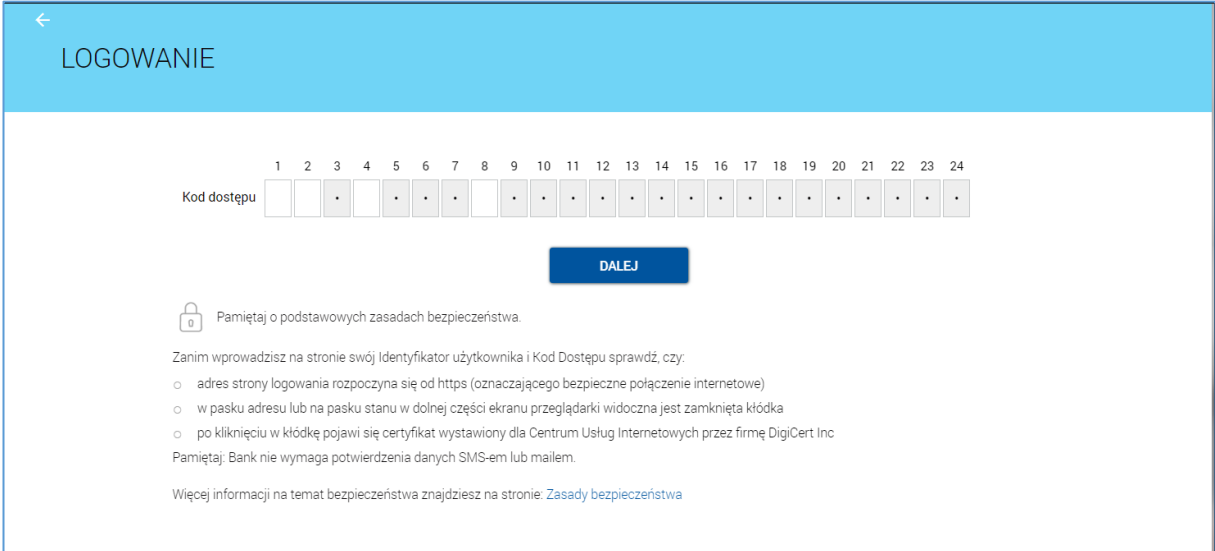
 Pamiętaj o podstawowych zasadach bezpieczeństwa.

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:


**UWAGA! W przypadku pierwszego logowania, dla klienta, system w pierwszym kroku poprosi o podanie hasła startowego. Wówczas system najpierw poprosi o ustalenie nowego hasła a po ustaleniu nowego hasła, aplikacja wymusi ponowne logowanie już z nowym hasłem.**



← LOGOWANIE

Kod dostępu

**DALEJ**

 Pamiętaj o podstawowych zasadach bezpieczeństwa.

