



**Bank Spółdzielczy w Szczytnie**

Grupa BPS

rok zał. 1910

## **Dokumentacja użytkownika systemu EBP**

## Spis treści

Rozdział 1. Konwencje typograficzne .....	1
Rozdział 2. Wstęp .....	3
Rozdział 3. Wprowadzenie .....	4
Rozdział 4. Korzystanie z przeglądarek internetowych pod kątem pracy w systemie EBP .....	5
Rozdział 5. Tryby dostępu do systemu .....	6
Rozdział 6. Logowanie do systemu .....	7
6.1. Kontrola usługi filtrowania IP w procesie logowania użytkownika .....	8
6.2. Logowanie do systemu za pomocą aplikacji mobilnej MToken MAA .....	8
6.2.1. Pierwsze logowanie wraz z rejestracją urządzenia .....	9
6.2.1.1. Proces parowania urządzenia podczas pierwszego logowania w aplikacji MAA .....	13
6.2.2. Logowanie po rejestracji urządzenia .....	17
6.3. Logowanie do systemu EBP przy pomocy karty mikroprocesorowej .....	23
6.3.1. Pierwsze logowanie do systemu EBP za pomocą karty mikroprocesorowej wraz z rejestracją urządzenia .....	24
6.3.2. Kolejne logowanie do systemu EBP przy pomocy karty mikroprocesorowej .....	26
6.4. Logowanie do systemu EBP przy pomocy hasła maskowanego + kodu SMS .....	26
6.4.1. Pierwsze logowanie do systemu EBP przy pomocy hasła maskowanego + kodu SMS .....	26
6.4.2. Kolejne logowanie do systemu EBP przy pomocy hasła maskowanego + kodu SMS (bez dodania urządzenia do zaufanych) .....	31
6.4.3. Kolejne logowanie do systemu EBP przy pomocy hasła maskowanego + kodu SMS (po dodaniu urządzenia do zaufanych) .....	33
Rozdział 7. Metody autoryzacji zleceń .....	35
7.1. Mobilny podpis .....	35
7.2. Karta mikroprocesorowa .....	35
7.3. Kod PIN + kod SMS .....	39
Rozdział 8. Wybór kontekstu przez użytkownika w systemie EBP .....	42
Rozdział 9. Pulpit .....	44
9.1. Edycja wyglądu pulpitu .....	48
9.2. Samouczek systemu EBP .....	50
9.3. Widok Moje miniaplikacje .....	53
Rozdział 10. Zarządzanie ustawieniami .....	56
10.1. Zmiana hasła dostępu do systemu .....	58
10.2. Dane osobowe/Dane firmy .....	62
10.3. Ustawienia importu i eksportu .....	63
10.3.1. Import opisu struktury .....	65
10.4. Kanały dostępu do systemu .....	67
10.4.1. Zablokowanie kanału Internet (WWW) dla systemu .....	68
10.5. Zmiana limitów dla kanału Internet (WWW) .....	69
10.6. Kanały dostępu i limity do rachunków .....	70
10.6.1. Zablokowanie kanału Internet (WWW) dla rachunku .....	71

10.6.2. Odblokowanie kanału Internet (WWW) dla rachunku .....	72
10.6.3. Zmiana limitów dla kanału Internet (WWW).....	73
10.7. Kanały dostępu i limity dla upoważnionych do rachunków .....	75
10.7.1. Zablokowanie kanału Internet (WWW) dla rachunku .....	77
10.7.2. Odblokowanie kanału Internet (WWW) dla rachunku .....	78
10.7.3. Zmiana limitów dla kanału Internet (WWW).....	79
10.8. Rejestr zdarzeń .....	80
10.9. Rachunek domyślny.....	85
10.10. Uprawnienia użytkowników .....	86
10.10.1. Uprawnienia funkcjonalne .....	87
10.10.1.1. Uprawnienia dla Rachunków .....	88
10.10.1.2. Uprawnienia dla Przelewów .....	88
10.10.1.3. Uprawnienia dla Paczek.....	89
10.10.1.4. Uprawnienia dla Szablonów .....	90
10.10.1.5. Uprawnienia dla Lokat .....	90
10.10.1.6. Uprawnienia dla Wiadomości .....	90
10.10.1.7. Uprawnienia dla Ustawień.....	91
10.10.1.8. Uprawnienia dla Kredytów .....	91
10.10.1.9. Uprawnienia dla Doładowań .....	91
10.10.1.10. Uprawnienia dla Kart .....	92
10.10.1.11. Uprawnienia dla Płatności masowych .....	92
10.10.2. Uprawnienia do rachunków .....	92
10.11. Filtrowanie adresów IP .....	94
10.11.1. Edycja konfiguracji adresów IP .....	97
10.11.2. Usunięcie konfiguracji adresów IP.....	99
10.11.3. Włączenie funkcjonalności kontroli adresów IP na poziomie globalnym.....	99
10.11.4. Zarządzaj konfiguracją dostępu.....	101
10.11.5. Nowa konfiguracja.....	103
10.12. Historia logowań.....	106
10.13. Konfiguracja powiadomień.....	108
10.13.1. Konfiguracja powiadomień dla rachunków .....	112
10.13.2. Konfiguracja powiadomień dla lokat .....	114
10.13.3. Konfiguracja powiadomień dla logowania .....	114
10.13.4. Konfiguracja powiadomień dla przelewów .....	115
10.14. Zmiana hasła telefonicznego .....	117
Rozdział 11. Zakończenie pracy z systemem .....	120




## Informacje o dokumencie


Niniejszy dokument jest dokumentacją użytkownika systemu EBP w wersji 4.09.000C.

## Rozdział 1. Konwencje typograficzne

W dokumentacji stosowane są następujące konwencje typograficzne:

Konwencja typograficzna lub znak wizualny	Opis
Standardowy	Podstawowy tekst dokumentacji
Tabela	Tekst w tabeli
<b>Nowe pojęcie</b>	Nowe pojęcia. Wyróżnienie ważnych fragmentów tekstu.
<i>Kursywa</i>	Pozycje na listach wartości. Komunikaty systemowe. Parametry lub zmienne, których rzeczywiste nazwy lub wartości mają być dostarczane przez użytkownika. Nazwy opcji systemu. Ścieżki, np. <i>Dane archiwalne</i> → <i>Przeglądanie</i> .
<b>Uwaga</b>	<p>Tekst uwagi, komentarza, zastrzeżenia - informacje, na które należy zwrócić uwagę podczas czytania dokumentacji lub pracy z systemem np.</p> <div style="border-left: 1px solid black; padding-left: 10px;"><p>Podany powyżej adres internetowy jest przykładowy. Informację o adresie strony usług internetowych udostępnia Bank.</p></div>

[Wpisz tutaj]

<b>Ostrzeżenie</b>	<p>Tekst ostrzeżenia - ostrzeżenia zawierają bardzo ważne informacje, na które należy zwrócić szczególną uwagę podczas czytania dokumentacji lub pracy z systemem, np.</p> <div style="display: flex; align-items: center;"><div style="margin-left: 10px;"><p>Zmiany przebiegowań nie są kontrolowane przez system i wykonywane są wyłącznie na własną odpowiedzialność operatora!</p></div></div>
<b>Link</b>	Odwołania do innych rozdziałów lub fragmentów tekstu. Adresy URL
<b>Kod źródłowy</b>	<p>Fragmenty kodu źródłowego. Przykłady wydruków</p> <pre style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;">{   "a": "b" }</pre>

Konwencja typograficzna lub znak wizualny	Opis
CAPS LOCK	Wyróżnienie nagłówków akapitów. Nazwy klawiszy na klawiaturze kombinacje klawiszy, które należy nacisnąć jednocześnie zawierają znak "+" pomiędzy, np. CTRL+F.
[ ]	Nazwy przycisków, np. [Czynności]

## Rozdział 2. Wstęp

System bankowości elektronicznej EBP zapewnia wysokiej jakości obsługę transakcyjną oraz rozwiązania z zakresu cash management i finansowania.

## Rozdział 3. Wprowadzenie

EBP (Enterprise Banking Platform) jest unikalnym rozwiązaniem bankowości internetowej i mobilnej opartym na najnowszej generacji Platformie internetowego dostępu użytkownika do produktów i usług biznesowych.

Dzięki zastosowaniu innowacyjnej koncepcji ekosystemu miniaplikacji, rozwiązanie to pozwala na osiągnięcie przewagi konkurencyjnej poprzez swobodne kształtowanie usług oferowanych użytkownikowi na Platformie zdalnego dostępu.

Rozwiązanie EBP wyróżnia innowacyjna koncepcja udostępniania funkcjonalności systemu dla klientów instytucji poprzez komponenty zwane miniaplikacjami. Miniaplikacje wraz z Platformą stanowią środowisko ich działania, tworzą swoisty ekosystem, w którym komunikacja odbywa się za pomocą ujednoczonego protokołu.

Otwartość architektury rozwiązania pozwala na opracowywanie nieograniczonej liczby miniaplikacji, o dowolnej skali złożoności bez konieczności dostosowywania aplikacji do pracy na różnych urządzeniach.

System EBP automatycznie dostosowuje swój wygląd i funkcjonalność do urządzenia, z którego użytkownik korzysta w danym momencie (jedno spójne rozwiązanie dla bankowości internetowej i mobilnej).

Rozwiązanie EBP pozwala na swobodne dopasowanie funkcjonalności do indywidualnych potrzeb i oczekiwań użytkownika.

**Platforma** to uniwersalna platforma dostępu internetowego do usług biznesowych. Stanowi środowisko działania miniaplikacji, a tym samym bazę do stworzenia systemu udostępnionego użytkownikom, poprzez dodawane miniaplikacje.

**Miniaplikacja** jest programowym modułem funkcjonalnym, osadzonym na Platformie, udostępniającym odbiorcom usługi świadczone przez instytucję, funkcjonalność biznesową np. Płatności.

Miniaplikacja integruje funkcjonalność tego samego obszaru funkcjonalnego np. Płatności i korzysta ze specyfikacji usług dostępnych na Platformie.



## Rozdział 4. Korzystanie z przeglądarek internetowych pod kątem pracy w systemie EBP

Z uwagi na kompatybilność systemu EBP z przeglądarkami mobilnymi zapewniona jest zgodność interfejsu użytkownika systemu z niżej wymienionymi wersjami bazowymi przeglądarek oraz wyższymi:

- Chrome 50.x
- Firefox 46.0
- Edge
- Safari (iOS 9.x)

Nie jest wymagana dodatkowa konfiguracja przeglądarki i praca odbywa się w trybie domyślnym. W kwestiach bezpieczeństwa i korzystania z bankowości internetowej, sugerowane jest przeglądanie w trybie incognito danej przeglądarki.

## Rozdział 5. Tryby dostępu do systemu

Użytkownik systemu EBP ma możliwość zalogowania się do systemu w następujących trybach:

- logowanie z dostępem do pełnej funkcjonalności systemu,
- logowanie po przekierowaniu z systemu zewnętrznego PayByNet - częściowy dostęp do funkcjonalności systemu, po poprawnym uwierzytelnieniu użytkownik przenoszony jest na formularz nowej płatności.

## Rozdział 6. Logowanie do systemu

W zależności od rodzaju wydanych użytkownikowi środków dostępu logowanie może przebiegać z wykorzystaniem:

- mobilnego podpisu,
- karty mikroprocesorowej,
- hasła maskowanego + kodu SMS.

Na pierwszej stronie logowania użytkownik ma możliwość zmiany języka systemu po wybraniu przycisku znajdującego się w lewej dolnej części formularza.



Strona logowania wyświetlana jest w następujących sytuacjach:

- w wyniku przejścia na adres serwisu (domyślny język strony - przekazany w parametrze wywołania lub polski, jeśli nie przekazano podczas wywołania),
- wskutek niepowodzenia procesu logowania do systemu,
- wskutek wylogowania z powodu wygaśnięcia sesji użytkownika w systemie (językiem strony logowania jest wówczas język użytkownika używany w systemie),
- w wyniku ponownego przejścia na stronę logowania (przyciskiem [ZALOGUJ PONOWNIE]) ze strony wylogowania (językiem strony jest język ze strony wylogowania).

Zachowanie strony logowania jest zgodne z paradygmatem Responsive Web Design, tj. w zależności od urządzenia, na którym otwarta została strona do logowania, wyświetlane są odpowiednie rozmiarowo pliki graficzne.

Po zalogowaniu się użytkownika do systemu EBP zostaje wyświetlany pulpit z miniaplikacjami. Dostępność miniaplikacji na pulpicie jest uzależniona od kontekstu w jakim użytkownik zalogował się do systemu EBP.

System automatycznie kończy sesję pracy użytkownika w systemie po upływie 4 minut bezczynności użytkownika. Po upływie czasu trwania sesji, wybranie dowolnej akcji w systemie powoduje zaprezentowanie strony wylogowania. W sytuacji, gdy do zakończenia sesji w systemie została 1 minuta w nagłówku systemu wyświetlany jest licznik prezentujący czas pozostały do zakończenia sesji wraz z komunikatem:



## 6.1. Kontrola usługi filtrowania IP w procesie logowania użytkownika

Funkcjonalność kontroli adresów IP dostępna jest tylko dla użytkowników logujących się do systemu EBP w kontekście firmowym oraz w kontekście indywidualnym.

W zależności od parametryzacji w opcji *Ustawienia* → *Filtrowanie adresów IP* następuje weryfikacja publicznych adresów IP, z których użytkownicy logują się w kontekście indywidualnym oraz firmowym do systemu EBP.

Włączenie funkcjonalności kontroli adresów IP może być wykonane tylko globalnie (na firmie), natomiast konfiguracja adresów IP może być wykonana zarówno globalna (na firmie) jak i indywidualna (na każdym użytkowniku uprawnionym do tej firmy).

Jeżeli w systemie EBP została wyłączona globalna kontrola adresów IP, wówczas logowanie użytkownika do systemu EBP jest dozwolone z każdego adresu IP. W przeciwnym wypadku (gdy jest włączona) to zgodnie z konfiguracją w opcji *Ustawienia* → *Filtrowanie adresów IP* następuje weryfikacja adresu IP, z jakiego użytkownik loguje się do systemu EBP.

System umożliwia wprowadzenie konfiguracji adresów IP na dwóch poziomach:

- globalnym – po zalogowaniu użytkownika do systemu EBP w kontekście firmowym,
- indywidualnym – po zalogowaniu użytkownika do systemu EBP w kontekście indywidualnym.

W przypadku gdy w opcji *Ustawienia* → *Filtrowanie adresów IP* wprowadzono globalną konfigurację adresów IP (na firmie), natomiast takiej konfiguracji nie zdefiniowano na użytkowniku, wówczas podczas logowania tego użytkownika do systemu EBP w kontekście tej firmy, system będzie weryfikował ustawienia globalne. W sytuacji gdy wprowadzono konfigurację adresów IP zarówno globalną (na firmie) i indywidualną (na użytkowniku), wówczas podczas logowania użytkownika do systemu EBP w kontekście tej firmy, system będzie weryfikował ustawienia indywidualne dla tego użytkownika z pominięciem ustawień globalnych.

Adres IP dozwolony oznacza adres IP, z którego użytkownik będzie mógł uzyskać dostęp do systemu EBP. Adres IP zabroniony oznacza adres IP, z którego nie będzie możliwości dostępu do systemu EBP przez użytkownika, dla którego taki adres został zdefiniowany.

W przypadku zablokowania dostępu do systemu EBP na podstawie adresu IP, system wyświetli komunikat informujący o braku możliwości zalogowania do systemu z powodu niepoprawnego adresu IP.


## 6.2. Logowanie do systemu za pomocą aplikacji mobilnej MToken MAA

Użytkownik ma możliwość zalogowania się do systemu EBP za pomocą aplikacji mobilnej MToken MAA pobranej ze sklepu - Google Play (Android), App Store (iOS) i zainstalowanej na urządzeniu mobilnym.

## 6.2.1. Pierwsze logowanie wraz z rejestracją urządzenia

Proces pierwszego logowania za pomocą aplikacji MToken MAA do EBP w przypadku gdy użytkownik nie posiada aktywnego sparowanego urządzenia autoryzującego przebiega w następujący sposób:

- użytkownik wprowadza numer identyfikacyjny oraz otrzymane za pomocą sms hasło tymczasowe,




### Logowanie

Zaloguj się do bankowości internetowej

Numer Identyfikacyjny

**DALEJ**

PL 

**ZASADY BEZPIECZEŃSTWA**  
BEZPIECZNE ZAKUPY W INTERNECIE

#### Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Numer Identyfikacyjny 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 Symantec

**Pamiętaj!**  
Bank nie wymaga potwierdzenia danych SMS-om lub mailem ani też instalacji jakichkolwiek aplikacji na komputerach użytkowników.

W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z naszym Bankiem



## Logowanie

Zaloguj się do bankowości internetowej

Kod dostępu

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
1	2	3	4	5	6	7
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		
8	9	10	11	12		

ZALOGUJ

COFNIJ

- użytkownik ustawia nowe hasło, zgodnie z polityką bezpieczeństwa widoczną na stronie oraz potwierdza zmianę hasła [ZAPISZ I ZALOGUJ],

## Polityka bezpieczeństwa banku wymaga zmiany hasła.

Numer Identyfikacyjny użytkownika  
LTMS4FCP

Nowe hasło

Powtórz nowe hasło

ZAPISZ I ZALOGUJ

### Zadbaj o zachowanie poufności swojego hasła.

Nie udostępniaj hasła innym osobom, na żadnych stronach internetowych, pocztą elektroniczną, wiadomością SMS lub w odpowiedzi na ządania otrzymane od pracowników banku.

Definiując swoje hasło pamiętaj o zachowaniu zasad bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

### Zasady budowy haseł są następujące:

- musi składać się z 4-8 znaków
- musi zawierać przynajmniej jedną wielką literę
- musi zawierać przynajmniej jedną małą literę
- musi zawierać przynajmniej jeden znak specjalny
- musi zawierać przynajmniej jedną cyfrę

- użytkownik wpisuje nazwę urządzenia i wybiera przycisk [ZALOGUJ],

## Urządzenie autoryzujące

Nazwa urządzenia

ZALOGUJ

COFNIJ

- system EBP generuje oraz prezentuje kod parowania urządzenia autoryzującego oraz komunikat jakie dane są wymagane do wprowadzenia przez użytkownika w aplikacji mobilnej MToken MAA w celu potwierdzenia

parowania. Po wpisaniu kodu aktywacyjnego w aplikacji MToken MAA użytkownik otrzyma SMS, w celu potwierdzenia logowania do aplikacji MToken MAA. Kroki do przejścia w aplikacji MToken MAA zostały opisane w rozdziale **Proces parowania urządzenia podczas pierwszego logowania w aplikacji MAA.**



W procesie rejestracji urządzenia autoryzującego podczas logowania użytkownika do systemu EBP mogą wystąpić następujące komunikaty informujące o błędach:

- **Błąd uwierzytelnienia.** Skontaktuj się z Administratorem, w sytuacji gdy:
  - Brak nr telefonu na kartotece klienta w systemie transakcyjnym,
  - inny błąd techniczny.
- **Błąd parowania urządzenia autoryzującego,** w sytuacji:
  - Niepowodzenia w aktywowaniu urządzenia autoryzacyjnego.
- **Przekroczono czas parowania urządzenia autoryzującego,** w sytuacji gdy:
  - upłynął czas na zakończenie procesu dodawania urządzenia.



### 6.2.1.1. Proces parowania urządzenia podczas pierwszego logowania w aplikacji MAA

Proces parowania urządzenia podczas pierwszego logowania w aplikacji MAA odbywa się w następujący sposób:

- użytkownik otwiera zainstalowaną aplikację MToken MAA na telefonie. Przy pierwszym otwarciu aplikacji okno wyświetla formatkę rejestracji urządzenia. W momencie wygenerowania przez system kodu aktywacyjnego, użytkownik przechodzi do kolejnego kroku za pomocą przycisku [POSIADAM KOD AKTYWACYJNY],



- użytkownik wpisuje kod wyświetlony przez system EBP i przechodzi do kolejnego okna za pomocą przycisku [DALEJ] w aplikacji MToken MAA,

**ASSECO**  
KOD AKTYWACYJNY



Kod wygenerowany został w bankowości internetowej

Wprowadź kod aktywacyjny

1	2	3
4	5	6
7	8	9
	0	⊗

DALEJ

- użytkownik wpisuje kod weryfikacyjny, przesłany za pomocą SMS,

**ASSECO**  
← WERYFIKACJA SMS →



Przepisz kod weryfikacyjny wysłany jako SMS

.....

1	2	3
4	5	6
7	8	9
	0	⊗

DALEJ

- użytkownik podanie PIN, który będzie służył do logowania do aplikacji MToken MAA oraz autoryzacji zdarzeń. PIN powinien składać się z 5-8 cyfr,

**GJSECO**

← NADAJ PIN ×



PIN służyć będzie do logowania oraz autoryzacji zdarzeń

..... ?

1	2	3
4	5	6
7	8	9
	0	⊗

➤ DALEJ

- użytkownik ponownie wprowadza PIN,



Po pozytywnym przejściu procesu parowania urządzenia, aplikacja MToken MAA wyświetla okno z komunikatem:



Użytkownik zostaje zalogowany do bakowości internetowej w systemie EBP oraz może zalogować się do aplikacji MToken MAA.

### 6.2.2. Logowanie po rejestracji urządzenia

Użytkownik ma możliwość zalogowania się do systemu EBP za pomocą aplikacji mobilnej MToken MAA, jeżeli posiada sparowane aktywne urządzenie oraz hasło stałe.

Proces logowania za pomocą aplikacji mobilnej MToken MAA do systemu EBP przebiega w następujący sposób:

- użytkownik wpisuje numer identyfikacyjny i hasło (ustawione przez użytkownika w momencie pierwszego logowania po sparowaniu urządzenia, zmienione w aplikacji lub zresetowane przez pracownika Banku) i wybiera przycisk [ZALOGUJ],



## Logowanie

Zaloguj się do bankowości internetowej

Numer Identyfikacyjny

DALEJ

## Logowanie

Zaloguj się do bankowości internetowej

Kod dostępu

•	•	•	•	•	•	•
---	---	---	---	---	---	---

1 2 3 4 5 6 7

•	•	•	•	•
---	---	---	---	---

8 9 10 11 12

ZALOGUJ

COFNIJ

- system EBP prezentuje ekran informujący o wysłaniu dyspozycji logowania do aplikacji MToken MAA,

## Uwierzytelnianie

Powiadomienie uwierzytelniające zostało wysłane do urządzenia mobilnego. Pozostań na tej stronie i potwierdź operację w aplikacji mobilnej.



Oczekiwanie na uwierzytelnienie aplikacją mobilną.