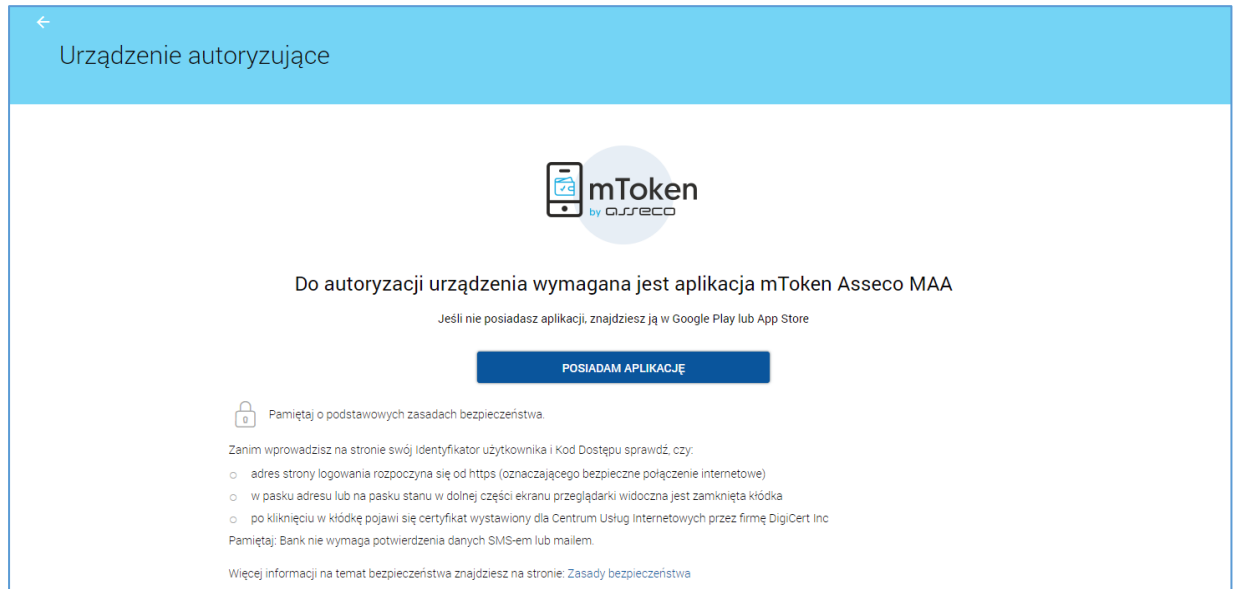
Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- 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

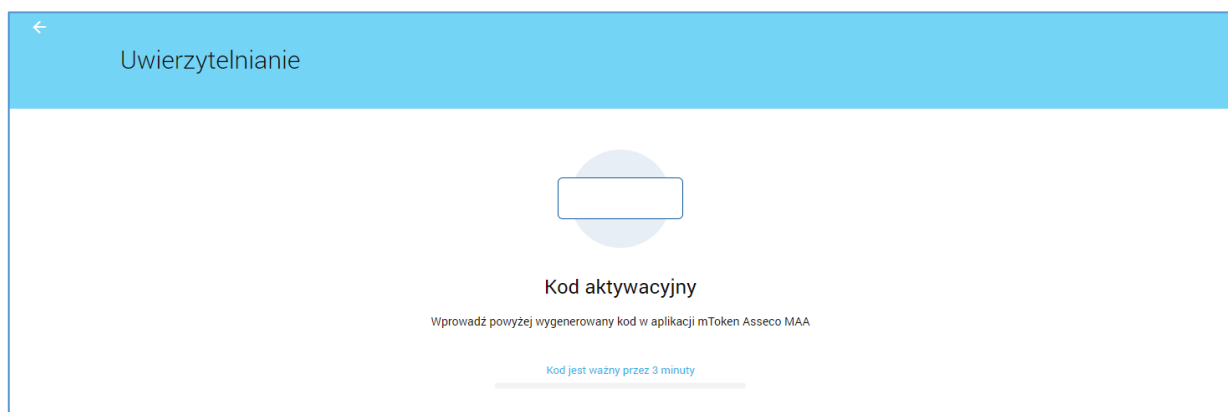
Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

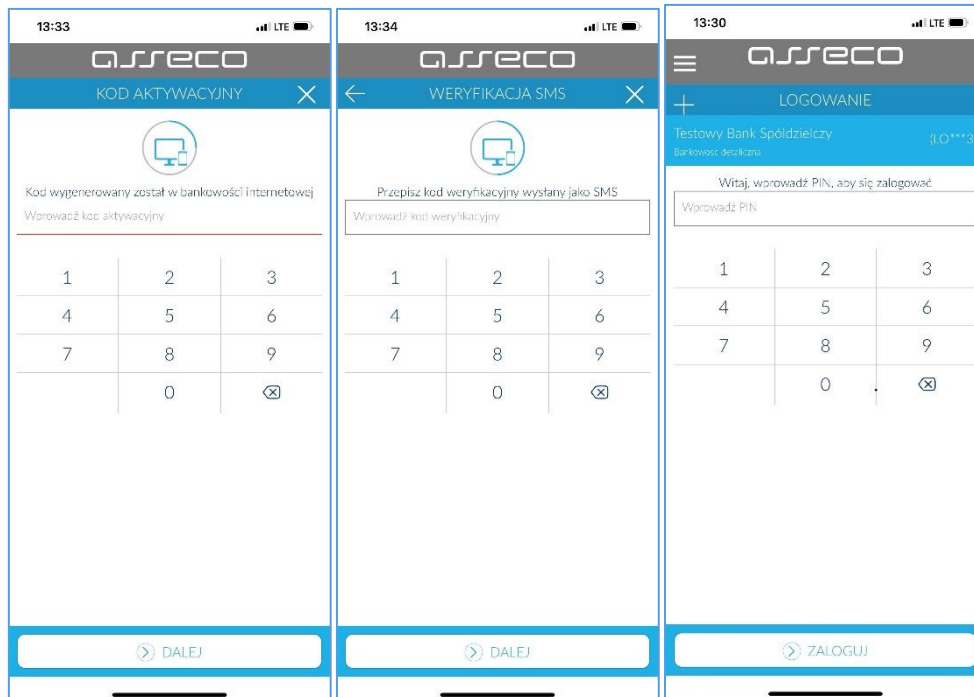
W przypadku braku sparowanego urządzenia, aplikacja wyświetli komunikat o sparowaniu urządzenia.



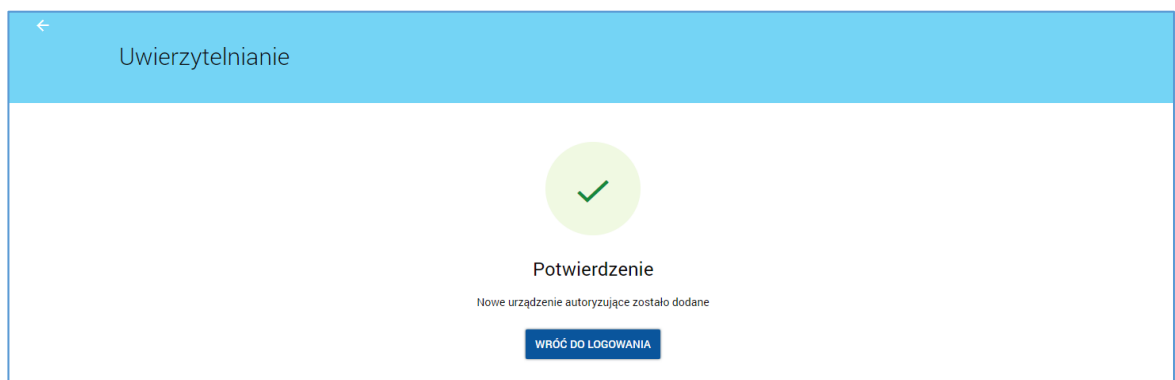
Po tym komunikacie, klient powinien pobrać aplikację na urządzenie mobilne. Po pobraniu aplikacji na urządzenie mobilne, w aplikacji internetowej Asseco CBP należy wybrać opcję „Posiadam aplikację”, gdzie wyświetla się kod aktywacyjny.



Na urządzeniu mobilnym klient, dodaje nowe urządzenie poprzez znak „+” i wprowadza kod, który wyświetli się w aplikacji internetowej (Kod w aplikacji Asseco CBP pokaże się po wejściu w opcję „Posiadam aplikację” (patrz zrzut powyżej)). W kolejnym kroku należy podać kod SMS, który zostanie przesłany na wskazany w Bank Admin numer telefonu i ustawić pin do aplikacji



Po wykonaniu w/w czynności, w aplikacji pojawi się komunikat o poprawnym sparowaniu. I system poprosi o ponowne zalogowanie do bankowości.