- system EBP wysyła do aplikacji MToken MAA powiadomienie PUSH o nowej dyspozycji logowania,
- aplikacja MToken MAA wyświetla na urządzeniu mobilnym baner powiadomienia PUSH z informacją o oczekującym powiadomieniu,
- użytkownik wybiera baner powiadomienia PUSH, które uruchamia aplikację mobilną MToken MAA lub bezpośrednio uruchamia aplikację z systemu operacyjnego urządzenia mobilnego,
- użytkownik loguje się do aplikacji mobilnej MToken MAA,

ASSECO

LOGOWANIE

(LR\*\*\*M)

Witaj, wprowadź PIN, aby się zalogować

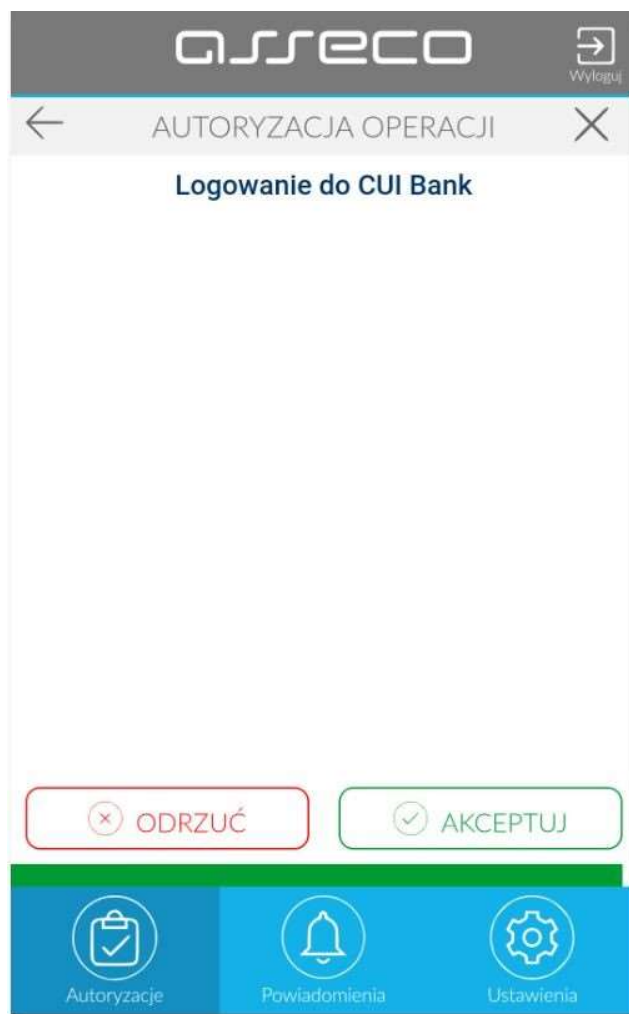
Wprowadź PIN

1	2	3
4	5	6
7	8	9
	0	⊗

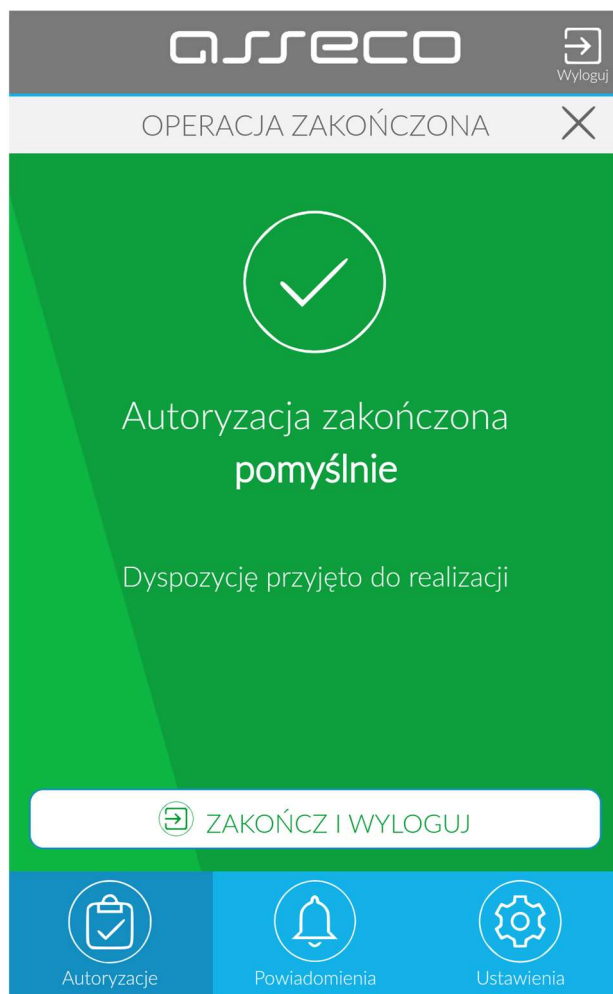
ZALOGUJ

- aplikacja mobilna MToken MAA pobiera z systemu dane do logowania,
- aplikacja mobilna MToken MAA prezentuje dane dyspozycji logowania,
- użytkownik weryfikuje wyświetlone dane oraz potwierdza realizację dyspozycji logowania,





- aplikacja podpisuje dyspozycje za pomocą klucza prywatnego,
- aplikacja MToken MAA wysyła podpisaną dyspozycję do systemu,
- system weryfikuje (z użyciem klucza publicznego) podpis dyspozycji złożony w aplikacji mobilnej MToken MAA oraz przekazuje wynik do aplikacji MToken MAA oraz EBP (weryfikacja pozytywna),
- użytkownik zostaje zalogowany do systemu EBP,
- aplikacja mobilna MToken MAA prezentuje potwierdzenie autoryzacji dyspozycji,

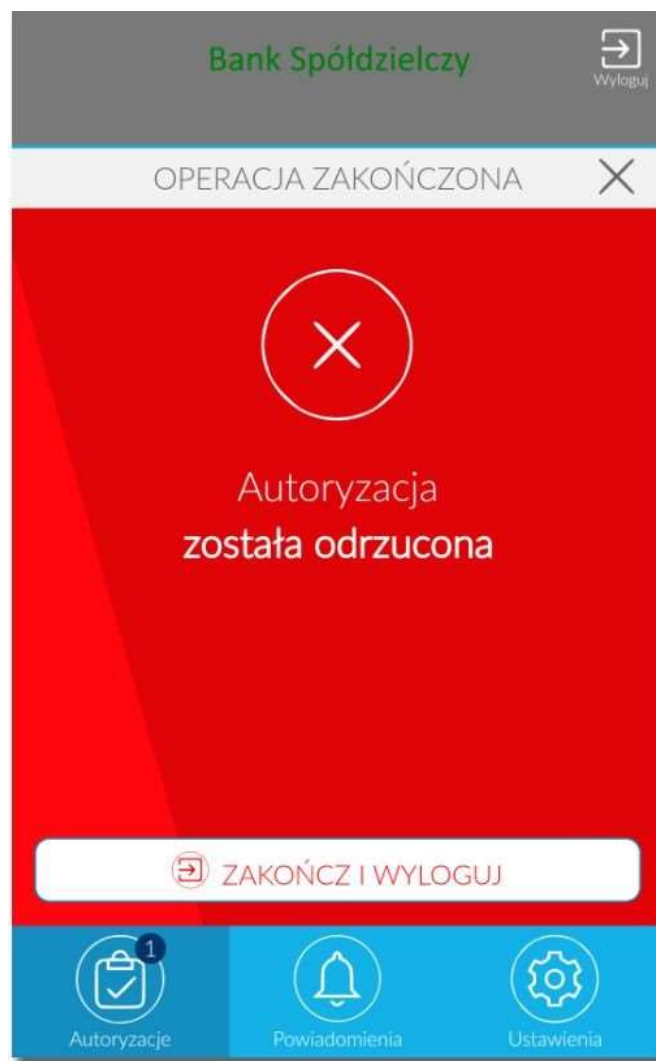


W przypadku, gdy użytkownik nie potwierdził autoryzacji dyspozycji logowania w określonym czasie po wskazaniu dyspozycji w aplikacji mobilnej MToken MAA, wówczas zostanie zaprezentowany następujący komunikat:

- *Upłynął czas akceptacji dyspozycji.*

W przypadku odrzucenia autoryzacji w aplikacji mobilnej MToken MAA zostanie zaprezentowany komunikat:

- *Autoryzacja została odrzucona.*



W procesie logowania do systemu EBP za pomocą aplikacji mobilnej MToken MAA, na etapie uwierzytelnienia może pojawić się komunikat z informacją o błędzie:

- *Błąd na etapie uwierzytelniania* w przypadku, gdy:
  - podano niepoprawne hasło,
  - inny błąd techniczny.
- *Błąd uwierzytelnienia* w przypadku:
  - braku podpisania dyspozycji w określonym czasie,
  - odrzucenia autoryzacji w aplikacji mobilnej MToken MAA.

### 6.3. Logowanie do systemu EBP przy pomocy karty mikroprocesorowej

Użytkownik ma możliwość zalogowania się do systemu EBP za pomocą karty mikroprocesorowej.

### 6.3.1. Pierwsze logowanie do systemu EBP za pomocą karty mikroprocesorowej wraz z rejestracją urządzenia

Proces pierwszego logowania za pomocą karty mikroprocesorowej do EBP przebiega w następujący sposób:

- użytkownik wprowadza identyfikator, oraz naciska przycisk [ZALOGUJ SIĘ ZA POMOCĄ E-PODPISU].

**Logowanie**

Zaloguj się do bankowości internetowej

Numer Identyfikacyjny użytkownika  
SG4EPQBLUV

**ZALOGUJ SIĘ ZA POMOCĄ E-PODPISU**

COFNIJ

ZASADY BEZPIECZEŃSTWA  
BEZPIECZNE ZAKUPY W INTERECIE

**GISECO**

**Pamiętaj o podstawowych zasadach bezpieczeństwa.**

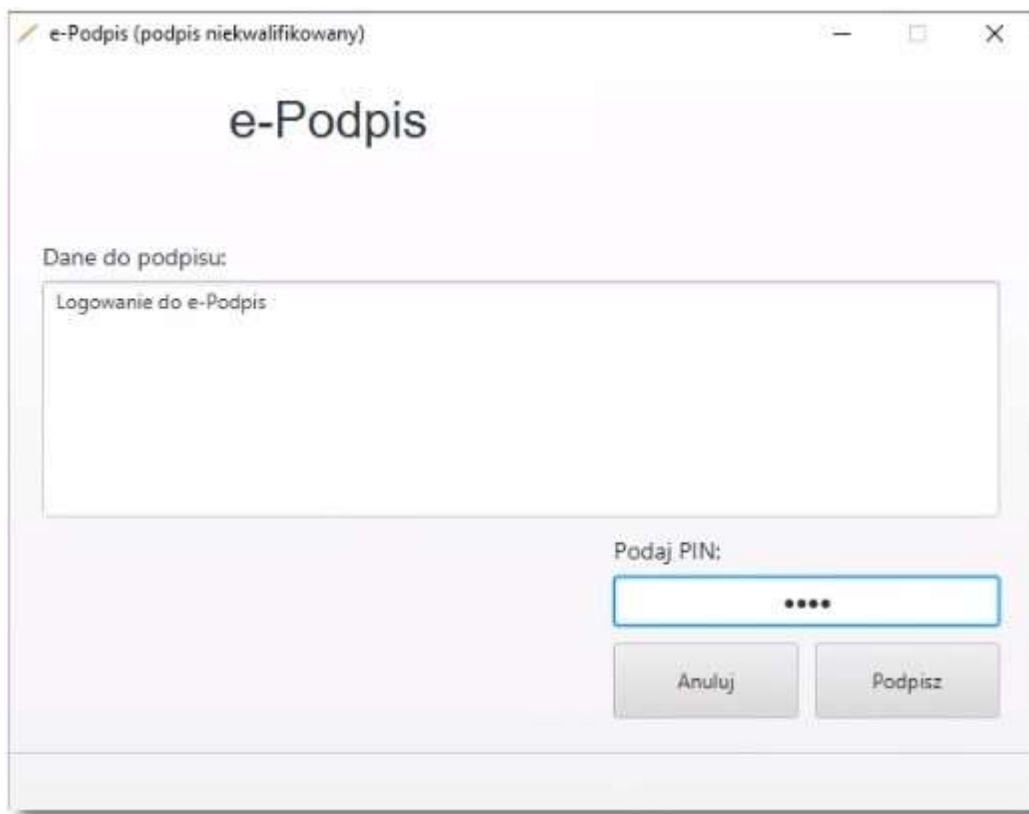
Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- 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 Symantec

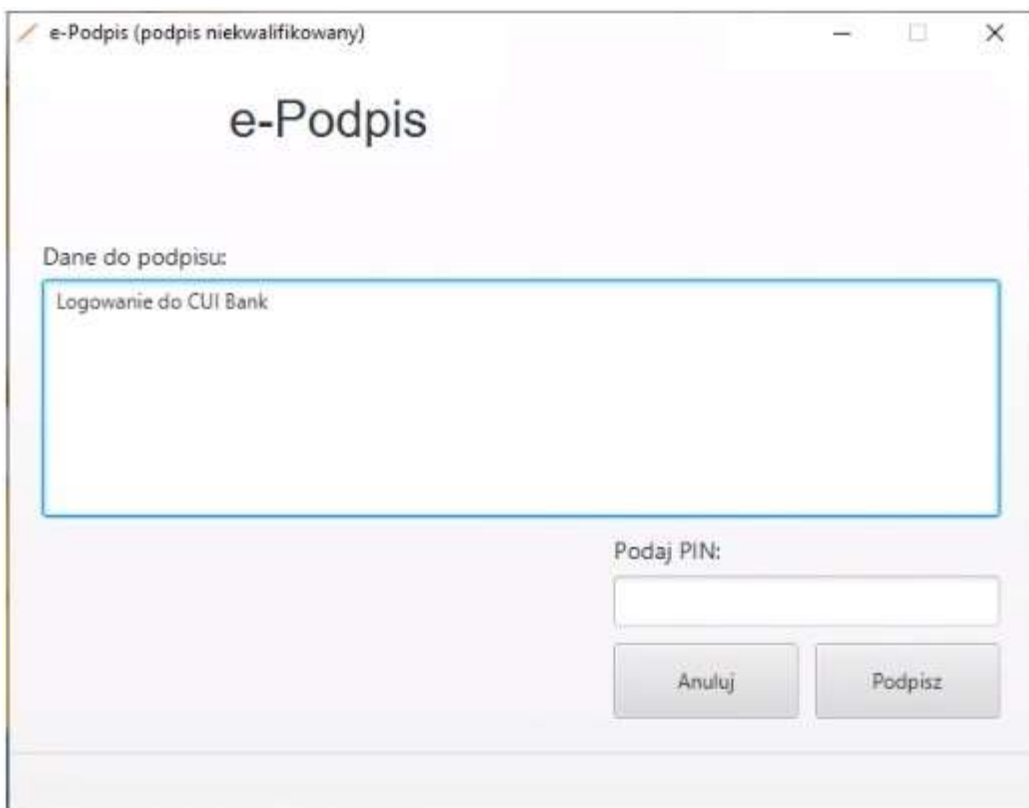
**Pamiętaj!**  
Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na komputerach użytkowników.

W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z naszym Bankiem

- system w nowym oknie przeglądarki pobiera aplikację SCSA pozwalającą na wykonanie podpisu kartą mikroprocesorową.
- po zainstalowaniu system prezentuje użytkownikowi ekran do zalogowania się do aplikacji SCSA.



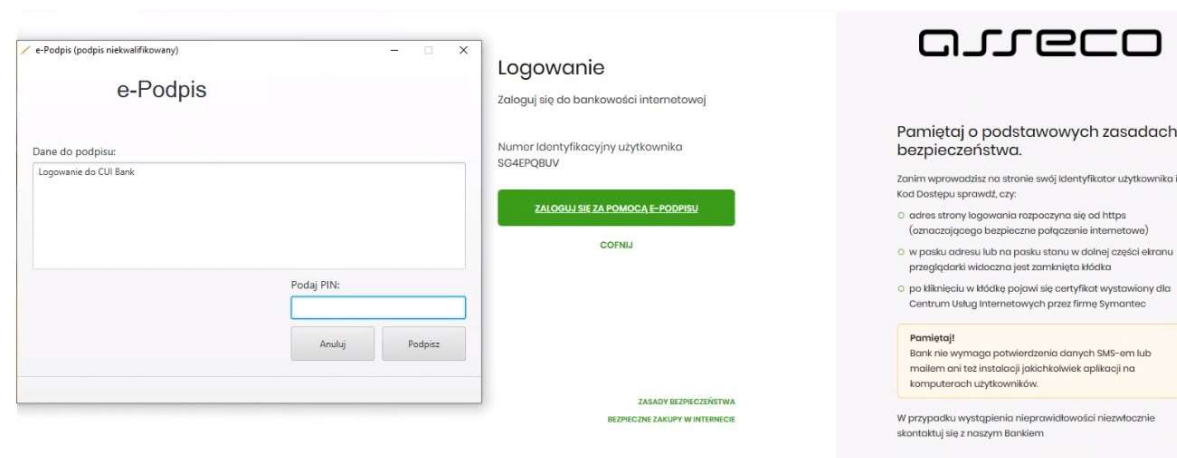
- użytkownik wpisuje PIN, następnie naciska przycisk [PODPISZ], system sprawdza aplikacja sprawdza poprawność wprowadzonych.
- po poprawnej weryfikacji wprowadzonego PIN-u, system na stronie logowania do systemu EBP prezentuje ekran do wprowadzenia PIN karty mikroprocesorowej.



- po poprawnym wprowadzeniu PIN system loguje użytkownika do systemu EBP.

## 6.3.2. Kolejne logowanie do systemu EBP przy pomocy karty mikroprocesorowej

Przy kolejnym logowaniu do systemu EBP, po wpisaniu identyfikatora system automatycznie podpowiada ekran do wprowadzenia PIN.



Po poprawnym wprowadzeniu PIN system loguje użytkownika do systemu EBP.

## 6.4. Logowanie do systemu EBP przy pomocy hasła maskowanego + kodu SMS

Użytkownik ma możliwość zalogowania się do systemu EBP za pomocą hasła maskowanego + kodu SMS.

### 6.4.1. Pierwsze logowanie do systemu EBP przy pomocy hasła maskowanego + kodu SMS

Po uruchomieniu systemu EBP wyświetlane jest okno logowania:

The image shows a web interface for logging into an internet banking account. On the left, there is a logo at the top, followed by the heading "Logowanie" and the instruction "Zaloguj się do bankowości internetowej". Below this is a label "Numer Identyfikacyjny" and an empty text input field. A green button labeled "DALEJ" is positioned below the input field. At the bottom left, there is a language selector showing "PL" with a dropdown arrow, and a link for "ZASADY BEZPIECZEŃSTWA" and "BEZPIECZNE ZAKUPY W INTERNECIE".

**Pamiętaj o podstawowych zasadach bezpieczeństwa.**

Zanim wprowadzisz na stronie swój Numer Identyfikacyjny 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 Symantec

**Pamiętaj!**  
Bank nie wymaga potwierdzenia danych SMS-om lub mailem ani też instalacji jakichkolwiek aplikacji na komputerach użytkowników.

W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z naszym Bankiem

Pierwsze logowanie odbywa się w następujących krokach:

- wprowadzenie identyfikatora użytkownika i naciśnięciu przycisku [DALEJ]. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tą wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami,
- wprowadzenie hasła, które zostało przesłane w wiadomości sms (hasło tymczasowe) i potwierdzeniu przyciskiem [ZALOGUJ],

## Logowanie

Zaloguj się do bankowości internetowej

Kod dostępu

1 2 3 4 5 6 7

8

ZALOGUJ

COFNIJ

ZASADY BEZPIECZEŃSTWA  
BEZPIECZNE ZAKUPY W INTERECIE

- potwierdzenie logowania otrzymanym kodem sms i naciśnięcie przycisku [ZALOGUJ],



## Logowanie

Zaloguj się do bankowości internetowej

Kod dostępu

•	•	•	•	•	•	•
1	2	3	4	5	6	7
•						
8						

Kod SMS

Dodaj do zaufanych

Dodaj urządzenie z którego się logujesz do "zaufanych" aby za każdym razem nie potwierdzać logowania SMS-em

[COFNIJ](#)

- możliwości wybrania za pomocą checkboxa DODAJ DO ZAUFANYCH – wybór tej opcji spowoduje pojawienie się okna z nazwą zaufanego urządzenia (nazwę można edytować, maksymalna liczba znaków to 50),

## Logowanie

Zaloguj się do bankowości internetowej

Kod dostępu

•	•	•	•	•	•	•
1	2	3	4	5	6	7
•						
8						

Kod SMS

Dodaj do zaufanych

Dodaj urządzenie z którego się logujesz do "zaufanych" aby za każdym razem nie potwierdzać logowania SMS-em

Nazwa zaufanego urządzenia

ZALOGUJ

COFNIJ

- ustawienie nowego hasła do logowania z zachowaniem zasad bezpieczeństwa, oraz potwierdzenie za pomocą przycisku [ZAPISZ I ZALOGUJ]:
  - hasło musi składać się z 4-8 znaków
  - hasło musi zawierać przynajmniej jedną małą i wielką literę
  - hasło musi zawierać przynajmniej jeden znak specjalny
  - hasło musi zawierać przynajmniej jedną cyfrę

## Polityka bezpieczeństwa banku wymaga zmiany hasła.

Numer Identyfikacyjny użytkownika  
LTMS4FCP

Nowe hasło

Powtórz nowe hasło

ZAPISZ I ZALOGUJ

### Zadbaj o zachowanie poufności swojego hasła.

Nie udostępniaj hasła innym osobom, na żadnych stronach internetowych, pocztą elektroniczną, wiadomością SMS lub w odpowiedzi na ządania otrzymane od pracowników banku.

Definiując swoje hasło pamiętaj o zachowaniu zasad bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

### Zasady budowy haseł są następujące:

- musi składać się z 4-8 znaków
- musi zawierać przynajmniej jedną wielką literę
- musi zawierać przynajmniej jedną małą literę
- musi zawierać przynajmniej jeden znak specjalny
- musi zawierać przynajmniej jedną cyfrę

Po poprawnym ustawieniu nowego hasła, użytkownik zostanie zalogowany do systemu EBP.

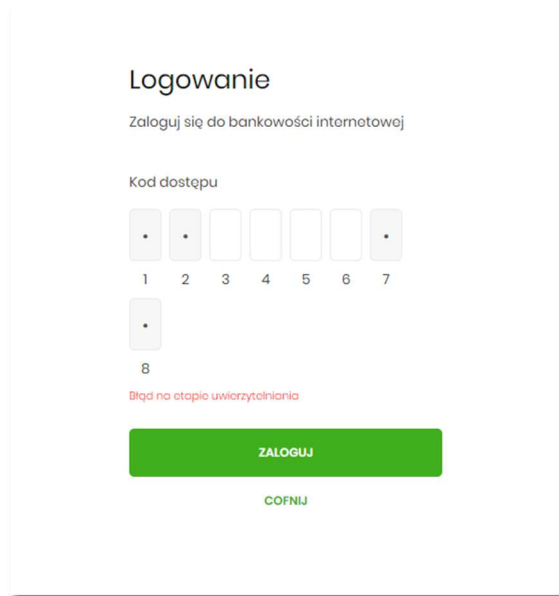
### 6.4.2. Kolejne logowanie do systemu EBP przy pomocy hasła maskowanego + kodu SMS (bez dodania urządzenia do zaufanych)

Podczas kolejnego logowania do systemu EBP, użytkownik musi wprowadzić:

- identyfikator użytkownika i nacisnąć przycisk [DALEJ],
- hasło i potwierdzić przyciskiem [ZALOGUJ],
- otrzymany kod SMS, potwierdzający logowanie i nacisnąć przycisk [ZALOGUJ].

W przypadku wprowadzenia poprawnych danych, użytkownik zostanie zalogowany do systemu EBP, natomiast w przypadku wprowadzenia błędnych danych, system zaprezentuje odpowiedni komunikat. W przypadku wprowadzenia:

- błędnego hasła, system zaprezentuje komunikat: *Błąd na etapie uwierzytelniania.*



The screenshot shows a login interface with the following elements:

- Logowanie** (Login)
- Zaloguj się do bankowości internetowej (Log in to internet banking)
- Kod dostępu (Access code)
- Input fields for digits 1 through 7, each containing a black dot.
- Input field for digit 8, also containing a black dot.
- Red error message: *Błąd na etapie uwierzytelniania* (Error during authentication).
- Green button: **ZALOGUJ** (Log in).
- Green text: **COFNIJ** (Go back).

- błędnego kodu SMS, system zaprezentuje komunikat: *Błędny kod SMS.*

## Logowanie

Zaloguj się do bankowości internetowej

Kod dostępu

1 2 3 4 5 6 7

8

Kod SMS

Błędny kod SMS

Dodaj do zaufanych

Dodaj urządzenie z którego się logujesz do "zaufanych" aby za każdym razem nie potwierdzać logowania SMS-em

[COFNIJ](#)

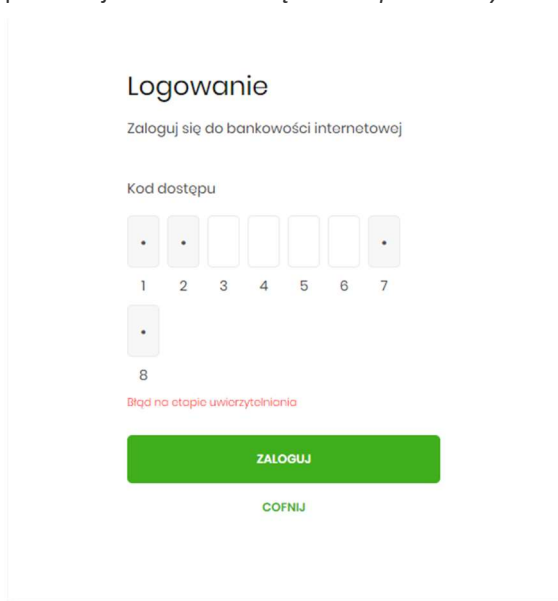
### 6.4.3. Kolejne logowanie do systemu EBP przy pomocy hasła maskowanego + kodu SMS (po dodaniu urządzenia do zaufanych)

Podczas kolejnego logowania do systemu EBP, użytkownik musi wprowadzić:

- identyfikator użytkownika i nacisnąć przycisk [DALEJ],
- hasło i potwierdzić przyciskiem [ZALOGUJ],

W przypadku wprowadzenia poprawnych danych, użytkownik zostanie od razu zalogowany do systemu EBP, natomiast w przypadku wprowadzenia błędnych danych, system zaprezentuje odpowiedni komunikat. W przypadku wprowadzenia:

- błędnego hasła, system zaprezentuje komunikat: *Błąd na etapie uwierzytelniania*.



The screenshot shows a login interface with the following elements:

- Logowanie** (Login)
- Zaloguj się do bankowości internetowej (Log in to internet banking)
- Kod dostępu (Access code)
- Input fields for digits 1 through 7, with the first and last fields containing a black dot.
- Input field for digit 8, containing a black dot.
- Red error message: *Błąd na etapie uwierzytelniania* (Error during authentication).
- Green button: **ZALOGUJ** (Log in)
- Text: **COFNIJ** (Cancel)

## Rozdział 7. Metody autoryzacji zleceń

Po uzyskaniu dostępu do aplikacji EBP użytkownik może korzystać z oferowanych mu funkcji aplikacji w celu wykonywania operacji bankowych w ramach udostępnionych mu rachunków bieżących. W aplikacji EBP dostępne są następujące sposoby uwierzytelniania operacji przez użytkownika:

- autoryzowanie operacji za pomocą karty mikroprocesorowej,
- autoryzowanie operacji za pomocą kodu PIN i kodu SMS,
- autoryzowanie operacji za pomocą podpisu mobilnego.

### 7.1. Mobilny podpis

W przypadku użytkowników posiadających przypisaną metodę autoryzacji Mobilny podpis, autoryzacja zleceń następuje po akceptacji operacji w aplikacji mobilnej MToken MAA na sparowanym urządzeniu autoryzującym.