Wówczas ponownie należy wykonać akcję logowania: 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
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**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

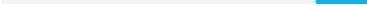
Pamiętaj! Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

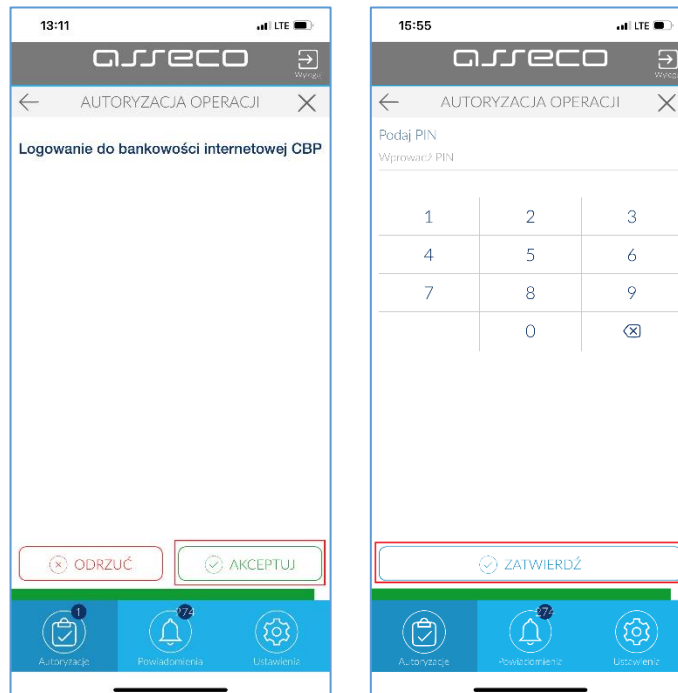
### Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:

← Uwierzytelnianie

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

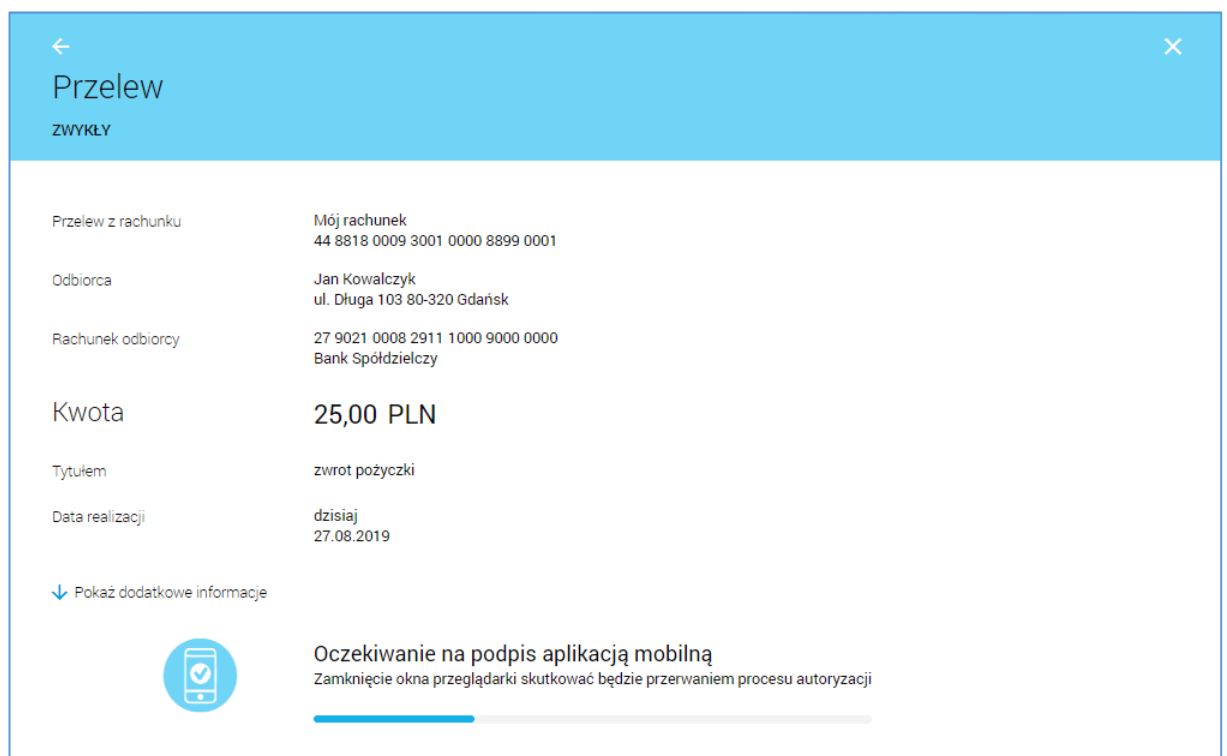


Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem logowania do systemu:

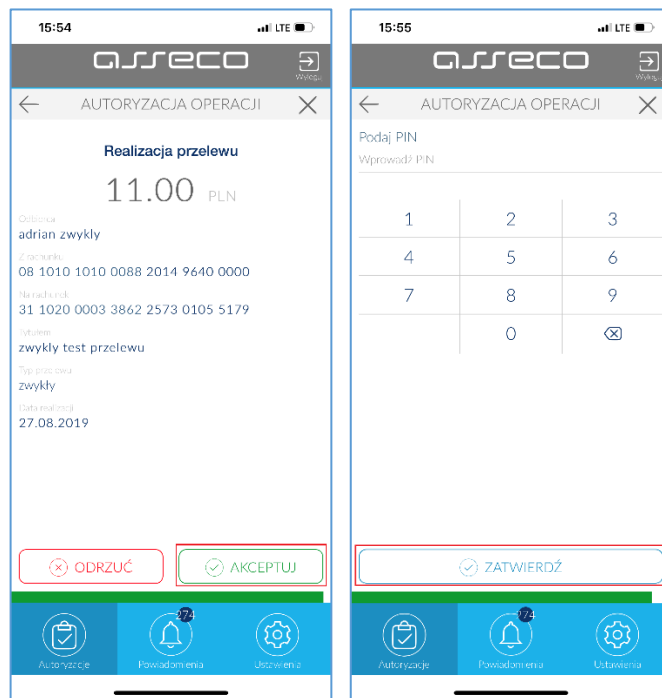


**ii) autoryzacja:**

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:



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



### 3. def3000/CEB – dostosowanie do wymagań SCA

Środki dostępu w bankowości korporacyjnej będą dostosowane do SCA zgodnie ze schematami przedstawionymi w tabeli 2:

Tabela 2	Przed wprowadzeniem SCA		Po wprowadzeniu SCA	
Nr schematu „autentykacja - autoryzacja”	Obecna autentykacja	Obecna autoryzacja	Nowa autentykacja	Nowa autoryzacja
1	Hasło stałe	Karta mikroprocesorowa (aplet java) + PIN	Karta mikroprocesorowa (aplet java) + PIN <sup>1</sup>	Karta mikroprocesorowa (aplet java) + PIN <sup>1</sup>
2	Hasło stałe + token RSA	Karta mikroprocesorowa (aplet java) + PIN	Hasło stałe + token RSA	Karta mikroprocesorowa (aplet java) + PIN <sup>1</sup>

Legenda:

- <sup>1</sup> - PIN do karty mikroprocesorowej
- <sup>2</sup> - PIN służący do uruchomienia tokena VASCO
- <sup>3</sup> - PIN do karty mikroprocesorowej wpisywany w aplikacji SCSA
- <sup>4</sup> - PIN służący do uruchomienia aplikacji mToken Asseco MAA

#### 3.1. Opis szczegółowy schemat nr 1 (dostosowanie do SCA środka dostępu – autentykacja: Hasło stałe, autoryzacja: Karta mikroprocesorowa (aplet java) + PIN)

- a) Zmiana sposobu logowania (z hasła stałego na autentykację kartą mikroprocesorową) zostanie wprowadzona dla wszystkich użytkowników w jednym terminie przez Asseco Poland S.A.