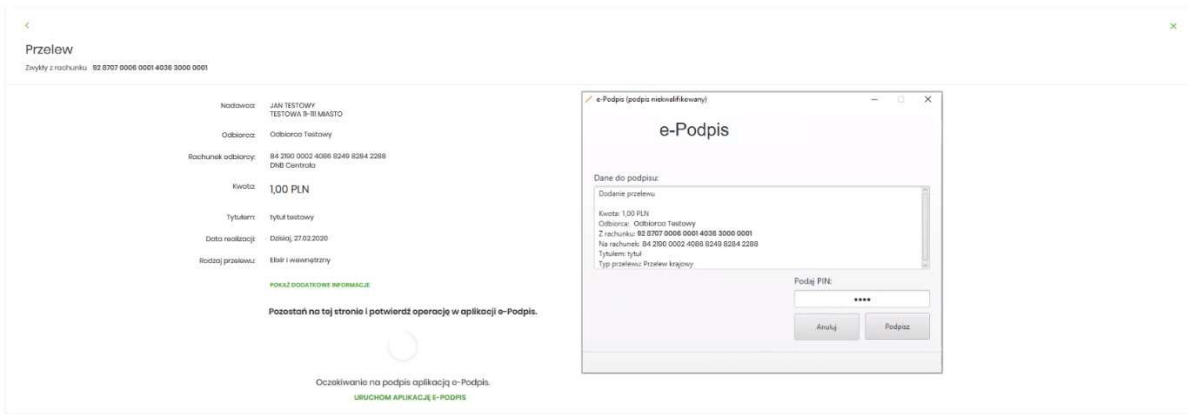
W procesie autoryzacji dyspozycji za pomocą aplikacji mobilnej MToken MAA mogą wystąpić następujące komunikaty informujące o błędzie:

- *Nastąpiło przekroczenie czasu oczekiwania na autoryzację*, w przypadku:
  - braku podpisania dyspozycji w określonym czasie.
- *Autoryzacja została odrzucona*, w przypadku:
  - odrzucenia autoryzacji w aplikacji mobilnej MToken MAA.
- *Brak odpowiedzi z serwera autoryzującego*, w przypadku gdy:
  - serwer autoryzacyjny nie zwrócił informacji w określonym czasie.
- *Błąd autoryzacji*, w przypadku:
  - błędu w systemie autoryzacyjnym.
- *Brakuje powiązanego urządzenia do autoryzacji mobilnej*, w przypadku gdy:
  - użytkownik nie posiada aktywnego urządzenia mobilnego.

### 7.2. Karta mikroprocesorowa

Autoryzacja dyspozycji przy pomocy karty mikroprocesorowej.

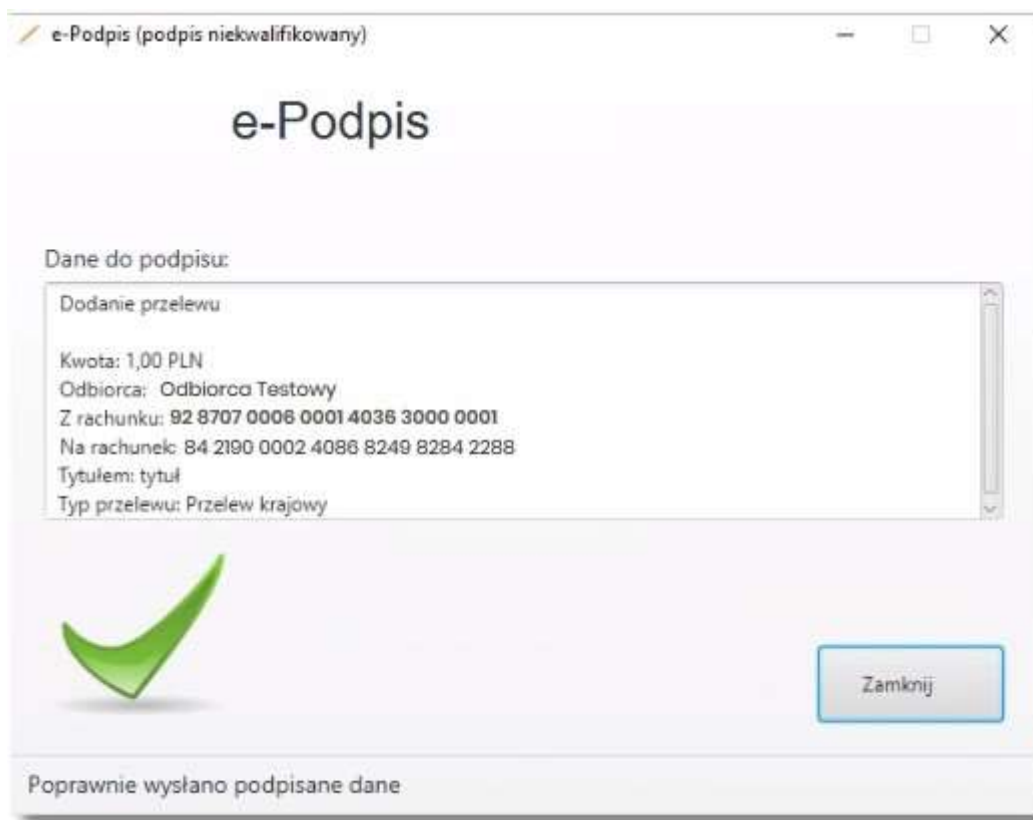
Po wprowadzeniu danych dyspozycji przelewu i naciśnięciu [DALEJ] system prezentuje formularz potwierdzenia wprowadzonych danych wraz oknem do prowadzenia kodu PIN



Na formularzu E-PODPIS dostępne są akcje:

- [ANULUJ] – umożliwia rezygnację z podpisania dyspozycji,
- [PODPISZ] – umożliwia podpisanie dyspozycji.

Po wprowadzeniu kodu PIN i naciśnięciu [PODPISZ] system prezentuje formularz z informacją o poprawnej autoryzacji dyspozycji.



Po naciśnięciu [ZAMKNIJ] system prezentuje formularz z potwierdzeniem realizacji dyspozycji.

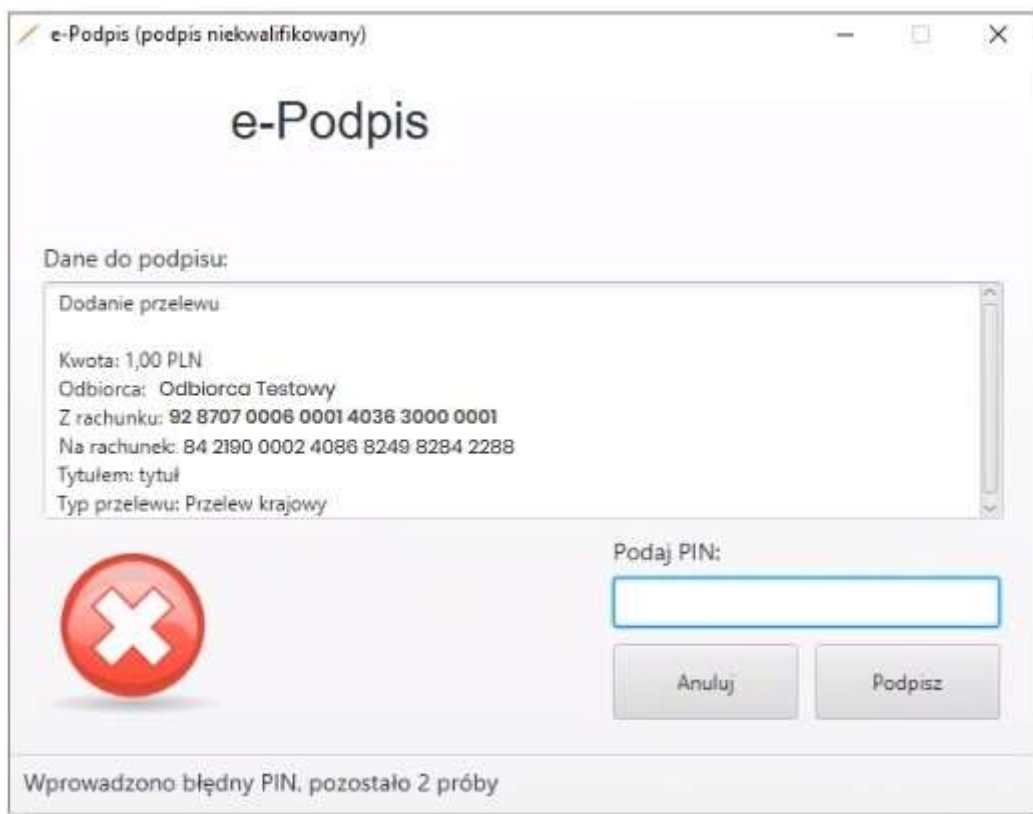




Na formularzu POTWIERDZENIE dostępne są akcje:

- [WRÓĆ DO PULPITU] – umożliwia powrót do pulpitu,
- [UTWÓRZ NOWY PRZELEW] – umożliwia utworzenie nowej dyspozycji,
- [ZAPISZ JAKO SZABLON] – umożliwia zapisanie dyspozycji jako szablon.

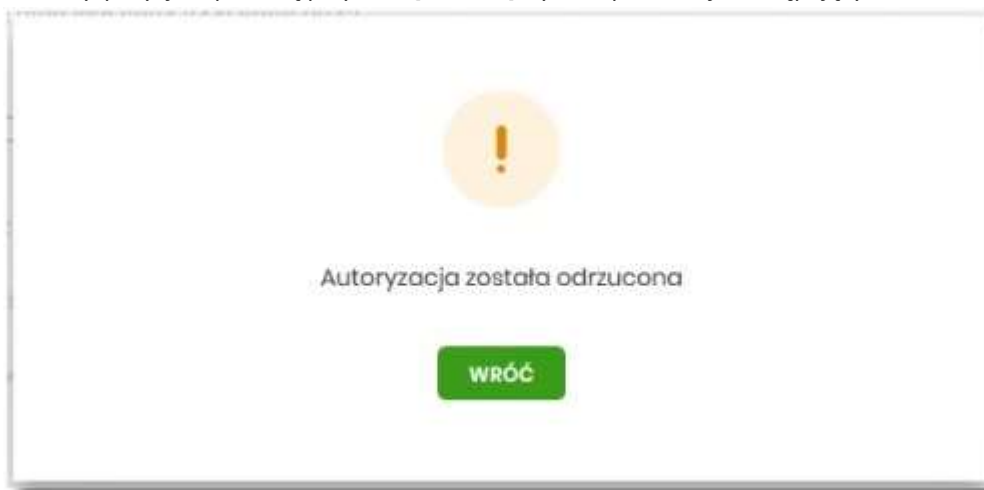
W przypadku gdy użytkownik wprowadzi błędny kod PIN system zaprezentuje komunikat:



Na formularzu E-PODPIS dostępne są akcje:

- [ANULUJ] – umożliwia rezygnację z podpisania dyspozycji,
- [PODPISZ] – umożliwia wprowadzenie poprawnego kodu i podpisanie dyspozycji.

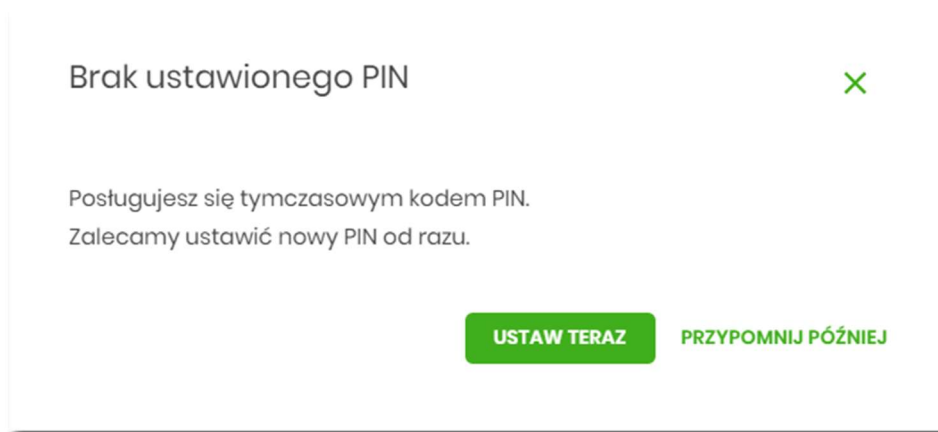
Po odrzuceniu dyspozycji za pomocą przycisku [ANULUJ], system prezentuje następujący komunikat:



## 7.3. Kod PIN + kod SMS

W przypadku użytkowników posiadających przypisaną metodę autoryzacji Kod PIN + Kod SMS, autoryzacja zleceń następuje po wprowadzeniu poprawnego kodu PIN oraz przesłanego kodu SMS.

Jeśli użytkownik ma ustawiony sposób autoryzacji na Kod PIN + kod SMS lub zrestartował PIN za pomocą administratora banku to po zalogowaniu system zaprezentuje komunikat zalecający zmianę PINu do autoryzacji.



Wybór przycisku [USTAW TERAZ] powoduje przeniesienie użytkownika do formatki ZMIANA PIN DO AUTORYZACJI. PIN ważny jest przez określony czas (np. 15 min).

Zadbaj o zachowanie poufności swojego PIN.

- Nie udostępniaj PIN innym osobom, na żadnych stronach internetowych, poczty elektronicznej, wiadomością SMS lub w odpowiedzi na zapytanie otrzymane od pracowników banku.
- Definiując swój PIN pamiętaj o zachowaniu zasad bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

Zasady budowy PIN są następujące:

- musi składać się z 4-8 znaków
- musi zawierać przynajmniej jedną wielką literę
- musi zawierać przynajmniej jedną małą literę
- musi zawierać przynajmniej jeden znak specjalny
- musi zawierać przynajmniej jedną cyfrę
- może zawierać wyłącznie znaki ze zbioru: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!@#\$%^&\*()-\_+=+[]\|:;'"<>/?

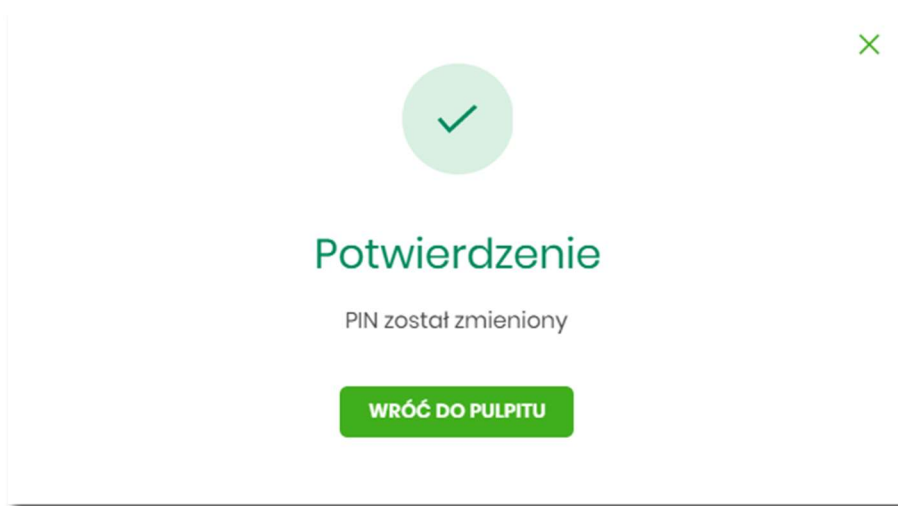
Użytkownik musi wpisać obecny PIN tymczasowy, który otrzymał za pomocą SMS oraz wpisać i powtórzyć nowy PIN, a następnie kliknąć przycisk [ZATWIERDŹ].

Nowy PIN musi być zgodny z Zasadami bezpieczeństwa zgodnie z informacją w dolnej części formularza, tzn.:

- musi składać się z 4-8 znaków,

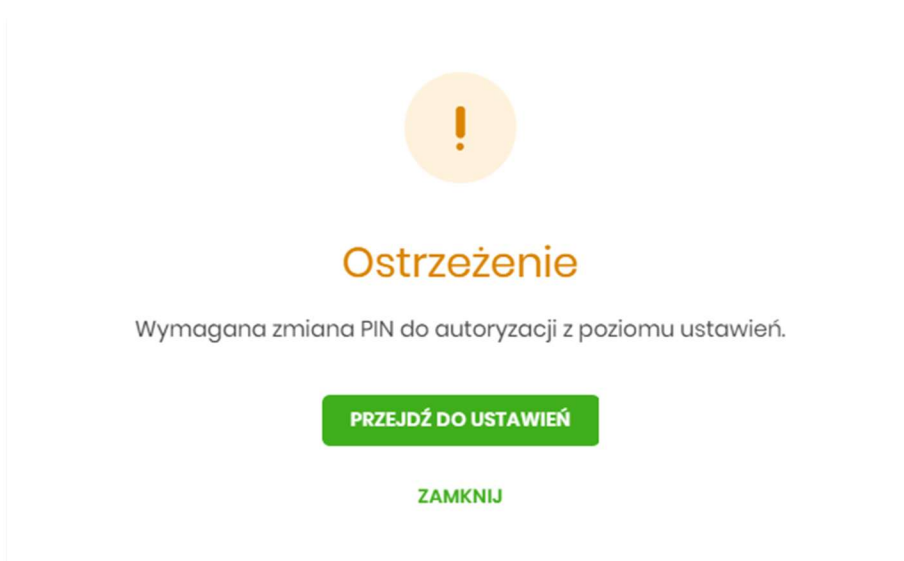
- musi zawierać przynajmniej jedną wielką literę,
- musi zawierać przynajmniej jedną małą literę,
- musi zawierać przynajmniej jeden znak specjalny,
- musi zawierać przynajmniej jedną cyfrę,
- może zawierać wyłącznie znaki ze zbioru:  
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!@#\$\$%^&\*()-  
\_=[\]\|;:“,<.>/?.

Po zatwierdzeniu zmian, system prezentuje komunikat: *PIN został zmieniony.*



Natomiast wybór przycisku [PRZYPOMNIJ PÓŹNIEJ] spowoduje, że system wyświetli komunikat o konieczności zmiany PIN po ponownym zalogowaniu.

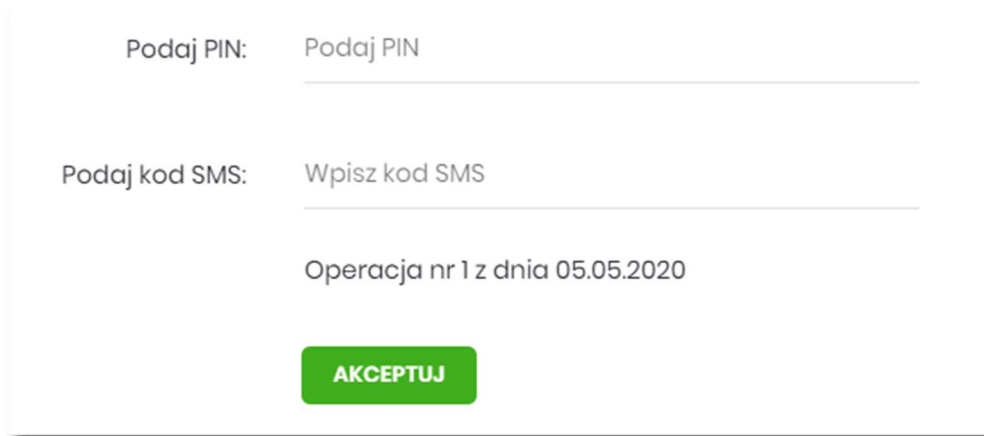
Jeśli użytkownik nie zmieni PIN do autoryzacji bezpośrednio po zalogowaniu i przejdzie do wykonania przelewów, to przy wejściu użytkownika na formularz potwierdzenia przelewu, system wymusza zmianę PINu, prezentując odpowiedni komunikat:



Wybór przycisku [PRZEJDŹ DO USTAWIĘŃ] powoduje przeniesienie użytkownika do formatki ZMIANA PIN DO AUTORYZACJI. PIN ważny jest przez określony czas (np. 15 min).

Po zmianie PINu tymczasowego, aby zautoryzować dyspozycję użytkownik będzie musiał:

- podać PIN w polu *Podaj PIN*,
- podać kod SMS w polu *Podaj kod SMS*,
- zatwierdzić zmiany za pomocą przycisku [AKCEPTUJ].



Podaj PIN: Podaj PIN

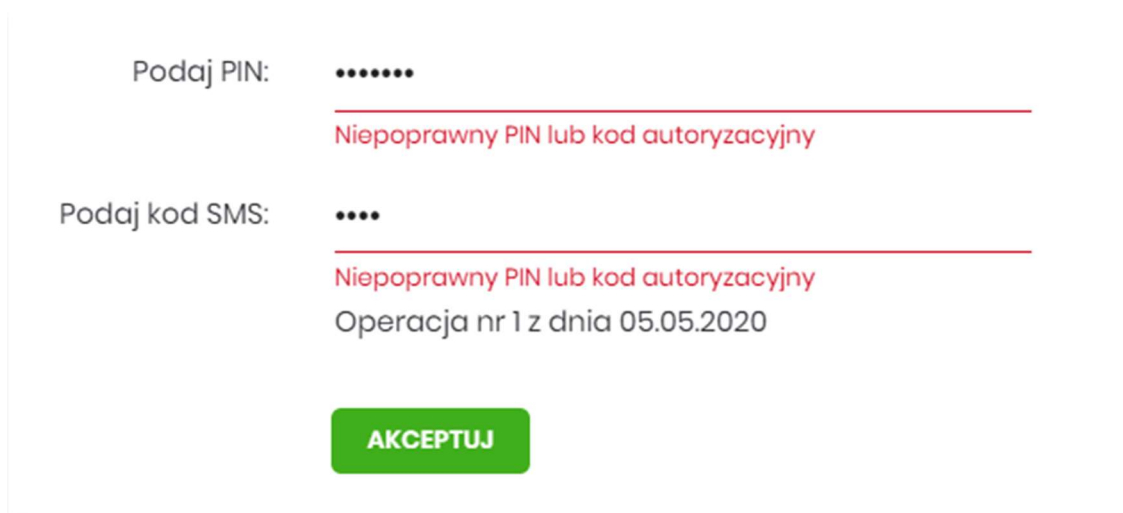
Podaj kod SMS: Wpisz kod SMS

Operacja nr 1 z dnia 05.05.2020

**AKCEPTUJ**

W przypadku poprawnej weryfikacji danych system zaprezentuje komunikat o poprawnej autoryzacji.

W przypadku wprowadzenia błędnego PINu albo kodu SMS, system wyświetli odpowiedni komunikat:



Podaj PIN: ●●●●●●

Niepoprawny PIN lub kod autoryzacyjny

Podaj kod SMS: ●●●●

Niepoprawny PIN lub kod autoryzacyjny

Operacja nr 1 z dnia 05.05.2020

**AKCEPTUJ**

## Rozdział 8. Wybór kontekstu przez użytkownika w systemie EBP

System EBP udostępnia nowoczesny tryb pracy, pozwalający na wybór przez użytkownika kontekstu (indywidualnego, firmowego), w jakim będzie zalogowany w systemie EBP. Funkcjonalność ta umożliwia użytkownikowi w trakcie pracy, swobodne przełączanie się pomiędzy kontekstami i w zależności od jego wyboru działanie jako użytkownik detaliczny (kontekst indywidualny) i obsługę rachunków indywidualnych lub jako użytkownik firmowy (kontekst firmowy) i obsługę rachunków firmowych.

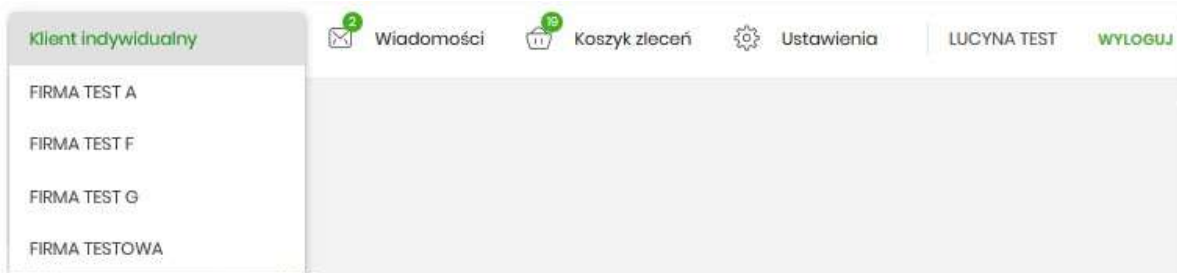
Obsługa kontekstów obejmuje następujące warianty:

- użytkownik posiada kontekst indywidualny, a nie posiada firmowego. W takim przypadku, po zalogowaniu użytkownik nie ma dostępu do zmiany kontekstu. System oferuje funkcjonalności dla użytkowników detalicznych.
- użytkownik posiada kontekst firmowy i jest użytkownikiem technicznym. W takim przypadku, po zalogowaniu użytkownik nie ma dostępu do zmiany kontekstu.
- użytkownik posiada nieaktywny kontekst firmowy. W takim przypadku, po zalogowaniu użytkownik nie ma dostępu do zmiany kontekstu. System oferuje funkcjonalności dla użytkowników detalicznych.
- użytkownik posiada aktywny kontekst firmowy, ale kontekst ten nie jest domyślny. W takim przypadku, po zalogowaniu użytkownik jest w kontekście indywidualnym, ale ma możliwość zmiany na kontekst firmowy.
- użytkownik posiada aktywny kontekst firmowy i jest on domyślny. W takim przypadku, po zalogowaniu użytkownik jest w kontekście firmowym i ma możliwość zmiany na kontekst indywidualny.
- użytkownik posiada wiele przypisanych kontekstów firmowych. Po zalogowaniu system prezentuje listę kontekstów. Lista zawiera nazwy aktywnych kontekstów firmowych oraz kontekst indywidualny.

W górnym menu, użytkownik ma możliwość podglądu i zmiany kontekstu, w którym obecnie jest zalogowany



Po naciśnięciu  system prezentuje listę dostępnych dla użytkownika kontekstów.