**UWAGA:**

W celu dostosowania systemu do wymogów SCA konieczne jest wyłączenia logowania samym hasłem stałym. Zatem po dniu 2019-09-13 użytkownik posługujący się tą metodą autentykacji (np. użytkownik pasywny bez środka autoryzacji) straci dostęp do def3000/CEB do momentu wydania mu środka autentykacji zgodnego z SCA.

- b) Wygląd formatek dla użytkownika  
 i) **autentykacja:**

Wybór metody autentykacji – Logowanie karta mikroprocesorową:

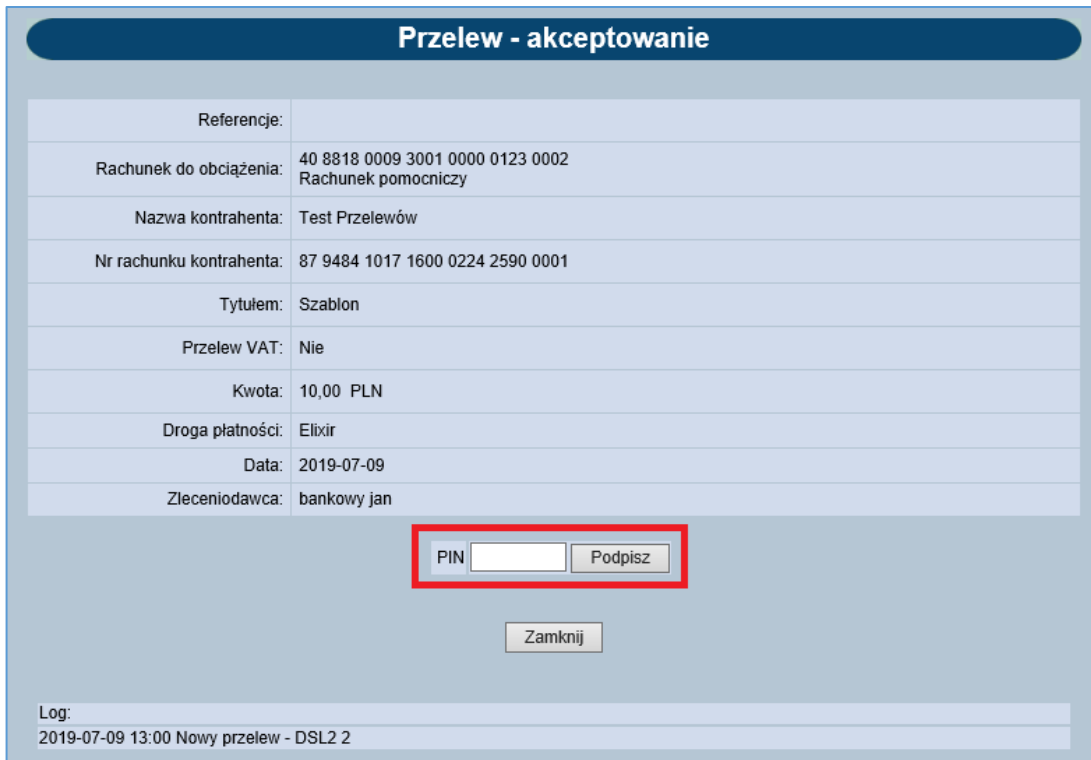


Umieszczenie karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenie numeru PIN karty mikroprocesorowej:



**ii) autoryzacja:**

Umieszczenie karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenie numeru PIN karty mikroprocesorowej:



3.2. Opis szczegółowy – schemat nr 2 (dostosowanie do SCA środka dostępu – autentykacja: Hasło stałe + token RSA, autoryzacja: Karta mikroprocesorowa (aplet java) +PIN)

- a) Rekonfiguracja użytkowników nie jest wymagana.
- b) Wygląd formatek dla użytkownika pozostaje bez zmian.