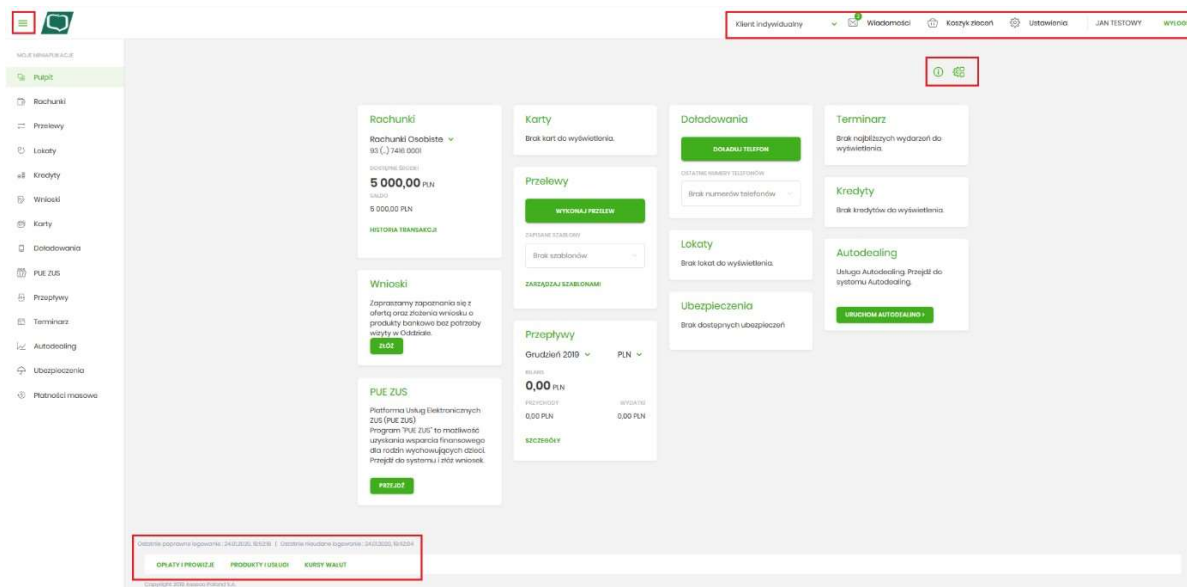
Wybór kontekstu z listy powoduje przełączenie użytkownika w kontekście którym będzie zalogowany w systemie EBP.

## Rozdział 9. Pulpit

Użytkownikowi po zalogowaniu do systemu EBP zostaje wyświetlany pulpit z miniaplikacjami w formie widżetów (kafli). Pulpit stanowi także obszar roboczy użytkownika, w którym prezentowana jest otwarta miniaplikacja.

Układ miniaplikacji na pulpicie jest indywidualnie pamiętany dla użytkownika w ramach danego kontekstu.

Kliknięcie w obszar wybranego widżetu powoduje przejście do wybranej miniaplikacji.



W górnej części formularza, system prezentuje menu z następującymi informacjami/opcjami:



•

– kliknięcie w opcję powoduje ukrycie/zaprezentowanie menu bocznego MOJE MINIAPLIKACJE,



•

– informacja na temat kontekstu w jakim zalogowany jest użytkownik wraz z opcją umożliwiającą zmianę kontekstu,



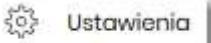
•

– umożliwi przejście do miniaplikacji Wiadomości (funkcjonalność opisana w ramach miniaplikacji Wiadomości),





- - koszyk zleceń (funkcjonalność opisana w ramach miniaplikacji Koszyk),



- - zapewnia dostęp użytkownikowi do opcji ustawień systemu,

JAN TESTOWY

- - nazwa użytkownika zalogowanego w systemie EBP,

WYLOGUJ

- - przycisk umożliwia bezpieczne wylogowanie użytkownika z systemu EBP.

W prawym górnym rogu nad miniaplikacjami system prezentuje dodatkowe opcje:



- - samouczek prezentujący użytkownikowi informację na temat parametryzacji i ustawień indywidualnych systemu EBP,



- - opcja umożliwiająca użytkownikowi dostosowanie pulpitu do swoich potrzeb, pozwala na zmianę widoczności miniaplikacji na pulpicie oraz zmianę kolejności ich prezentacji (zgodnie z opisem w punkcie 9.1).

W dolnej części formularza głównego, system prezentuje:

- informacje na temat logowania użytkownika do systemu EBP:
  - ostatniego poprawnego logowania (w formacie RRRR.MM.DD GG:MM:SS), ◦
  - ostatniego nieudanego logowania (w formacie RRRR.MM.DD GG:MM:SS),

- opcje:
  - [PRODUKTY I USŁUGI] – umożliwia przekierowanie użytkownika do strony z produktami i usługami,
  - [OPŁATY I PROWIZJE] – umożliwia przekierowanie użytkownika do strony z opłatami i prowizjami,
  - [KURSY WALUT] – umożliwia przekierowanie użytkownika do strony z kursami walut,

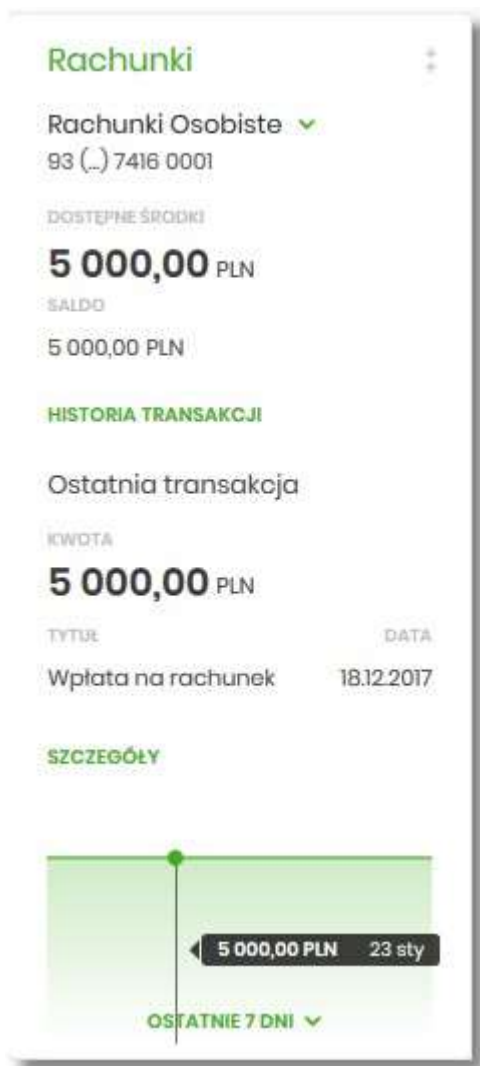
[PRODUKTY I USŁUGI](#)   [OPŁATY I PROWIZJE](#)   [KURSY WALUT](#)

Widżet na pulpicie może być w dwóch rozmiarach:



- standardowym,



- rozszerzonym.



W zależności od wariantu rozmiaru po najechnaniu myszką na prawy górny róg widżetu widoczne są następujące ikony:


- 
 • ikona – powoduje rozszerzenie widżetu o dodatkowe informacje,
- 
 • ikona – powoduje powrót do rozmiaru standardowego.

Kliknięcie w tytuł widżetu na pulpicie np. Rachunki, Przelewy, Lokaty, powoduje przejście do miniaplikacji i otwarcie jej na pulpicie.

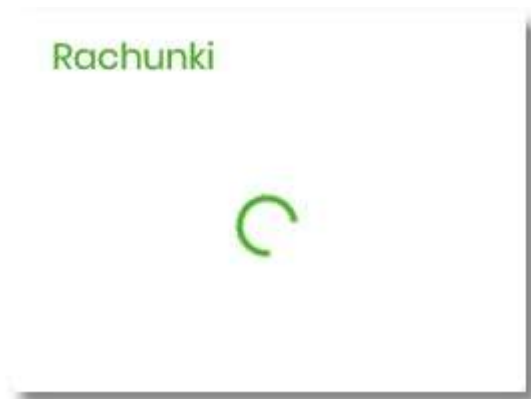
Użytkownik może w dowolnym momencie korzystania z systemu oraz z poziomu dowolnej miniaplikacji wyświetlić pulpit:

- wybierając dostępną w menu bocznym opcję *Pulpit*,



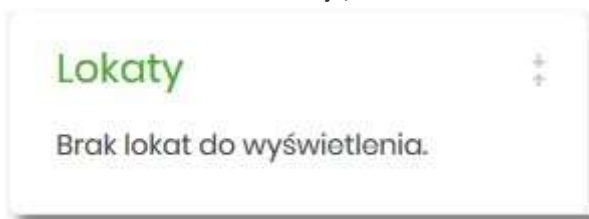
- naciskając  przycisk umieszczonym w prawym, górnym rogu miniaplikacji.

Jeżeli ładowanie danych na widżet trwa dłużej niż ustalona maksymalna długość oczekiwania, wówczas widżet prezentowany jest w trybie ładowania danych:

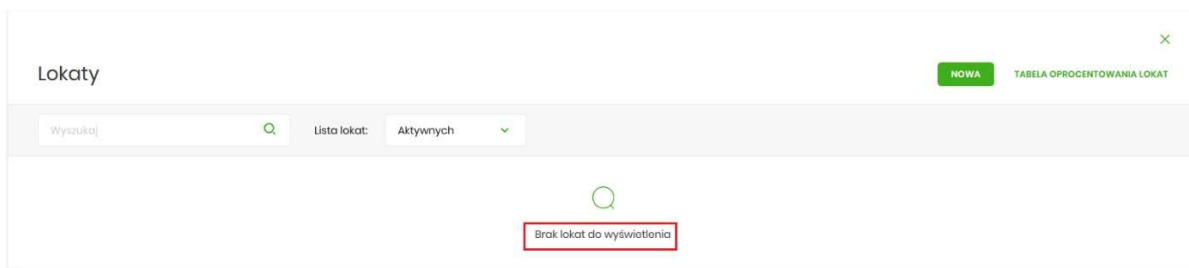


W przypadku, gdy użytkownik nie posiada dedykowanego produktu, wówczas:

- na widżecie będzie prezentowana stosowna informacja,




- po kliknięciu w miniaplikację nastąpi przekierowanie na formularz szczegółów miniaplikacji, z informacją o braku danych do wyświetlenia.

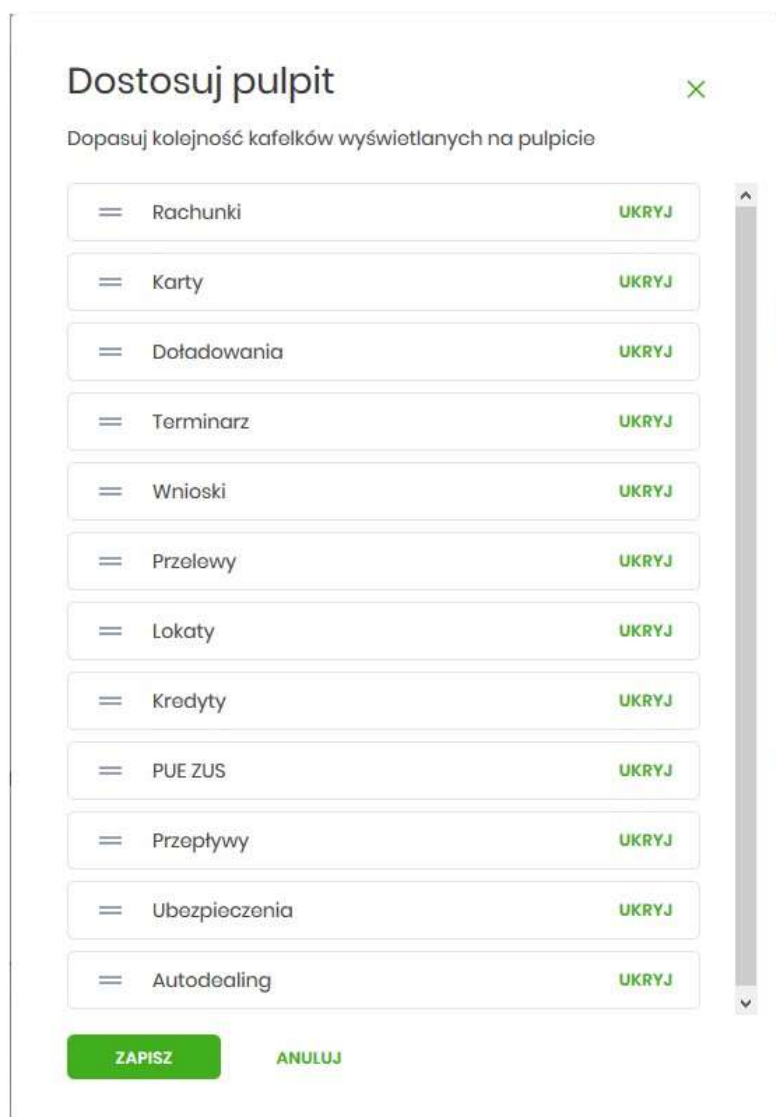



## 9.1. Edycja wyglądu pulpitu



Za pomocą ikony  znajdującej się na pulpicie głównym, użytkownik ma możliwość zmiany widoczności miniaplikacji oraz zmiany kolejności ich prezentacji na pulpicie.

Po naciśnięciu tej opcji, wyświetlane jest okno Dostosuj pulpit, na którym widoczny jest zestaw wszystkich miniaplikacji.



Zmiana położenia kafla polega na kliknięciu w ikonę  przy wybranej miniaplikacji (kursor myszki zmienia się na krzyżyk), przytrzymaniu lewego przycisku myszki a następnie przeciągnięcie pozycji na dowolne miejsce listy.

Pokazanie/ukrycie kafla sprowadza się do kliknięcia w przycisk znajdujący się przy wskazanej miniaplikacji: [POKAŻ]/[UKRYJ].

### Dostosuj pulpit ×

Dopasuj kolejność kafelków wyświetlanych na pulpicie


<input checked="" type="checkbox"/>	Rachunki	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Karty	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Doładowania	<input type="checkbox"/>
<input type="checkbox"/>	Terminarz	<input type="checkbox"/>
<input type="checkbox"/>	Wnioski	<input type="checkbox"/>
<input type="checkbox"/>	Przelewy	<input type="checkbox"/>
<input type="checkbox"/>	Lokaty	<input type="checkbox"/>
<input type="checkbox"/>	Kredyty	<input type="checkbox"/>
<input type="checkbox"/>	PUE ZUS	<input type="checkbox"/>
<input type="checkbox"/>	Przepływy	<input type="checkbox"/>
<input type="checkbox"/>	Ubezpieczenia	<input type="checkbox"/>
<input type="checkbox"/>	Autodealing	<input type="checkbox"/>

W dolnej części formularza dostępne są następujące akcje:

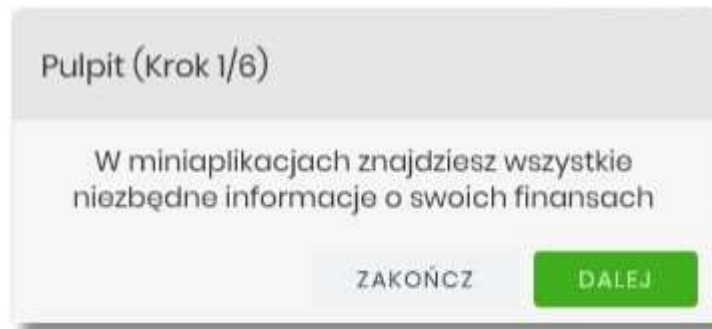
- [ZAPISZ] – pozwala na zapisanie wprowadzonych zmian,
- [ANULUJ] – pozwala na anulowanie wprowadzonych zmian.

## 9.2. Samouczek systemu EBP

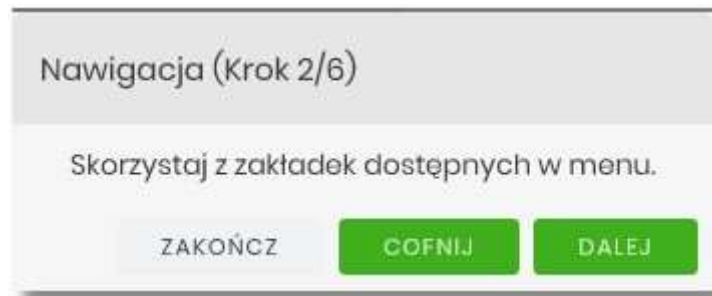


Po wyborze ikony  znajdującej się na pulpicie głównym, system zaprezentuje użytkownikowi w sześciu krokach (na sześciu ekranach), informację na temat parametryzacji oraz ustawień indywidualnych systemu EBP:

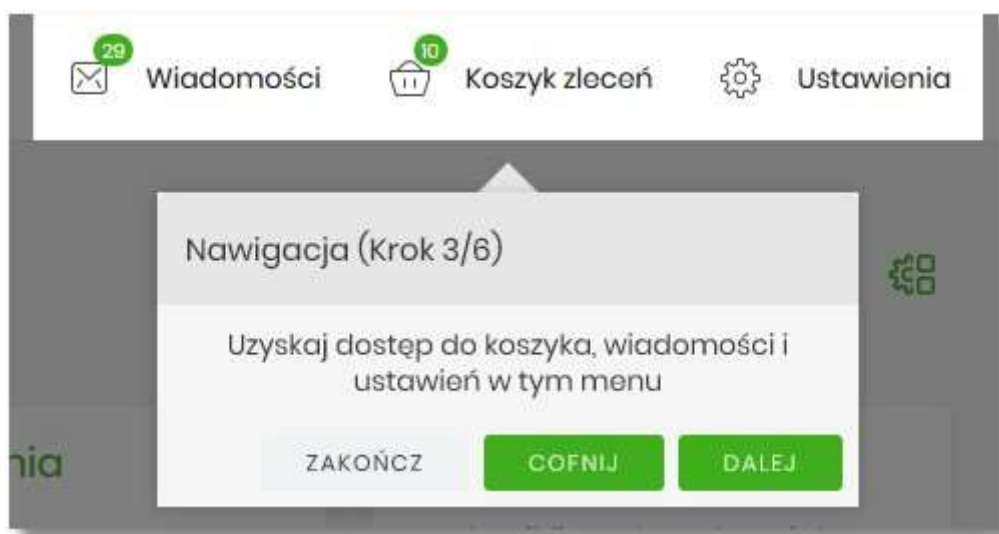
- krok 1



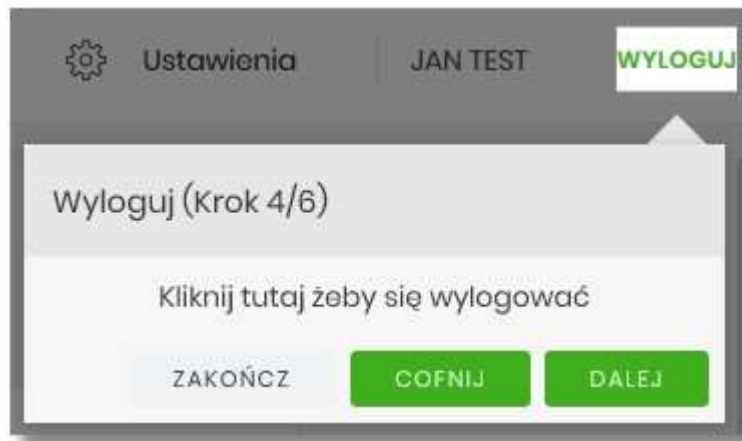
- krok 2



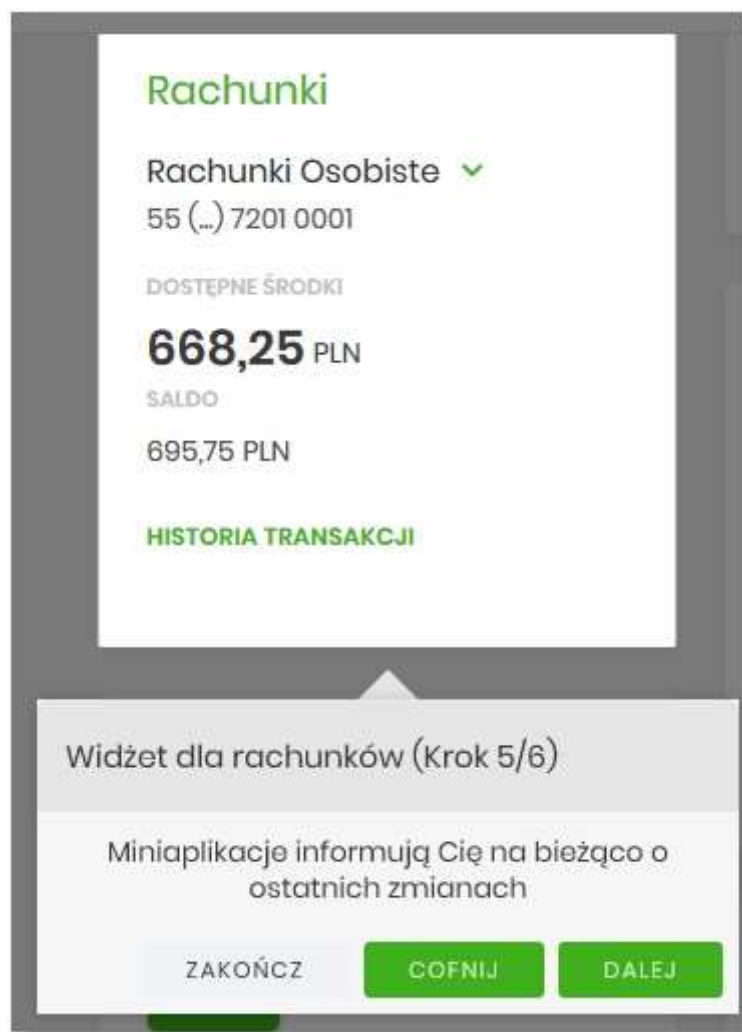
- krok 3



- krok 4

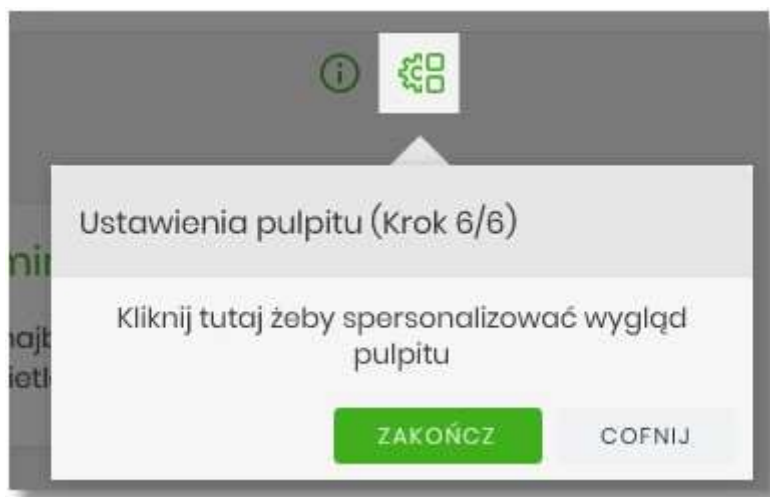


- krok 5



- krok 6





Aby przejść pomiędzy kolejnymi krokami, użytkownik ma do dyspozycji następujące przyciski:

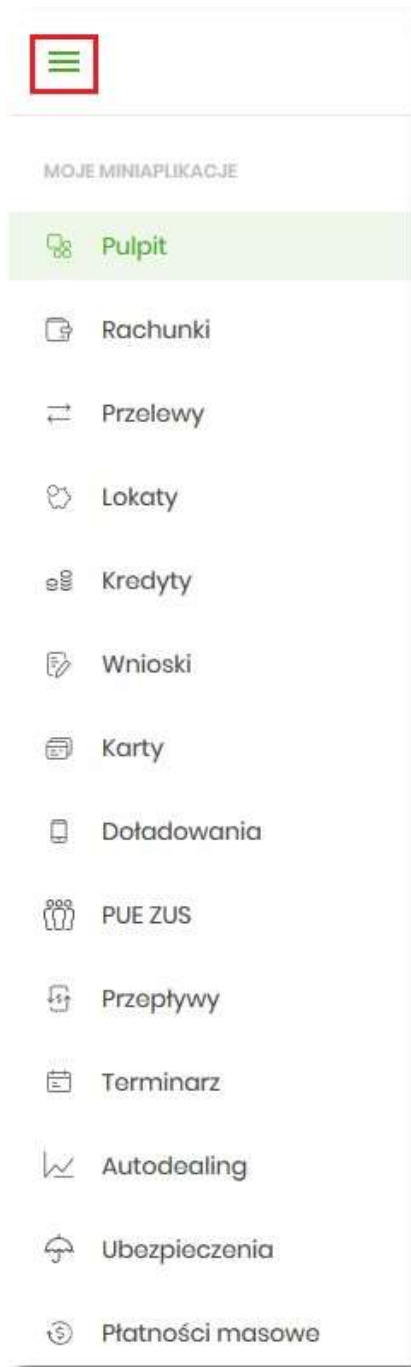
- [ZAKOŃCZ] – naciśnięcie powoduje wyjście z samouczka,
- [COFNIJ] – następuje cofnięcie do wcześniejszego kroku,
- [DALEJ] – następuje przejście do kolejnego kroku.

### 9.3. Widok Moje miniaplikacje

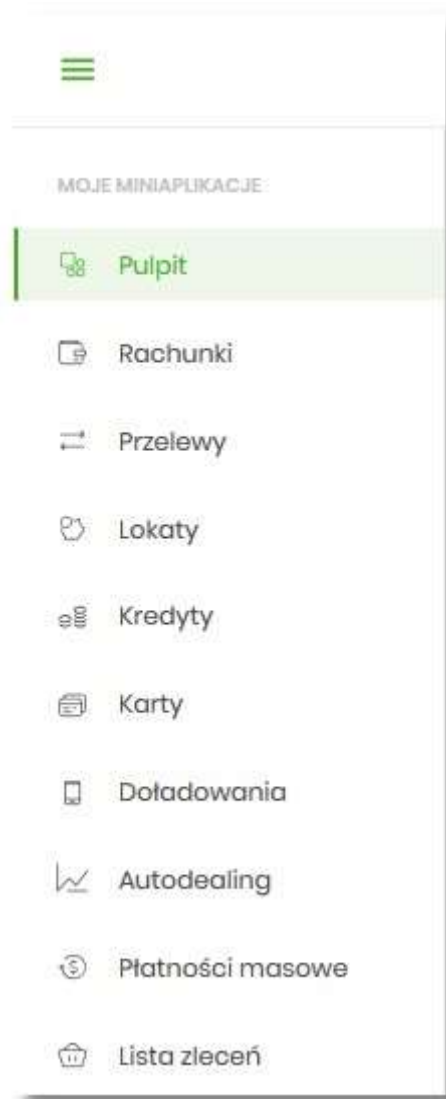
Widok *MOJE MINIAPLIKACJE* obejmuje wszystkie miniaplikacje dostępne dla użytkownika. Na widoczność opcji prezentowanych w menu ma także wpływ aktualnie wybrany kontekst. Kolejność miniaplikacji ustalona dla widoku uwzględnia znaczenie biznesowe miniaplikacji.

Dostępność miniaplikacji w *MOJE MINIAPLIKACJE*, jest uzależniona od tego w jakim kontekście (indywidualnym, firmowym) użytkownik jest zalogowany do systemu EBP.

*MOJE MINIAPLIKACJE* w kontekście indywidualnym:



MOJE MINIAPLIKACJE w kontekście firmowym:



Wybranie konkretnej miniaplikacji na liście powoduje przejście do widoku głównego tej miniaplikacji.

Użytkownik może zamknąć (ukryć) menu boczne poprzez użycie ikony .

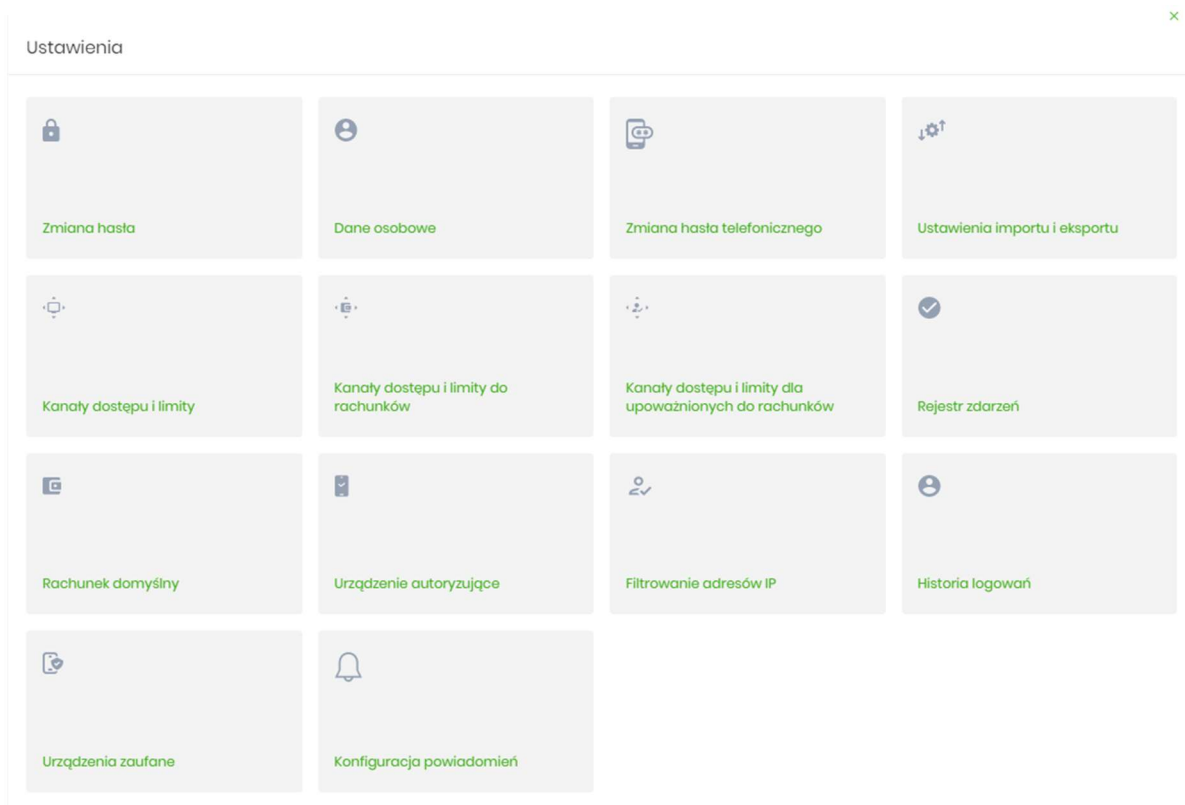
## Rozdział 10. Zarządzanie ustawieniami

Do zarządzania ustawieniami systemu służy opcja *Ustawienia*, dostępna na pulpicie głównym w górnym pasku menu. Wybranie tej opcji powoduje wyświetlenie opcji pozwalającej na konfigurację ustawień. Dostępność opcji dla użytkownika jest uzależniona od kontekstu w jakim pracuje (indywidualny, firmowym) oraz uprawnień które posiada.



Wybranie tej opcji powoduje wyświetlenie zestawu kafli dotyczących konfiguracji ustawień:

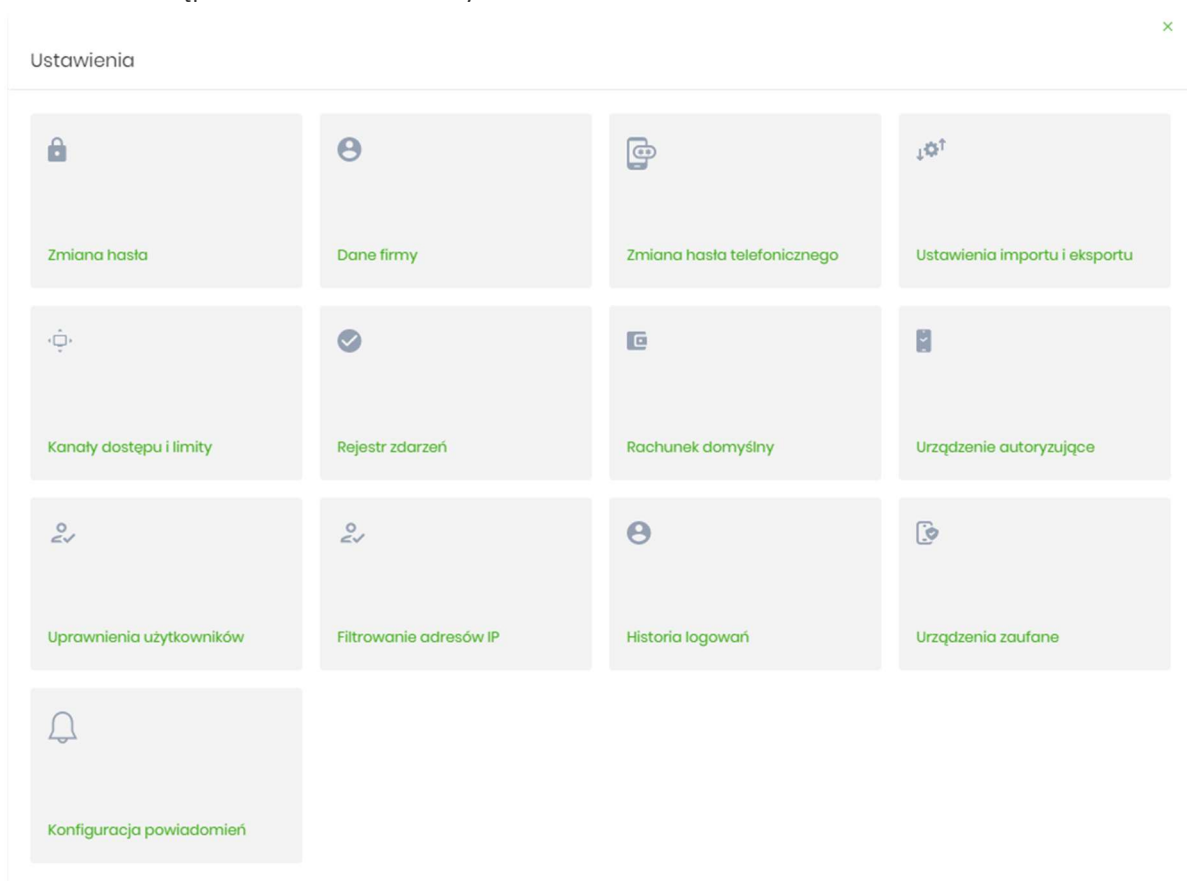
Ustawienia dostępne w kontekście indywidualnym:



- Zmiana hasła do logowania – umożliwia zmianę kodu dostępu do logowania,
- Dane osobowe – umożliwia wyświetlenie danych osobowych zalogowanego użytkownika,
- Zmiana hasła telefonicznego - umożliwia zmianę hasła do obsługi telefonicznej,
- Ustawienia importu i eksportu – umożliwia ustawienie formatu importowanych przelewów/szablonów z danymi odbiorców oraz eksportu historii operacji,
- Kanały dostępu do systemu – umożliwia wyświetlenie limitów dla kanałów, edycję limitów, zablokowanie kanałów oraz odblokowanie kanału,
- Kanały dostępu i limity do rachunków – umożliwia wyświetlenie limitów dla kanałów, edycję limitów, zablokowanie kanałów do rachunków,
- Kanały dostępu i limity dla upoważnionych do rachunków – umożliwia wyświetlenie limitów dla kanałów, zablokowanie kanałów dla upoważnionych do rachunków,

- Rejestr zdarzeń – zapis akcji użytkownika,
- Rachunek domyślny – ustawienie rachunku domyślnego w systemie,
- Urządzenie autoryzujące – kafel widoczny dla użytkownika, który ma przypisaną autoryzację mobilną (podpis niekwalifikowany) za pomocą aplikacji mToken MAA. Umożliwia:
  - sparowanie urządzenia autoryzującego z systemem EBP,
  - podgląd listy urządzeń przypisanych do użytkownika (sparowanego z systemem EBP),
  - usunięcie urządzenia autoryzującego.
- Filtrowanie adresów IP – umożliwia definicję adresów IP z których użytkownik może/nie może logować się do systemu EBP,
- Historia logowań – historia poprawnych/niepoprawnych logowań użytkownika do systemu EBP.
- Urządzenia zaufane – umożliwia podgląd listy dodanych urządzeń zaufanych oraz usunięcie urządzenia zaufanego.
- Konfiguracja powiadomień – umożliwia włączenie i konfigurację powiadomień.

Ustawienia dostępne w kontekście firmowym:



- Zmiana hasła do logowania – umożliwia zmianę kodu dostępu do logowania,
- Dane firmy – umożliwia wyświetlenie danych firmy,
- Zmiana hasła telefonicznego - umożliwia zmianę hasła do obsługi telefonicznej,

- Ustawienia importu i eksportu – umożliwia ustawienie formatu importowanych przelewów/szablonów z danymi odbiorców oraz eksportu historii operacji,
- Kanały dostępu do systemu – umożliwia wyświetlenie limitów dla kanałów, edycję limitów, zablokowanie kanałów oraz odblokowanie kanału,
- Rejestr zdarzeń – zapis akcji użytkownika,
- Rachunek domyślny – ustawienie rachunku domyślnego w systemie,
- Urządzenie autoryzujące – kafel widoczny dla użytkownika, który ma przypisaną autoryzację mobilną (podpis niekwalifikowany) za pomocą aplikacji mToken MAA. Umożliwia:
  - sparowanie urządzenia autoryzującego z systemem EBP,
  - podgląd urządzenia przypisanego do użytkownika (sparowanego z systemem EBP),
  - usunięcie urządzenia autoryzującego.
- Uprawnienia użytkowników – uprawnienia dla użytkowników: funkcjonalne i do rachunków,
- Filtrowanie adresów IP – umożliwia definicję adresów IP z których użytkownik może/nie może logować się do systemu EBP,
- Urządzenia zaufane – umożliwia podgląd listy dodanych urządzeń zaufanych oraz usunięcie urządzenia zaufanego.
- Historia logowań – historia poprawnych/niepoprawnych logowań użytkownika do systemu EBP,

## 10.1. Zmiana hasła dostępu do systemu

Operację zmiany kodu dostępu użytkownik może przeprowadzić z opcji *Ustawienia* → *Zmiana hasła*, opcja ta jest dostępna tylko dla użytkownika logującego się do systemu za pomocą:

- hasła maskowanego + kodu SMS,
- aplikacji mobilnej.

Po uruchomieniu opcji system wyświetla formularz do ustalenia nowego kodu dostępu wraz z warunkami jakie musi spełniać hasło (wygląd ekranu jest uzależniony od posiadanej przez użytkownika metody logowania).

< Zmiana hasła do logowania x

Zadbaj o zachowanie poufności swojego hasła.  
Nie udostępniaj hasła innym osobom, na zewnętrznych stronach internetowych, poczcie elektronicznej, wiadomością SMS lub w odpowiedzi na zapytania otrzymane od pracowników banku.  
Definiując swoje hasło pamiętaj o zachowaniu zasad bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

Zasady budowy haseł są następujące:

- musi składać się z 10-25 znaków
- musi zawierać przynajmniej jedną małą literę

Obecne hasło

1 2 3 4 5 6 7 8

9 10 11 12

Nowe hasło

Powtórz nowe hasło

ZATWIERDZ

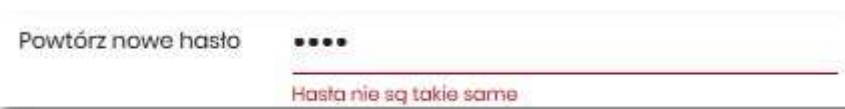
System pobiera z Serwera Autoryzacji metodę uwierzytelnienia użytkownika i aktualną jej konfigurację. W oknie do zmiany hasła należy wprowadzić dotychczasowy klucz uwierzytelniający zgodny z metodą uwierzytelnienia (**Obecne hasło**) oraz dwukrotnie nowe hasło (**Nowe hasło, Powtórz nowe hasło**).

W przypadku gdy nowe hasło nie spełnia wymogów polityki bezpieczeństwa, system zaprezentuje następujący komunikat: *Hasło nie spełnia wymogów polityki bezpieczeństwa*.



The screenshot shows a form with a label "Nowe hasło" and a password input field containing ten black dots. Below the input field, a red error message reads "Hasło nie spełnia wymogów polityki bezpieczeństwa".

Wprowadzone hasło w polach Nowe hasło oraz Powtórz nowe hasło, muszą być jednakowe. W przypadku, gdy w polach wprowadzono dwa różne hasła, system wyświetla komunikat: *Hasła nie są takie same*, uniemożliwiając tym samym zakończenie procesu zmiany hasła.





The screenshot shows a form with a label "Powtórz nowe hasło" and a password input field containing four black dots. Below the input field, a red error message reads "Hasła nie są takie same".

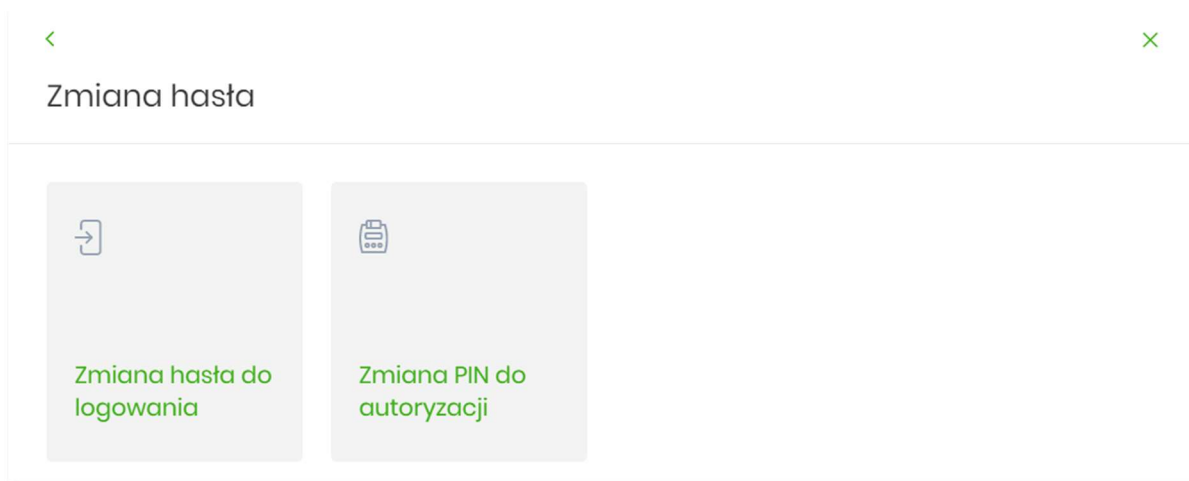
Po poprawnym wypełnieniu formularza, zmiany należy zaakceptować za pomocą przycisku [ZATWIERDŹ].



W górnej części formularza ZMIANA HASŁA DO LOGOWANIA znajdują się przyciski:

-  – umożliwiający powrót do formularza USTAWIENIA,
-  – umożliwiający przejście do głównego menu.

W przypadku metody logowania za pomocą hasła maskowanego + kodu SMS, dodatkowo w opcji *Ustawienia* → *Zmiana hasła*, dostępna jest opcja *Zmiana PIN do autoryzacji*, w której użytkownik ma możliwość zmiany PIN do autoryzacji.



Po wyborze opcji *Zmiana PIN do autoryzacji*, system prezentuje formularz ZMIANA PIN DO AUTORYZACJI, na którym użytkownik ma możliwość zmiany PINu.

Zadbaj o zachowanie poufności swojego PIN.

- Nie udostępniaj PIN innym osobom, na żadnych stronach internetowych, pocztą elektroniczną, wiadomością SMS lub w odpowiedzi na ządania otrzymane od pracowników banku.
- Definiując swój PIN pamiętaj o zachowaniu zasad bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

Zasady budowy PIN są następujące:

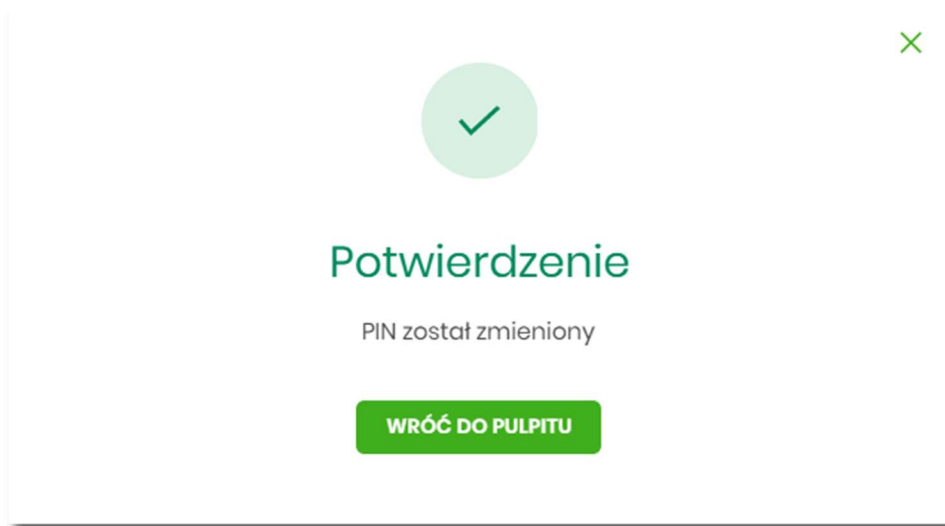
- musi składać się z 4-8 znaków
- musi zawierać przynajmniej jedną wielką literę
- musi zawierać przynajmniej jedną małą literę
- musi zawierać przynajmniej jeden znak specjalny
- musi zawierać przynajmniej jedną cyfrę
- może zawierać wyłącznie znaki ze zbioru: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!@#\$%^&\*()-\_+[]\|:;\"/>

Na formularzy ZMIANA PIN DO AUTORYZACJI dostępne są:

- parametry:
  - Obecny PIN – użytkownik wprowadza obecny PIN,
  - Nowy PIN – użytkownik wprowadza nowy PIN,
  - Powtórz nowe PIN – użytkownik ponownie wprowadza nowy PIN,
- akcja:
  - [ZATWIERDŹ] – umożliwiająca zatwierdzenie zmiany hasła.

Po wprowadzeniu nowego hasła i naciśnięciu przycisku [ZATWIERDŹ] system zmienia hasło i prezentuje komunikat o poprawnym wykonaniu operacji.





Dla użytkownika logującego się do systemu za pomocą karty mikroprocesorowej opcja *Ustawienia* → *Zmiana hasła* jest niedostępna. Użytkownik ma możliwość zmiany hasła, tylko w aplikacji SCSA. Po uruchomieniu zmiany hasła w systemie SCSA, system prezentuje następujący ekran

A screenshot of a Windows-style dialog box titled 'Zmiana kodu PIN'. The dialog has a white background and a grey border. It contains three text input fields stacked vertically. The first field is labeled 'Stary kod PIN:', the second 'Nowy kod PIN:', and the third 'Powtórz kod PIN:'. Below the input fields is a grey button with the text 'Zmień'. The dialog also features standard window control buttons (minimize, maximize, close) in the top right corner.

Na formularzy ZMIANA KODU PIN dostępne są:

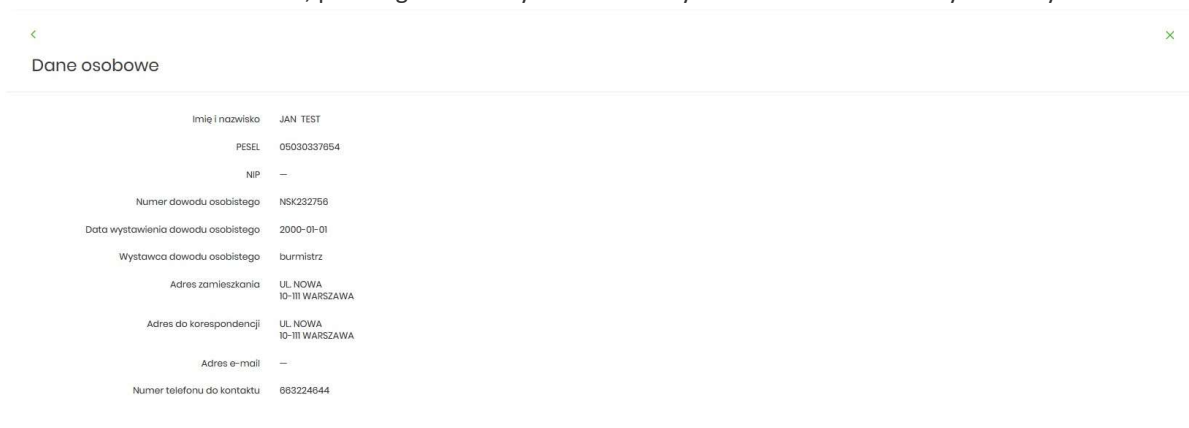
- parametry:
  - Stary kod PIN – użytkownik wprowadza obecny kod PIN,
  - Nowy kod PIN – użytkownik wprowadza nowy kod PIN,
  - Powtórz kod PIN – użytkownik ponownie wprowadza nowy kod PIN,
- akcja:
  - [ZMIENŃ] – umożliwiająca zatwierdzenie zmiany kodu PIN.

Po poprawnym wprowadzeniu kodu PIN i naciśnięciu [ZMIENŃ] system zmienia kod PIN.

## 10.2. Dane osobowe/Dane firmy

W opcji *Ustawienia* w zależności od kontekstu w jakim użytkownik jest zalogowany do systemu EBP, zostaną wyświetlone ale *Dane osobowe* albo *Dane firmy*. Użytkownik ma możliwość wyświetlenia (w trybie podglądu) danych osobowych albo danych firmy.

Formularz DANE OSOBOWE, po zalogowaniu użytkownika do systemu w kontekście indywidualnym

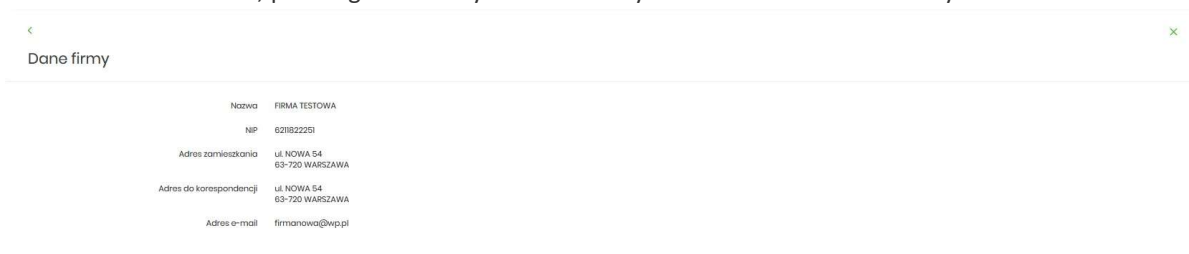


Imię i nazwisko	JAN TEST
PESEL	05030337854
NIP	—
Numer dowodu osobistego	NSK232758
Data wystawienia dowodu osobistego	2000-01-01
Wystawca dowodu osobistego	burmistrz
Adres zamieszkania	UL. NOWA 10-111 WARSZAWA
Adres do korespondencji	UL. NOWA 10-111 WARSZAWA
Adres e-mail	—
Numer telefonu do kontaktu	663224644

Na formularzu widoczne są następujące dane użytkownika:

- Imię i nazwisko,
- PESEL,
- NIP – Numer Identyfikacji Podatkowej, • Numer dowodu osobistego,
- Data wystawienia dowodu osobistego,
- Wystawca dowodu osobistego,
- Adres zamieszkania – w układzie 3 linii (w jednej linii kod pocztowy oraz miejscowość),
- Adres do korespondencji – w układzie 3 linii (w jednej linii kod pocztowy oraz miejscowość),
- Adres e-mail – adres e-mail,
- Numer telefonu do kontaktu – bez dodatkowego formatowania/prezentacja w formacie zapisanym.

Formularz DANE FIRMY, po zalogowaniu użytkownika do systemu w kontekście firmowym



Nazwa	FIRMA TESTOWA
NIP	621822251
Adres zamieszkania	UL. NOWA 54 63-720 WARSZAWA
Adres do korespondencji	UL. NOWA 54 63-720 WARSZAWA
Adres e-mail	firmanowa@vpp.pl

Na formularzu widoczne są następujące dane użytkownika:

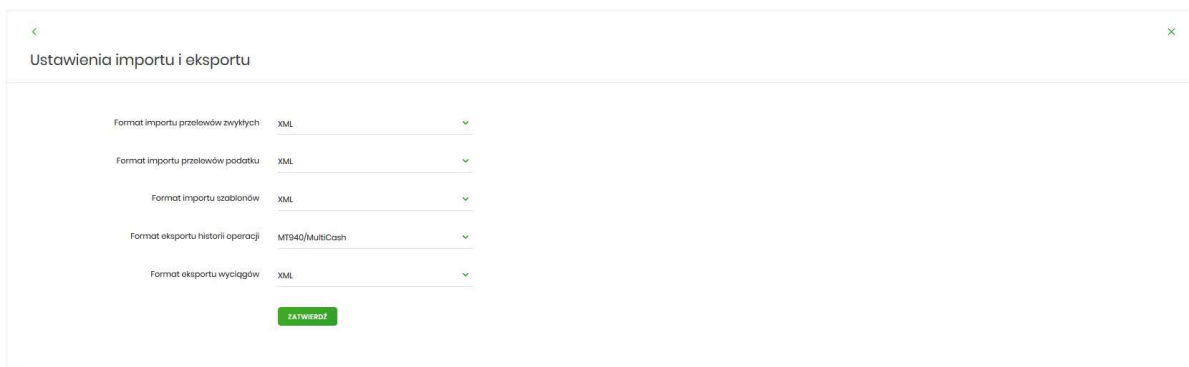
- Nazwa – nazwa firmy,
- NIP – Numer Identyfikacji Podatkowej,

- Adres zamieszkania – w układzie 3 linii (w jednej linii kod pocztowy oraz miejscowość),
- Adres do korespondencji – w układzie 3 linii (w jednej linii kod pocztowy oraz miejscowość),
- Adres e-mail – adres e-mail.

### 10.3. Ustawienia importu i eksportu

W opcji *Ustawienia* → *Ustawienia importu i eksportu* użytkownik ma możliwość wyboru formatu importu/eksportu danych oraz wczytania struktur plików dla formatów liniowych. Formaty importu/eksportu danych w EBP (w tym schemat dla formatu liniowego) konfigurowane są w kontekście każdego użytkownika osobno. Jeżeli dwóch lub więcej użytkowników będzie miało dostęp do kilku różnych rachunków należących do kilku różnych użytkowników, to format importu będzie określany wg zalogowanego użytkownika.

Formularz USTAWIENIA IMPORTU I EKSPORTU, po zalogowaniu użytkownika do systemu w kontekście indywidualnym



Na formularzu użytkownik ma możliwość ustawienia formatu dla:

- importu przelewów zwykłych,
- importu przelewów podatku,
- importu szablonów,
- eksportu historii operacji,
- eksportu wyciągów.

Formularz USTAWIENIA IMPORTU I EKSPORTU, po zalogowaniu użytkownika do systemu w kontekście firmowym

Na formularzu użytkownik ma możliwość ustawienia formatu dla:

- importu przelewów zwykłych,
- importu przelewów podatku,
- importu szablonów,
- eksportu historii operacji, • eksportu statusów przelewów,
- eksportu wyciągów.

W górnej części formularza USTAWIENIA IMPORTU I EKSPORTU znajdują się przyciski:



•

– umożliwiający powrót do formularza USTAWIENIA,



•

– umożliwiający przejście do głównego menu.

Dla formatów liniowych aplikacja umożliwia określenie struktury plików poprzez import pliku w formacie standardowego opisu używanego przez administratora Źródeł Danych ODBC w systemach Windows (plik `schema.ini`).

Wszystkie dostępne w aplikacji formaty to:

- XML,
- Elixir,
- Liniowy,
- VideoTel,
- Telekonto,

- MT940,
- MT940/MultiCash,
- CSV.

Przy każdej pozycji importu wyświetlone są dostępne formaty dla danego typu. Domyślnie prezentowany jest format XML.

Dla poszczególnych importów oraz eksportów dostępne są następujące formaty:

- import przelewów zwykłych – XML, Elixir, Liniowy, Telekonto, VideoTel,
- import przelewów podatku – XML, Elixir, Liniowy,
- import szablonów – XML, Liniowy, Telekonto,
- eksport historii operacji – XML, Liniowy, MT940, MT940/MultiCash, CSV,
- eksportu statusów przelewów – XML, Liniowy, CSV,
- eksportu wyciągów – XML, Liniowy, MT940, MT940/MultiCash, CSV.

Po wybraniu formatu importu/eksportu zmiany należy zapisać za pomocą przycisku [ZATWIERDŹ].

ZATWIERDŹ

### 10.3.1. Import opisu struktury

W przypadku ustawienia formatu importu/eksportu na wartość Liniowy konieczne jest zaimportowanie pliku z zapisaną strukturą formatu schema.ini.

W tym celu należy:

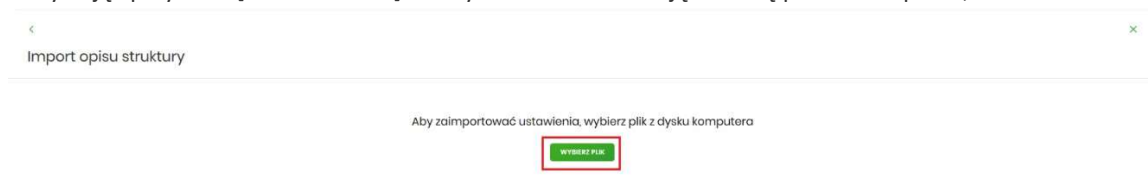
- kliknąć w przycisk [IMPORT STRUKTURY].



Format importu przelewów podatku Liniowy

IMPORT STRUKTURY

- używając przycisku [WYBIERZ PLIK] należy wskazać lokalizację i nazwę pliku do importu,

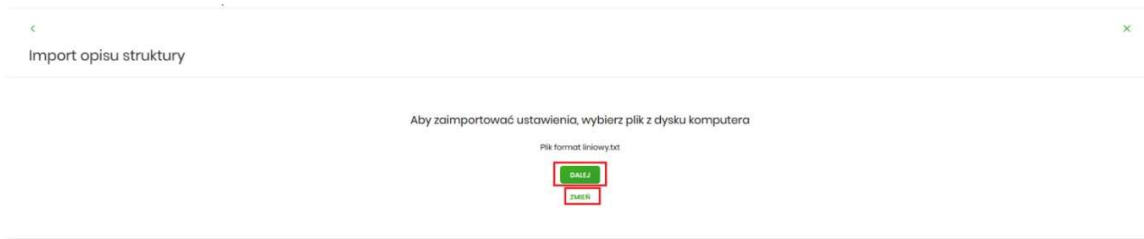


Import opisu struktury

Aby zaimportować ustawienia, wybierz plik z dysku komputera

WYBIERZ PLIK

- uruchomić import przyciskiem [DALEJ], odnośnik [ZMIENŃ] umożliwia zmianę wcześniej wybranego pliku importu,



Po poprawnym zaimportowaniu struktury zostanie zaprezentowany komunikat *Opis struktury został zaimportowany*.



Dla poprawnie zaimportowanej struktury liniowej, na formularzu USTAWIENIA IMPORTU I EKSPORTU dostępne są następujące akcje:



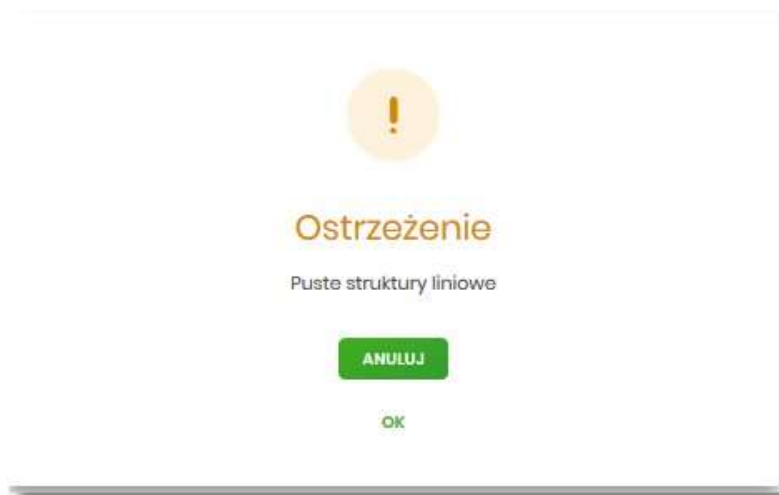
- [IMPORT STRUKTURY] – służy do zacytowania (zmiany) pliku opisującego strukturę danych,
- [POKAŹ STRUKTURĘ] – służy do obejrzenia zacytowanej struktury,
- [USUŃ STRUKTURĘ] – usuwa zacytowaną strukturę z bazy danych.

Przycisk [ZATWIERDŹ] na formularzu USTAWIENIA IMPORTU I EKSPORTU zapisuje bieżące ustawienia.

W przypadku wyboru pliku z błędnym formatem system zaprezentuje komunikat o błędzie i nie pozwoli na przejście dalej.



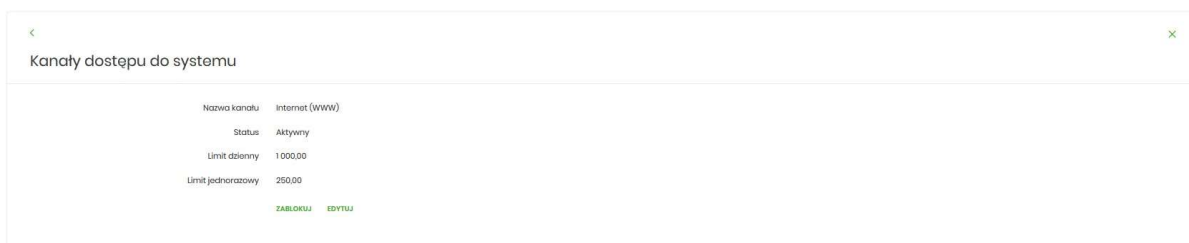
W sytuacji gdy struktura liniowa nie zostanie zaimportowana, w momencie zapisu ustawień (przycisk [ZATWIERDŹ]) prezentowane jest ostrzeżenie: *Puste struktury liniowe*.



## 10.4. Kanały dostępu do systemu

W opcji *Ustawienia* → *Kanały dostępu do systemu* użytkownik ma możliwość:

- wyświetlenia limitów dla kanałów,
- edycji limitów,
- zablokowania kanału.



Na formularzu KANAŁY DOSTĘPU DO SYSTEMU system prezentuje:

- informacje:
  - Nazwa kanału – nazwa kanału,
  - Status – status kanału,
  - Limit dzienny – kwota wraz z walutą limitu dziennego,
  - Limit jednorazowy – kwota wraz z walutą limitu jednorazowego,
- przyciski:
  - [ZABLOKUJ] – umożliwiający zablokowanie kanału Internet (WWW),
  - [EDYTUJ] – umożliwiający zmianę limitów dla kanału Internet (WWW).

W górnej części formularza KANAŁY DOSTĘPU DO SYSTEMU znajdują się przyciski:



- – umożliwiający powrót do formularza USTAWIENIA,



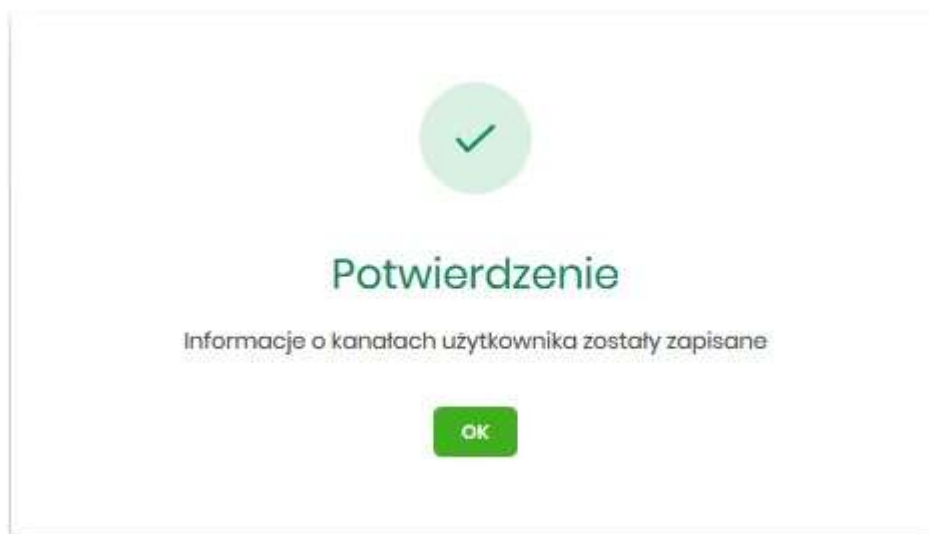
- – umożliwiający przejście do głównego menu.

### 10.4.1. Zablokowanie kanału Internet (WWW) dla systemu

W celu zablokowania kanału Internet (WWW) należy wybrać przycisk [ZABLOKUJ] na formularzu KANAŁY DOSTĘPU DO SYSTEMU. Po naciśnięciu przycisku zostanie zaprezentowany formularz potwierdzający zmianę statusu kanału dostępu, na którym należy wprowadzić poprawne dane autoryzacyjne oraz zatwierdzić naciskając przycisk [AKCEPTUJ], za pomocą dostępnej metody autoryzacji.

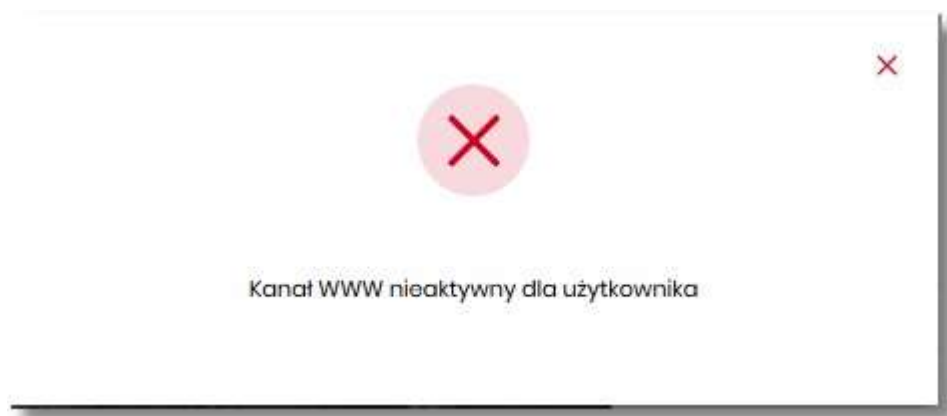
Nazwa kanału	Internet (WWW)
Status	Aktywny
Limit dzienny	1 000,00
Limit jednorazowy	250,00
Podaj kod autoryzacyjny:	<input type="text" value="Wpisz kod"/>
Operacja nr 1 z dnia 31.01.2020	
<input type="button" value="ZAPISZ"/>	

Po poprawnej autoryzacji i naciśnięciu przycisku [ZAPISZ], system prezentuje następujący komunikat:





Po zablokowaniu Internet (WWW), system automatycznie wylogowuje użytkownika z systemu EBP, przy próbie zalogowania się do systemu EBP z zablokowanym kanałem Internet (WWW), po poprawnym wprowadzeniu danych autoryzacyjnych system prezentuje następujący komunikat:



Odblokowanie kanału Internet (WWW) odbywa się przez pracownika banku.

## 10.5. Zmiana limitów dla kanału Internet (WWW)

W celu zmiany limitów dla kanału Internet (WWW) (limit dzienny i limit jednorazowy) na formularzu KANAŁY DOSTĘPU DO SYSTEMU, należy wybrać przycisk [EDYCJA].

Na formularzu system prezentuje:

- pola:
  - Nazwa kanału – nazwa kanału pole zablokowane do edycji,
  - Limit dzienny – pole do zmiany limitu dziennego, ◦ Limit jednorazowy – pole do zmiany limitu jednorazowego,
- przycisk:
  - [AKCEPTUJ] – pozwalająca na zatwierdzenie wprowadzonej zmiany limitów.

Po naciśnięciu przycisku [AKCEPTUJ], system przechodzi na formularz w którym użytkownik musi zatwierdzić zmianę limitów za pomocą dostępnej metody autoryzacji.

<
×

Kanały dostępu do systemu

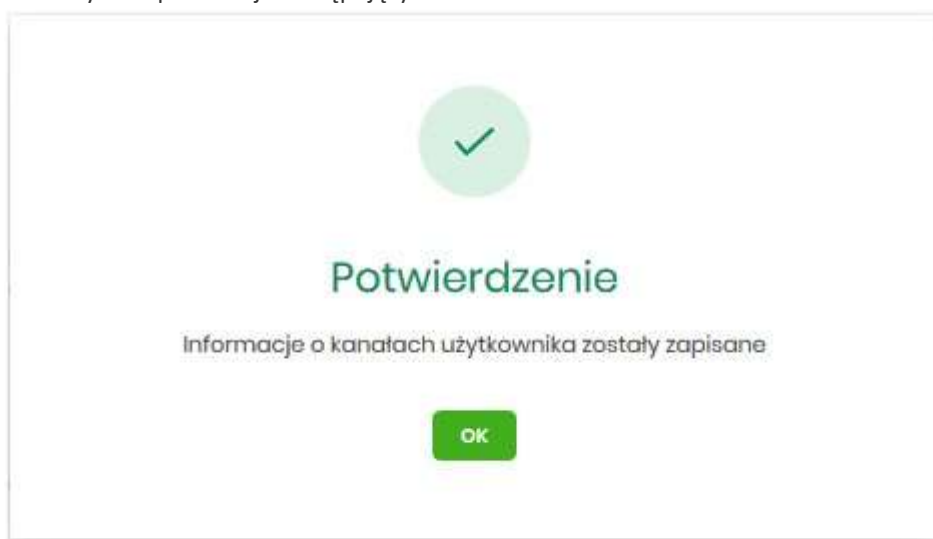
---

Nazwa kanału	Internet (WWW)
Status	Aktywny
Limit dzienny	2000,00 PLN
Limit jednorazowy	250,00 PLN
Podaj kod autoryzacyjny:	Wpisz kod

Operacja nr 1 z dnia 31.01.2020

ZAPISZ

Po zatwierdzeniu system prezentuje następujący komunikat:



## 10.6. Kanały dostępu i limity do rachunków

W opcji *Ustawienia* → *Kanały dostępu i limity do rachunków*, użytkownik ma możliwość:

- wyboru rachunku (z lity dostępnych dla użytkownika), dla którego chce wyświetlić limity dla kanału,
- wyświetlenia limitów dla kanału Internet (WWW),
- edycji limitów Internet (WWW),
- zablokowania kanałów do rachunków,
- odblokowanie kanałów do rachunków.

<
×

Kanały dostępu i limity do rachunków

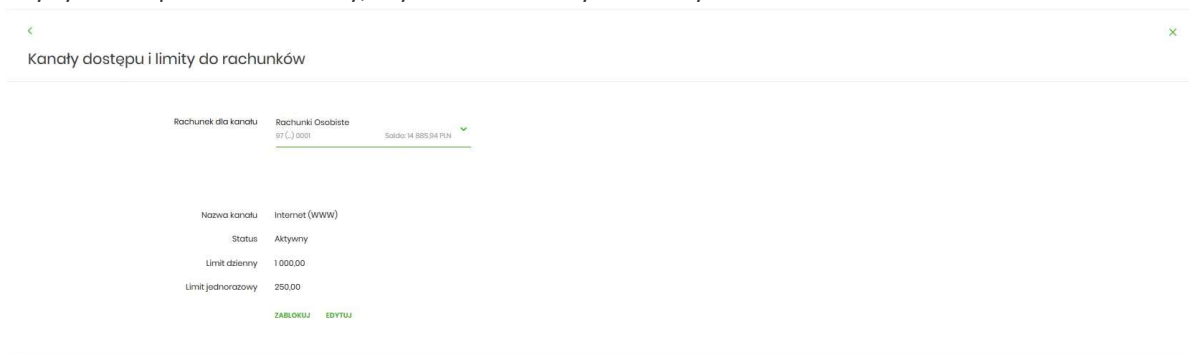
---

Rachunek dla kanału Wybierz ▼

🔍

Brak kanałów do wyświetlenia

Aby system zaprezentował limity, użytkownik musi wybrać z listy rachunek.



Rachunek dla kanału	Rachunki Osobiste 97 (...) 0001	Saldo: 14 885,94 PLN
Nazwa kanału	Internet (WWW)	
Status	Aktywny	
Limit dzienny	1 000,00	
Limit jednorazowy	250,00	
	ZABLOKUJ	EDYTUJ

Po wskazaniu rachunku na formularzu KANAŁY DOSTĘPU I LIMITY DO RACHUNKÓW system prezentuje:

- informacje:
  - Rachunek dla kanału – wskazany numer rachunku częściowo zamaskowany wraz z saldem,
  - Nazwa kanału – nazwa kanału,
  - Status – status kanału,
  - Limit dzienny – kwota wraz z walutą limitu dziennego, ◦ Limit jednorazowy – kwota wraz z walutą limitu jednorazowego,
- przyciski:
  - [ZABLOKUJ] lub [ODBLOKUJ] – umożliwiający zablokowanie, odblokowanie kanału Internet (WWW) dla rachunku,
  - [EDYTUJ] – umożliwiający zmianę limitów dla kanału Internet (WWW).

W górnej części formularza KANAŁY DOSTĘPU I LIMITY DO RACHUNKÓW znajdują się przyciski:



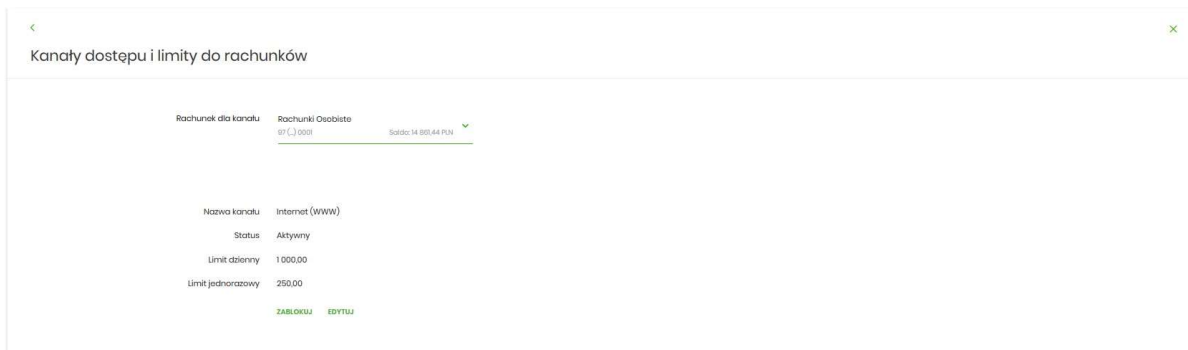
- – umożliwiający powrót do formularza USTAWIENIA,



- – umożliwiający przejście do głównego menu.

### 10.6.1. Zablokowanie kanału Internet (WWW) dla rachunku

W celu zablokowania kanału Internet (WWW) dla rachunku, należy wybrać przycisk [ZABLOKUJ] na formularzu KANAŁY DOSTĘPU I LIMITY DO RACHUNKÓW.



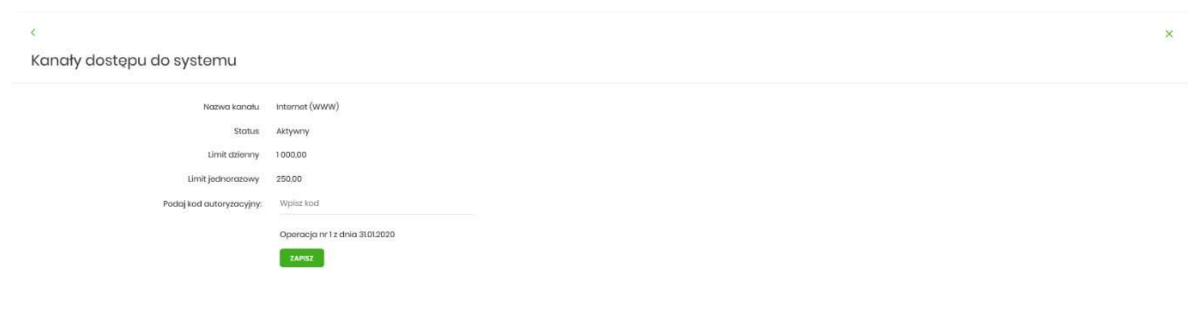
Kanały dostępu i limity do rachunków

Rachunek dla kanału: Rachunki Osobiste  
01.03.2020 Saldo: 14 885,44 PLN

Nazwa kanału: Internet (WWW)  
Status: Aktywny  
Limit dzienny: 1 000,00  
Limit jednorazowy: 250,00

ZABLOKUJ EDYTUJ

Po naciśnięciu przycisku zostanie zaprezentowany formularz potwierdzający zmianę statusu kanału dostępu dla rachunku, na którym należy wprowadzić poprawne dane autoryzacyjne oraz zatwierdzić naciskając przycisk [AKCEPTUJ], za pomocą dostępnej metody autoryzacji.



Kanały dostępu do systemu

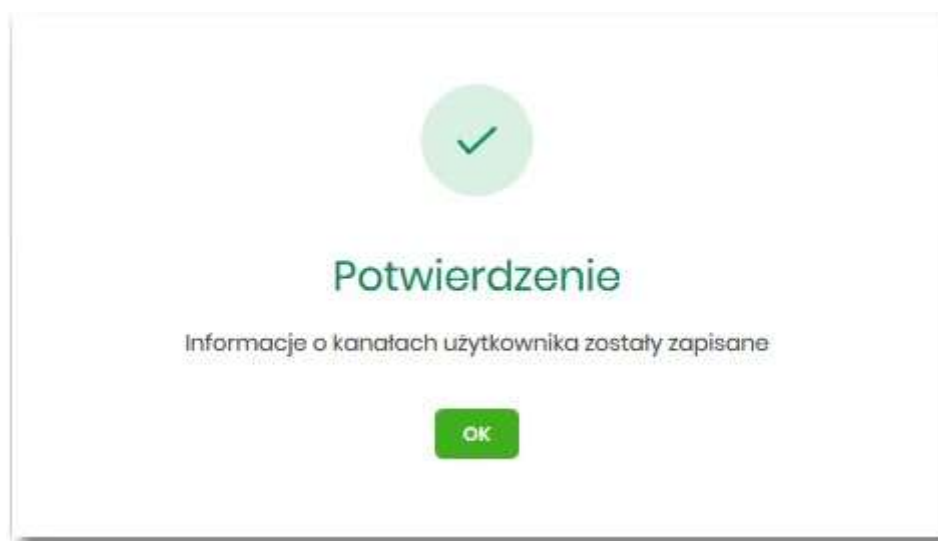
Nazwa kanału: Internet (WWW)  
Status: Aktywny  
Limit dzienny: 1 000,00  
Limit jednorazowy: 250,00

Podaj kod autoryzacyjny: Wpisz kod

Operacja nr 1 z dnia 31.01.2020

ZAPISZ

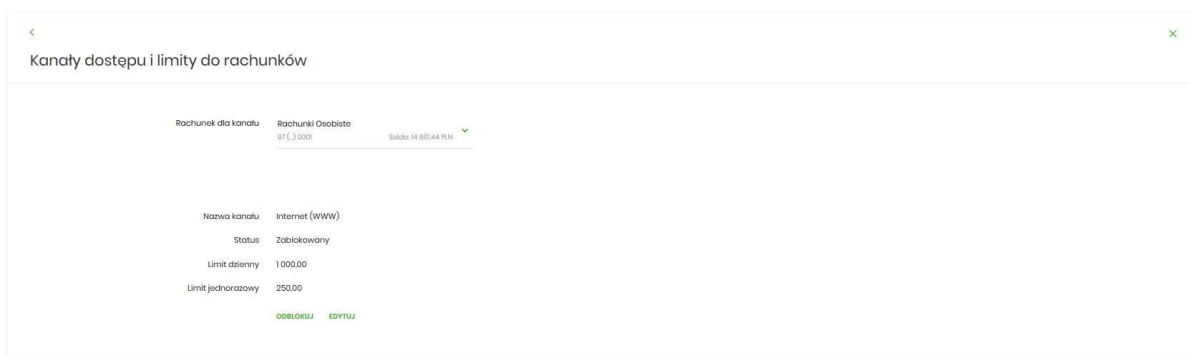
Po poprawnej autoryzacji i naciśnięciu przycisku [ZAPISZ], system prezentuje następujący komunikat:



Po zablokowaniu kanału dla rachunku, nie jest on widoczny na liście rachunków użytkownika w systemie EBP.

### 10.6.2. Odblokowanie kanału Internet (WWW) dla rachunku

W celu odblokowania kanału Internet (WWW) dla rachunku, należy wybrać przycisk [ODBLOKUJ] na formularzu KANAŁY DOSTĘPU I LIMITY DO RACHUNKÓW.



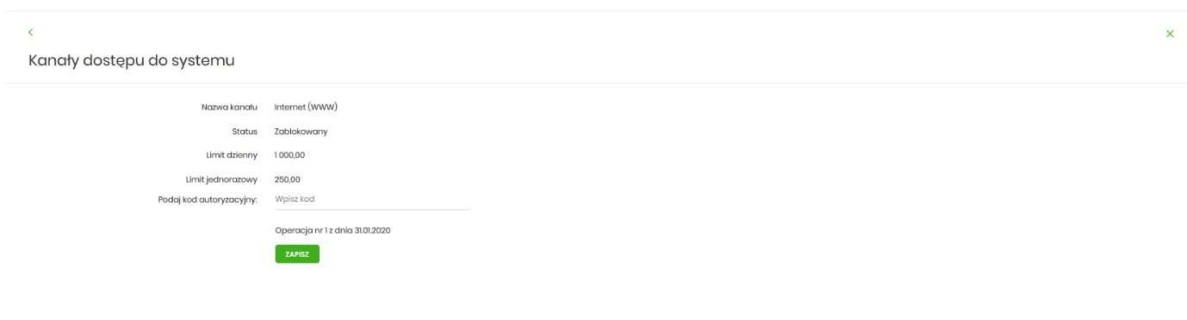
Kanady dostępu i limity do rachunków

Rachunek dla kanału: Rachunki Osobiste  
 07 (...) 0000 Saldo: 14 801.44 PLN

Nazwa kanału: Internet (WWW)  
 Status: Zablokowany  
 Limit dzienny: 1 000.00  
 Limit jednorazowy: 250.00

ODBLOKUJ EDYTUJ

Po naciśnięciu przycisku zostanie zaprezentowany formularz potwierdzający zmianę statusu kanału dostępu dla rachunku, na którym należy wprowadzić poprawne dane autoryzacyjne oraz zatwierdzić naciskając przycisk [AKCEPTUJ], za pomocą dostępnej metody autoryzacji.



Kanady dostępu do systemu

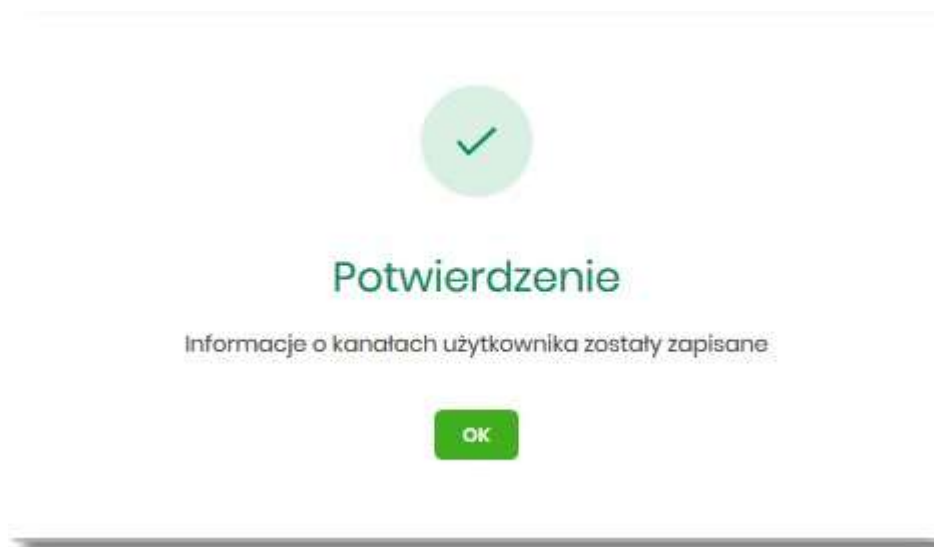
Nazwa kanału: Internet (WWW)  
 Status: Zablokowany  
 Limit dzienny: 1 000.00  
 Limit jednorazowy: 250.00

Podaj kod autoryzacyjny: Wpisz kod

Operacja nr 1 z dnia 31.08.2020

ZAPISZ

Po poprawnej autoryzacji i naciśnięciu przycisku [ZAPISZ], system prezentuje następujący komunikat:



Po odblokowaniu kanału dla rachunku, nie jest on widoczny na liście rachunków użytkownika w systemie EBP.

### 10.6.3. Zmiana limitów dla kanału Internet (WWW)

W celu zmiany limitów (limit dzienny i limit jednorazowy) wybranego rachunku dla kanału Internet (WWW) na formularzu KANAŁY DOSTĘPU I LIMITY DO RACHUNKÓW, należy wybrać przycisk [EDYCJA].

Kanały dostępu do systemu

Nazwa kanału	Internet (WWW)
Status	Aktywny
Limit dzienny	2000.00 PLN
Limit jednorazowy	250 PLN

**AKCEPTUJ**

Na formularzu system prezentuje:

- pola:
  - Nazwa kanału – nazwa kanału pole zablokowane do edycji,
  - Limit dzienny – pole do zmiany limitu dziennego, ◦ Limit jednorazowy – pole do zmiany limitu jednorazowego,
- przycisk:
  - [AKCEPTUJ] – pozwalająca na zatwierdzenie wprowadzonej zmiany limitów.

Po naciśnięciu przycisku [AKCEPTUJ], system przechodzi na formularz w którym użytkownik musi zatwierdzić zmianę limitów za pomocą dostępnej metody autoryzacji.

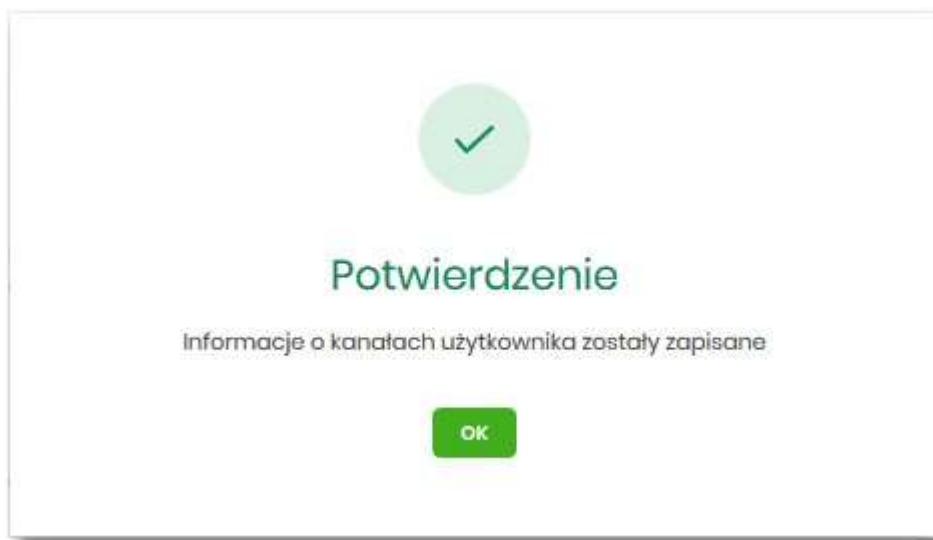
Kanały dostępu do systemu

Nazwa kanału	Internet (WWW)
Status	Aktywny
Limit dzienny	2000.00 PLN
Limit jednorazowy	250.00 PLN
Podaj kod autoryzacyjny:	Wpisz kod

Operacja nr 1 z dnia 31.01.2020

**ZATWIERDZ**

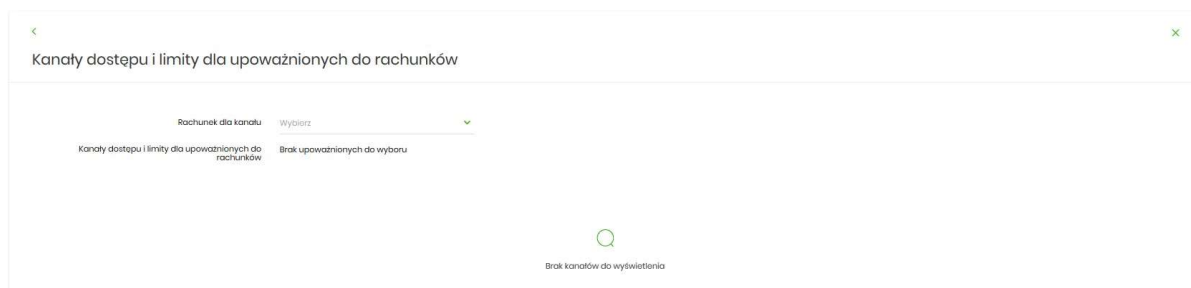
Po zatwierdzeniu system prezentuje następujący komunikat:



## 10.7. Kanały dostępu i limity dla upoważnionych do rachunków

W opcji *Ustawienia* → *Kanały dostępu i limity dla upoważnionych do rachunków*, użytkownik ma możliwość:

- wyboru rachunku (z lity dostępnych dla użytkownika), dla którego chce wyświetlić limity dla kanału,
- wyboru użytkownika (z lity dostępnych użytkowników) upoważnionego do rachunku, dla którego chce wyświetlić limity dla kanału,
- wyświetlenia limitów dla kanału Internet (WWW),
- zablokowania kanałów dla upoważnionych do rachunków,
- odblokowanie kanałów dla upoważnionych do rachunków.



Na formularzu KANAŁY DOSTĘPU I LIMITY DLA UPOWAŻNIONYCH DO RACHUNKÓW, dostępne jest pole:

- Rachunek dla kanału – lista rachunków dostępnych dla użytkownika.

Po wybraniu rachunku system prezentuje pole:

- Kanały dostępu i limity dla upoważnionych do rachunków – lista upoważnionych użytkowników do rachunku

Po wskazaniu rachunku oraz wyborze użytkownika na formularzu KANAŁY DOSTĘPU I LIMITY DLA UPOWAŻNIONYCH DO RACHUNKÓW system prezentuje:

- informacje:

- Rachunek dla kanału – wskazany numer rachunku częściowo zamaskowy wraz z saldem,
- Kanały dostępu i limity dla upoważnionych do rachunków – dane wybranego użytkownika,
- Nazwa kanału – nazwa kanału,
- Status – status kanału,
- Limit dzienny – kwota wraz z walutą limitu dziennego, ◦ Limit jednorazowy – kwota wraz z walutą limitu jednorazowego,

- przyciski:

- [ZABLOKUJ] lub [ODBLOKUJ] – umożliwiający zablokowanie, odblokowanie kanału Internet (WWW) dla rachunku,
- [EDYTUJ] – umożliwiający zmianę limitów dla kanału Internet (WWW).

W górnej części formularza KANAŁY DOSTĘPU I LIMITY DLA UPOWAŻNIONYCH DO RACHUNKÓW znajdują się przyciski:



– umożliwiający powrót do formularza USTAWIENIA,



– umożliwiający przejście do głównego menu.



### 10.7.1. Zablokowanie kanału Internet (WWW) dla rachunku

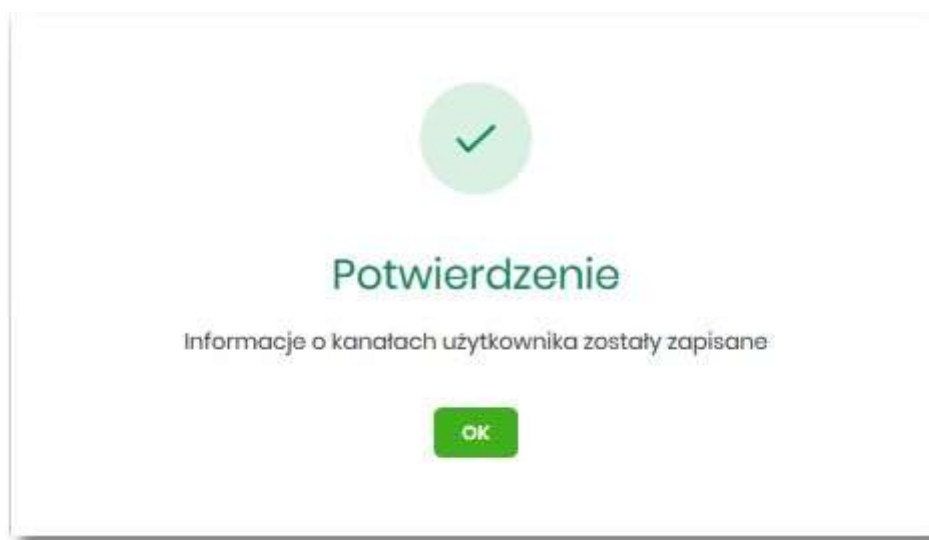
W celu zablokowania kanału Internet (WWW) dla wybranego rachunku i użytkownika, należy wybrać przycisk [ZABLOKUJ] na formularzu KANAŁY DOSTĘPU I LIMITY DLA UPOWAŻNIONYCH DO RACHUNKÓW.

Rachunek dla kanału	Rachunki Osobiste	Saldo: 14 881,64 PLN
Kanały dostępu i limity dla upoważnionych do rachunków	JAN TESTOWY	
Nazwa kanału	Internet (WWW)	
Status	Aktywny	
Limit dzienny	1200,00	
Limit jednorazowy	300,00	
	ZABLOKUJ	EDYTUJ

Po naciśnięciu przycisku zostanie zaprezentowany formularz potwierdzający zmianę statusu kanału dostępu dla wybranego rachunku i użytkownika, na którym należy wprowadzić poprawne dane autoryzacyjne oraz zatwierdzić naciskając przycisk [AKCEPTUJ], za pomocą dostępnej metody autoryzacji.

Nazwa kanału	Internet (WWW)
Status	Aktywny
Limit dzienny	1200,00
Limit jednorazowy	300,00
Podaj kod autoryzacyjny:	Wpisz kod
Operacja nr 1 z dnia 31.01.2020	
ZAPISZ	

Po poprawnej autoryzacji i naciśnięciu przycisku [ZAPISZ], system prezentuje następujący komunikat:



Po zablokowaniu kanału, rachunek nie jest widoczny w systemie EBP liście rachunków dla wskazanego użytkownika.

## 10.7.2. Odblokowanie kanału Internet (WWW) dla rachunku

W celu odblokowania kanału Internet (WWW) dla wybranego rachunku i użytkownika, należy wybrać przycisk [ODBLOKUJ] na formularzu KANAŁY DOSTĘPU I LIMITY DLA UPOWAŻNIONYCH DO RACHUNKÓW.

Kanały dostępu i limity dla upoważnionych do rachunków

Rachunek dla kanału: Rachunki Osobiste  
RIT (L) 0000  
Saldo: 14 883,44 PLN

Kanały dostępu i limity dla upoważnionych do rachunków: JAN TESTOWY

Nazwa kanału: Internet (WWW)  
Status: Zablokowany  
Limit dzienny: 1 200,00  
Limit jednorazowy: 300,00

ODBLOKUJ EDYTUJ

Po naciśnięciu przycisku zostanie zaprezentowany formularz potwierdzający zmianę statusu kanału dostępu dla wybranego rachunku i użytkownika, na którym należy wprowadzić poprawne dane autoryzacyjne oraz zatwierdzić naciskając przycisk [AKCEPTUJ], za pomocą dostępnej metody autoryzacji.

Kanały dostępu do systemu

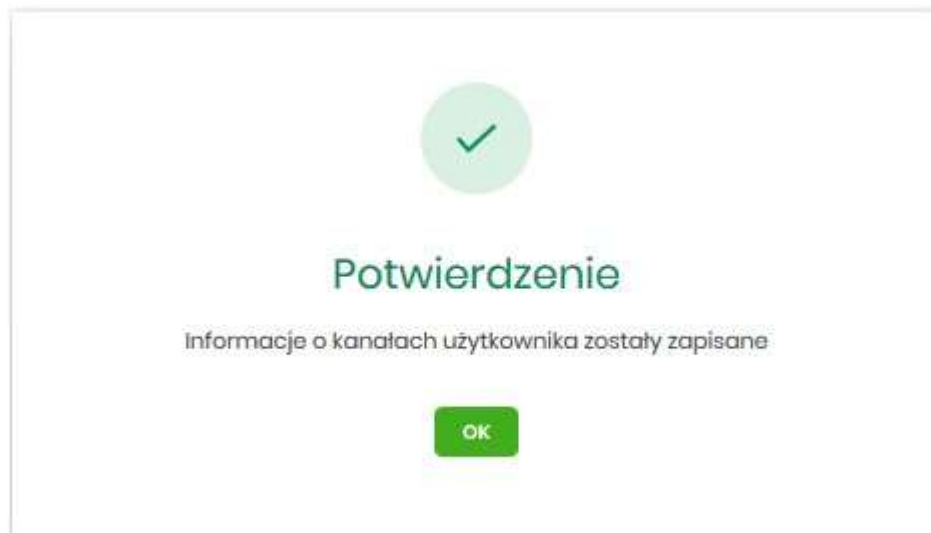
Nazwa kanału: Internet (WWW)  
Status: Zablokowany  
Limit dzienny: 1 200,00  
Limit jednorazowy: 300,00

Podaj kod autoryzacyjny: Wpisz kod

Operacja nr 1 z dnia 31.01.2020

ZAPISZ

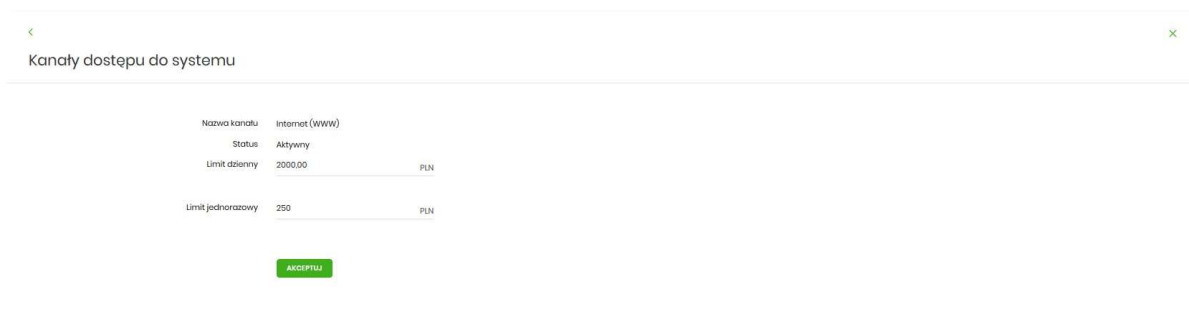
Po poprawnej autoryzacji i naciśnięciu przycisku [ZAPISZ], system prezentuje następujący komunikat:



Po odblokowaniu kanału, rachunek jest widoczny w systemie EBP liście rachunków dla wskazanego użytkownika.

### 10.7.3. Zmiana limitów dla kanału Internet (WWW)

W celu zmiany limitów (limit dzienny i limit jednorazowy) wybranego rachunku i użytkownika dla kanału Internet (WWW) na formularzu KANAŁY DOSTĘPU I LIMITY DLA UPOWAŻNIONYCH DO RACHUNKÓW, należy wybrać przycisk [EDYCJA].

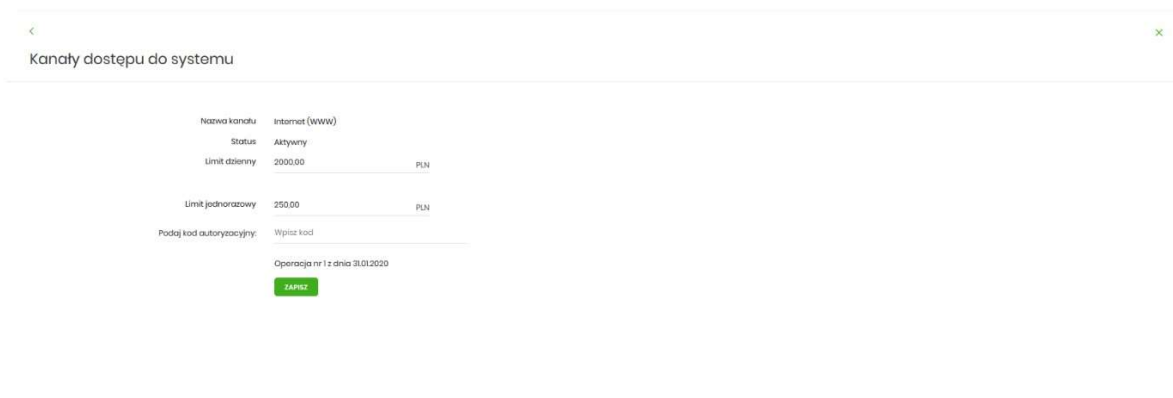


Nazwa kanału	Internet (WWW)
Status	Aktywny
Limit dzienny	2000,00 PLN
Limit jednorazowy	250 PLN

Na formularzu system prezentuje:

- pola:
  - Nazwa kanału – nazwa kanału pole zablokowane do edycji,
  - Limit dzienny – pole do zmiany limitu dziennego, ◦ Limit jednorazowy – pole do zmiany limitu jednorazowego,
- przycisk:
  - [AKCEPTUJ] – pozwalająca na zatwierdzenie wprowadzonej zmiany limitów.

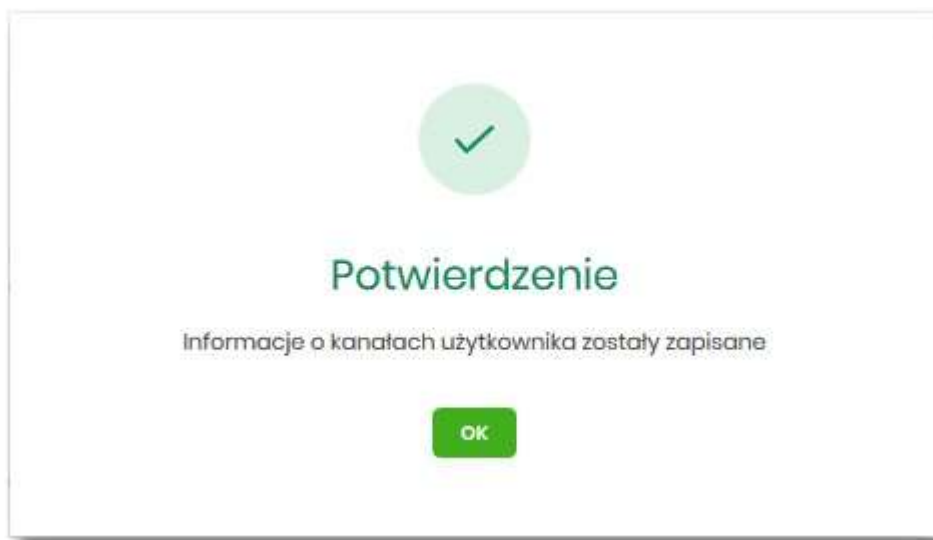
Po naciśnięciu przycisku [AKCEPTUJ], system przechodzi na formularz w którym użytkownik musi zatwierdzić zmianę limitów za pomocą dostępnej metody autoryzacji.



Nazwa kanału	Internet (WWW)
Status	Aktywny
Limit dzienny	2000,00 PLN
Limit jednorazowy	250,00 PLN
Podaj kod autoryzacyjny:	Wpisz kod

Operacja nr 1 z dnia 31.01.2020

Po zatwierdzeniu system prezentuje następujący komunikat:



## 10.8. Rejestr zdarzeń

W opcji *Ustawienia* → *Rejestr zdarzeń*, użytkownik ma możliwość przeglądania akcji wykonanych w danym kanale.

ZDARZENIE	DATA ZDARZENIA
Podpisanie paczki	28.01.2020, 14:05:00
Dodanie paczki zleceń	28.01.2020, 14:03:47
Dodanie przelewu do koszyka	28.01.2020, 13:59:58
Dodanie przelewu do koszyka	28.01.2020, 13:59:40
Dodanie przelewu do koszyka	28.01.2020, 13:59:25
Dodanie przelewu do koszyka	28.01.2020, 13:59:04
Podpisanie paczki	28.01.2020, 13:39:23
Dodanie paczki zleceń	28.01.2020, 13:38:58
Dodanie przelewu do koszyka	28.01.2020, 13:38:06
Dodanie przelewu do koszyka	28.01.2020, 13:37:50

W celu zawężenia prezentacji listy zdarzeń, system umożliwi zastosowanie filtru zaawansowanego za pomocą przycisku [POKAŻ FILTRY].

Ostatnie: 30 dni

Zakres dat: 28.12.2019 - 28.01.2020

Kanał: Wybierz

Typ zdarzenia: Wybierz

FILTRUJ

Użytkownik ma możliwość ustawiania filtru zaawansowanego dla następujących pól:

- Ostatnie – liczba dni poprzedzających datę bieżącą, dla których ma zostać zaprezentowana historia zdarzeń, domyślnie 30 dni,

- Zakres dat - zakres dat od do, dla których ma zostać wyświetlona historia zdarzeń, od miesiąca wstecz do daty bieżącej (alternatywa dla pola Ostatnie). Kliknięcie w obszar pól z datami otwiera okno kalendarza, za pomocą którego można określić zakres dat wybierając konkretną datę z kalendarza.



- Kanał – kanał, w którym zaistniało zdarzenie, wybór z listy kanałów: WWW,IVR.



- Typ zdarzenia – typ wyszukiwanego zdarzenie (wybór konkretnego zdarzenia z listy wartości), na liście dostępne są następujące typy zdarzeń:
  - Zmiana ustawień udostępnienia rachunku,
  - Złożenie przelewu,
  - Usunięcie przelewu,
  - Autoryzacja przelewu,
  - Modyfikacja przelewu,
  - Dodanie przelewu do koszyka,
  - Złożenie wniosku,
  - Anulowanie wniosku,
  - Autoryzacja wniosku,
  - Przeczytanie komunikatu przez użytkownika,

- Usunięcie komunikatu przez użytkownika,
- Zmiana ustawień udostępnienia do umów,
- Zmiana ustawień udostępnienia użytkownika,
- Zmiana nazwy własnej produktu,
- Zmiana konfiguracji ustawień i wyglądu,
- Zmiana konfiguracji skrótów,
- Zmiana hasła,
- Dodanie szablonu,
- Usunięcie szablonu,
- Modyfikacja szablonu,
- Aktywacja karty,
- Modyfikacja odbiorcy,
- Usunięcie odbiorcy,
- Wysłanie wiadomości,
- Przeczytanie wiadomości,
- Archiwizacja wiadomości,
- Odpowiedź na wiadomość,
- Złożenie dyspozycji otwarcia zlecenia stałego,
- Anulowanie dyspozycji otwarcia zlecenia stałego,
- Autoryzacja dyspozycji otwarcia zlecenia stałego,
- Dodanie dyspozycji otwarcia zlecenia stałego do koszyka,
- Złożenie dyspozycji modyfikacji zlecenia stałego,
- Anulowanie dyspozycji modyfikacji zlecenia stałego,
- Autoryzacja dyspozycji modyfikacji zlecenia stałego,
- Dodanie dyspozycji modyfikacji zlecenia stałego do koszyka,
- Złożenie dyspozycji zerwania zlecenia stałego,
- Anulowanie dyspozycji zerwania zlecenia stałego,
- Dodanie dyspozycji zerwania zlecenia stałego do koszyka,
- Złożenie dyspozycji otwarcia przelewu odroczonego,
- Anulowanie dyspozycji otwarcia przelewu odroczonego,
- Autoryzacja dyspozycji otwarcia przelewu odroczonego,

- Dodanie dyspozycji otwarcia przelewu odroczonego do koszyka,
- Złożenie dyspozycji modyfikacji przelewu odroczonego,
- Anulowanie dyspozycji modyfikacji przelewu odroczonego,
- Autoryzacja dyspozycji modyfikacji przelewu odroczonego,
- Dodanie dyspozycji modyfikacji przelewu odroczonego do koszyka,
- Złożenie dyspozycji zerwania przelewu odroczonego,
- Anulowanie dyspozycji zerwania przelewu odroczonego,
- Dodanie dyspozycji zerwania przelewu odroczonego do koszyka,
- Złożenie dyspozycji otwarcia lokaty,
- Anulowanie dyspozycji otwarcia lokaty,
- Autoryzacja dyspozycji otwarcia lokaty,
- Dodanie dyspozycji otwarcia lokaty do koszyka,
- Złożenie dyspozycji zerwania lokaty,
- Anulowanie dyspozycji zerwania lokaty,
- Dodanie dyspozycji zerwania lokaty do koszyka,
- Złożenie dyspozycji doładowania,
- Anulowanie dyspozycji doładowania,
- Autoryzacja dyspozycji doładowania,
- Dodanie dyspozycji doładowania do koszyka,
- Poprawne logowanie,
- Niepoprawne logowanie,
- Zmiana hasła logowania,
- Zmiana hasła autoryzacji,
- Skopiowanie przelewu w koszyku,
- Wypakowanie przelewu z paczki,
- Usunięcie przelewu z paczki,
- Utworzenie kopii przelewu z paczki,
- Dodanie paczki zleceń,
- Dodanie zleceń do paczki,
- Utworzenie kopii paczki,
- Podpisanie paczki,

- Wycofanie podpisu,
- Przekazanie do realizacji,
- Modyfikacja paczki,
- Usunięcie paczki,
- Edycja przelewu w paczce,
- Utworzenie filtru IP,
- Edycja filtru IP,
- Utworzenie filtru czasu dostępu,
- Edycja filtru czasu dostępu,
- Usunięcie filtru IP,
- Usunięcie filtru czasu dostępu,
- Import przelewów,
- Import szablonów.

Lista zdarzeń jest stronicowana, użytkownik ma możliwość przejścia do kolejnych stron za pomocą przycisków nawigacji znajdujących się w dolnej części formularza.



Zastosowanie filtru zaawansowanego aktywuje się za pomocą przycisku [FILTRUJ].

W górnej części formularza REJESTR ZDARZEŃ znajdują się przyciski:



– umożliwiający powrót do formularza USTAWIENIA,

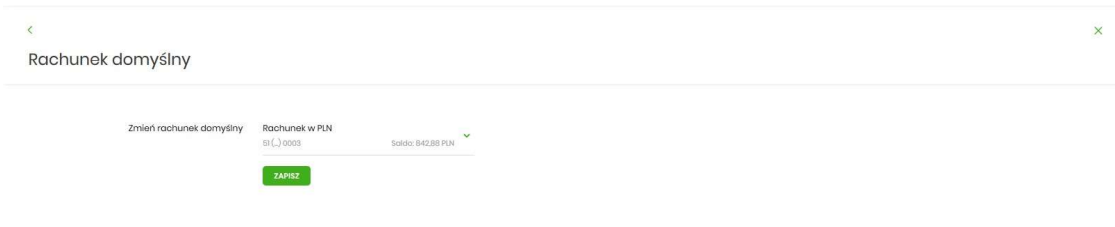


– umożliwiający przejście do głównego menu.



## 10.9. Rachunek domyślny

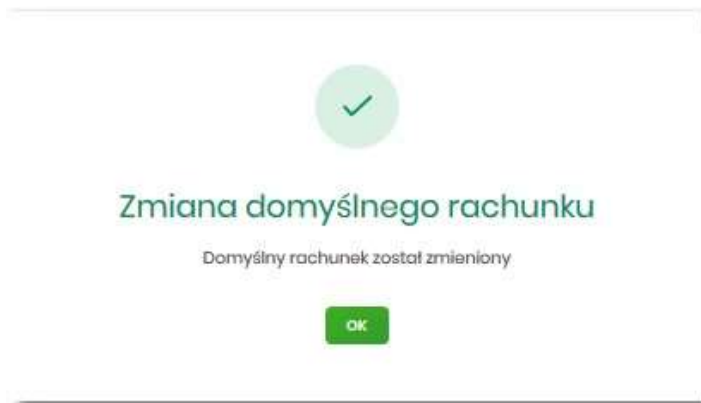
Opcja *Ustawienia* → *Rachunek domyślny* służy do ustawienia rachunku domyślnego, który jest podpowiadany użytkownikowi np. podczas składania przelewów.



W celu ustawienia rachunku domyślnego, użytkownik wybiera rachunek z listy dostępnych i zatwierdza zmiany za pomocą przycisku [ZAPISZ].





Po zapisaniu system prezentuje komunikat z informacją:



Ustawienie i zmiana rachunku domyślnego nie wymaga zatwierdzenia przez użytkownika za pomocą dostępnej metody autoryzacji.

W górnej części formularza RACHUNEK DOMYŚLNY znajdują się przyciski:

-  – umożliwiający powrót do formularza USTAWIENIA,
-  – umożliwiający przejście do głównego menu.

## 10.10. Uprawnienia użytkowników

W opcji *Ustawienia* → *Uprawnienia użytkowników* (opcja dostępna wyłącznie dla administratora klienta korporacyjnego), administrator ma możliwość zarządzania uprawnieniami użytkowników do poszczególnych rachunków oraz funkcjonalności w systemie.

W górnej części formularza UPRAWNIENIA UŻYTKOWNIKÓW dostępne są następujące przyciski:



•

– umożliwiający powrót do formularza USTAWIENIA,



•

– umożliwiający przejście do głównego menu.

Na formularzu UPRAWNIENIA UŻYTKOWNIKÓW, dostępne są następujące parametry:

- wybór użytkownika – administrator musi wybrać z listy wartości użytkownika, któremu chce nadać uprawnienia,
- zakres uprawnień – administrator musi wybrać z listy wartości jedną z dwóch dostępnych na liście wartości:
  - Funkcjonalne – uprawnienia pozwalające na zarządzanie dostępem do funkcjonalności w systemie EBP,
  - Rachunki – uprawnienia w zakresie możliwości ich obciążania lub oglądania.

## 10.10.1. Uprawnienia funkcjonalne

Na formularzu UPRAWNIENIA UŻYTKOWNIKÓW po wyborze w parametrze *Uprawnienia* wartości *Funkcjonalne*, administrator ma możliwość nadania poszczególnym użytkownikom (uprawnionym do firmy) uprawnień do poszczególnych funkcji systemu.

Zakres uprawnień  
Nadaj uprawnienia do funkcji w systemie i do rachunków dla wybranego użytkownika.

Uprawnienia: Funkcjonalne

Zaznacz:  WSZYSTKIE  PASYWNE

MINIFUNKCJA	UPRAWNIENIA
Rachunki	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Salda <input checked="" type="checkbox"/> Historia operacji <input checked="" type="checkbox"/> Wyciągi
Przelewy	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Dodawanie <input checked="" type="checkbox"/> Edycja <input checked="" type="checkbox"/> Usuwanie <input checked="" type="checkbox"/> Akceptowanie <input checked="" type="checkbox"/> Przekazywanie <input checked="" type="checkbox"/> Import
Paczki	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Dodawanie <input checked="" type="checkbox"/> Edycja <input checked="" type="checkbox"/> Usuwanie <input checked="" type="checkbox"/> Akceptowanie <input checked="" type="checkbox"/> Przekazywanie
Szablony	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Dodawanie <input checked="" type="checkbox"/> Edycja <input checked="" type="checkbox"/> Usuwanie <input checked="" type="checkbox"/> Import
Lokaty	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Dodawanie <input checked="" type="checkbox"/> Edycja <input checked="" type="checkbox"/> Zrywanie
Wiadomości	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Wysyłanie <input checked="" type="checkbox"/> Usuwanie
Ustawienia	<input checked="" type="checkbox"/> Podgląd uprawnień
Kredyty	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Historia <input checked="" type="checkbox"/> Spłata
Dodatowania	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Dodawanie
Karty	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Przeglądanie własnych <input checked="" type="checkbox"/> Przeglądanie wszystkich <input checked="" type="checkbox"/> Historia <input checked="" type="checkbox"/> Limity <input checked="" type="checkbox"/> Zarządzanie
Płatności masowe	<input type="checkbox"/> Przeglądanie <input type="checkbox"/> Historia operacji

ZAPISZ ZMIANY

Użytkownik może nadać albo odebrać uprawnienia pojedynczo albo za pomocą przycisków:

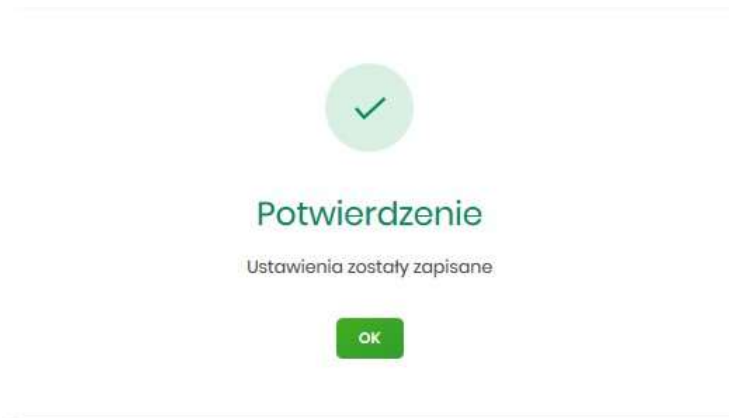
[WSZYSTKIE] – zaznaczenie/odznaczenie wszystkich uprawnień,

[PASYWNE] – zaznaczenie/odznaczenie wszystkich uprawnień pasywnych, W

dolnej części formularza UPRAWNIENIA UŻYTKOWNIKÓW dostępny jest akcja:

- [ZAPISZ ZMIANY] – pozwalająca na zapisanie wprowadzonych zmian.

Po naciśnięciu [ZAPISZ ZMIANY] system zapisuje wprowadzone zmiany, oraz prezentuje komunikat potwierdzający zapisanie wprowadzonych przez użytkownika zmian.



Zmiana uprawnień, nie wymaga zatwierdzenia przez użytkownika za pomocą dostępnej metody autoryzacji.

Zmiany uprawnień wymagają przelogowania użytkownika, którego dotyczą wprowadzone zmiany.

### 10.10.1.1. Uprawnienia dla Rachunków

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi do rachunków:

Rachunki	<input checked="" type="checkbox"/> Przeglądanie	<input checked="" type="checkbox"/> Salda	<input checked="" type="checkbox"/> Historia operacji	<input checked="" type="checkbox"/> Wyciągi
----------	--	---	---	---

- Przeglądanie – opcja steruje dostępem (prezentacją) miniaplikacji Rachunki. Jeżeli brak uprawnienia to użytkownik nie widzi miniaplikacji Rachunki, ukryty jest widżet i opcja w menu. W opcjach wyboru rachunku obciążanego przy realizacji przelewu, lista rachunków jest dostępna.
- Saldo – oznacza, że użytkownik ma dostępną informację o kwocie dostępnych środków (dotyczy również prezentacji w szczegółach rachunku na listach wyboru rachunku, widżet itd.).
- Historia operacji – oznacza, że użytkownik ma dostęp do wszystkich opcji dla historii operacji rachunku, dotyczy również:
  - eksportu statusów operacji (opcja *Przelewy* → *Eksport statusów*),
  - blokad na rachunku (opcja *Rachunki* → *Blokady*).
- Wyciągi – oznacza, że użytkownik ma dostęp do przeglądania listy wyciągów i pobierania (nie jest połączone z uprawnieniem Saldo).

Dodatkowe informacje:

- prezentacja wykresu salda na rachunku na widżet jest zależna od uprawnienia: Saldo.
- dostęp do opcji *podgląd historii operacji* jest zależny wyłącznie od uprawnienia historii operacji, prezentacja salda na podsumowaniu oraz przy operacji na zestawieniu nie jest zależna od uprawnienia Saldo.
- administrator będzie mógł nadawać pozostałe uprawnienia tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przełqdnie*, w innym przypadku pozostałe uprawnienia będą wyszarzone.

### 10.10.1.2. Uprawnienia dla Przelewów

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie przelewów:

Przelewy	<input checked="" type="checkbox"/> Przeglądanie	<input checked="" type="checkbox"/> Dodawanie	<input checked="" type="checkbox"/> Edycja	<input checked="" type="checkbox"/> Usuwanie
	<input checked="" type="checkbox"/> Akceptowanie	<input checked="" type="checkbox"/> Przekazywanie	<input checked="" type="checkbox"/> Import	

- Przeglądanie – dostęp do opcji przeglądania przelewów na liście (opcja: *Przelewy*, *Lista zleceń*),
- Dodawanie – możliwość tworzenia nowego przelewu w tym:
  - dodanie przelewu z listy kontrahentów,
  - dodanie przelewu na podstawie szablonu,
  - dodanie przelewu z poziomu rachunku,
  - ponowienie przelewu z historii operacji,
  - kopiowanie przelewów,

- przelew PayByNet.
- Edycja – edycja przelewu na liście w tym również:
  - edycja przelewu odroczonego oraz cyklicznego,
  - anulowanie przelewu odroczonego oraz cyklicznego,
  - zawieszenie przelewu cyklicznego,
  - aktywacja zawieszonych przelewów cyklicznych.
- Usuwanie – usuwanie przelewu z listy (nie dotyczy przelewów w paczce)
- Akceptacja – akceptacji przelewów posiadanych narzędziem autoryzacyjnym,
- Przekazanie – przekazanie przelewów do realizacji,
- Import – import przelewów w zdefiniowanych formatach.

Uprawnienia dotyczą również zleceń stałych.

Dodatkowe informacje:

- administrator będzie mógł nadawać pozostałe uprawnienia tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przeglądanie*, w innym przypadku pozostałe uprawnienia będą wyszarzone.

### 10.10.1.3. Uprawnienia dla Paczek

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie paczek przelewów:

Paczki	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Akceptowanie	<input checked="" type="checkbox"/> Dodawanie <input checked="" type="checkbox"/> Przekazywanie	<input checked="" type="checkbox"/> Edycja	<input checked="" type="checkbox"/> Usuwanie
--------	--	--	--	--

- Przeglądanie – przeglądanie listy paczek, bez możliwości importu, edycji, usuwania,
- Dodawanie – możliwość tworzenia paczek (dotyczy również tworzenia paczek przy imporcie przelewów), kopiowanie paczek,
- Edycja – możliwość edycji danych paczki (dotyczy również: rozpakowania paczki, wypakowania przelewu z paczki, edycji przelewu w paczce),
- Usuwanie – usuwanie paczki, usuwanie przelewu z paczki,
- Akceptacja – akceptacja paczki posiadanych narzędziem autoryzacyjnym,
- Przekazanie – przekazanie paczek do realizacji.

Dodatkowe informacje:

- administrator będzie mógł nadawać pozostałe uprawnienia tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przeglądanie*, w innym przypadku pozostałe uprawnienia będą wyszarzone.

#### 10.10.1.4. Uprawnienia dla Szablonów

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie szablonów:

Szablony	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Import	<input checked="" type="checkbox"/> Dodawanie	<input checked="" type="checkbox"/> Edycja	<input checked="" type="checkbox"/> Usuwanie
----------	--	---	--	--

- Przeglądanie – przeglądanie listy szablonów bez możliwości dodania/edycji/usunięcia,
- Dodawanie – dodanie szablonu,
- Edycja – edycja szablonu,
- Usuwanie – usunięcie danych szablonu,
- Import – import szablonów.

Dodatkowe informacje:

- administrator będzie mógł nadawać pozostałe uprawnienia tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przełqđnie*, w innym przypadku pozostałe uprawnienia będą wyszarzone.

#### 10.10.1.5. Uprawnienia dla Lokat

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie lokat:

Lokaty	<input checked="" type="checkbox"/> Przeglądanie	<input checked="" type="checkbox"/> Dodawanie	<input checked="" type="checkbox"/> Edycja	<input checked="" type="checkbox"/> Zrywanie
--------	--	---	--	--

- Przeglądanie – przeglądanie listy lokat,
- Dodawanie – dodanie lokaty ,
- Edycja (zmiana zadysponowania odnowieniem lokaty oraz dopłata do lokaty) – edycja warunków lokaty,
- Zrywanie – opcja zerwania lokaty przed terminem.

Dodatkowe informacje:

- administrator będzie mógł nadawać pozostałe uprawnienia tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przełqđnie*, w innym przypadku pozostałe uprawnienia będą wyszarzone.

#### 10.10.1.6. Uprawnienia dla Wiadomości

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie wiadomości:

Wiadomości	<input checked="" type="checkbox"/> Przeglądanie	<input checked="" type="checkbox"/> Wysyłanie	<input checked="" type="checkbox"/> Usuwanie
------------	--	---	--

- Przeglądanie – przeglądanie wiadomości (wysłanych i odebranych) i ich szczegółów,
- Wysyłanie – wysyłanie wiadomości,
- Usuwanie – usuwanie wiadomości, komunikatów itd.

Dodatkowe informacje:

- administrator będzie mógł nadawać pozostałe uprawnienia tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przeglądanie*, w innym przypadku pozostałe uprawnienia będą wyszarzone.

### 10.10.1.7. Uprawnienia dla Ustawień

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie ustawień:



- Podgląd uprawnień – podgląd uprawnień użytkownika.

### 10.10.1.8. Uprawnienia dla Kredytów

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie kredytów:



- Przeglądanie – przeglądanie listy kredytów i szczegółów kredytu (stan zadłużenia),
- Historia – podgląd historii kredytu,
- Spłata – spłata raty kredytu.

Dodatkowe informacje:

- administrator będzie mógł nadawać pozostałe uprawnienia tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przeglądanie*, w innym przypadku pozostałe uprawnienia będą wyszarzone.

### 10.10.1.9. Uprawnienia dla Doładowań

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie doładowań:



- Przeglądanie – przeglądanie listy doładowań,
- Dodawanie – dodanie nowego doładowania.

Dodatkowe informacje:

- administrator będzie mógł nadawać uprawnienie DODAWANIE tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przeglądanie*, w innym przypadku uprawnienie to będzie wyszarzone.

### 10.10.1.10. Uprawnienia dla Kart

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie kart:

Karty	<input checked="" type="checkbox"/> Przeglądanie <input checked="" type="checkbox"/> Limity	<input checked="" type="checkbox"/> Przeglądanie własnych <input checked="" type="checkbox"/> Zarządzanie	<input checked="" type="checkbox"/> Przeglądanie wszystkich	<input checked="" type="checkbox"/> Historia
-------	--	--	---	--

- Przeglądanie – przeglądanie listy kart,
- Przeglądanie własnych – przeglądanie tylko listy kart własnych,
- Przeglądanie wszystkich – przeglądanie listy wszystkich kart,
- Historia – przeglądanie historii operacji kartowych oraz eksport danych,
- Limity – zmiana limitów kart,
- Zarządzanie – dostęp do następujących akcji:
  - aktywacja karty,
  - zastrzeżenie karty,
  - spłata karty kredytowej.

Dodatkowe informacje:

- administrator będzie mógł nadawać pozostałe uprawnienia tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przeglądanie*, w innym przypadku pozostałe uprawnienia będą wyszarzone.

### 10.10.1.11. Uprawnienia dla Płatności masowych

Administrator ma możliwość zarządzania następującymi uprawnieniami funkcjonalnymi w zakresie płatności masowych:

Płatności masowe	<input checked="" type="checkbox"/> Przeglądanie	<input type="checkbox"/> Historia operacji
------------------	--	--

- Przeglądanie – przeglądanie płatności masowych,
- Historia operacji – przeglądanie analityki płatności masowej.

Dodatkowe informacje:

- administrator będzie mógł nadawać pozostałe uprawnienia tylko wtedy gdy użytkownik będzie miał nadane uprawnienie *Przeglądanie*, w innym przypadku pozostałe uprawnienia będą wyszarzone.

## 10.10.2. Uprawnienia do rachunków

Na formularzu UPRAWNIENIA UŻYTKOWNIKÓW po wyborze w parametrze *Uprawnienia* wartości *Rachunki*, administrator ma możliwość nadania poszczególnym użytkownikom (uprawnionym do firmy), uprawnień do rachunków firmowych.

W systemie dostępne są następujące uprawnienia do rachunków:



- Może podglądać,
- Może obciążać.

Uprawnienia są nadawane per rachunek i użytkownik.

- Może podglądać – użytkownik posiadający to uprawnienie, ma dostęp do oglądania rachunku (szczegółowy zakres widocznych danych dla rachunku określają uprawnienia do funkcjonalności w poszczególnej miniaplikacji).
- Może obciążać – użytkownik posiadający to uprawnienie ma dostęp do realizacji dyspozycji z tego rachunku (rachunek jest widoczny do wyboru jako rachunek do obciążania w tych miniaplikacjach, gdzie można złożyć dyspozycje np. Przelewy, zlecenia stałe, lokaty itp.)

Zakres uprawnień  
Nadaj uprawnienia do funkcji w systemie i do rachunków dla wybranego użytkownika.

Uprawnienia: Rachunki

**ODZNAĆ WSZYSTKIE**

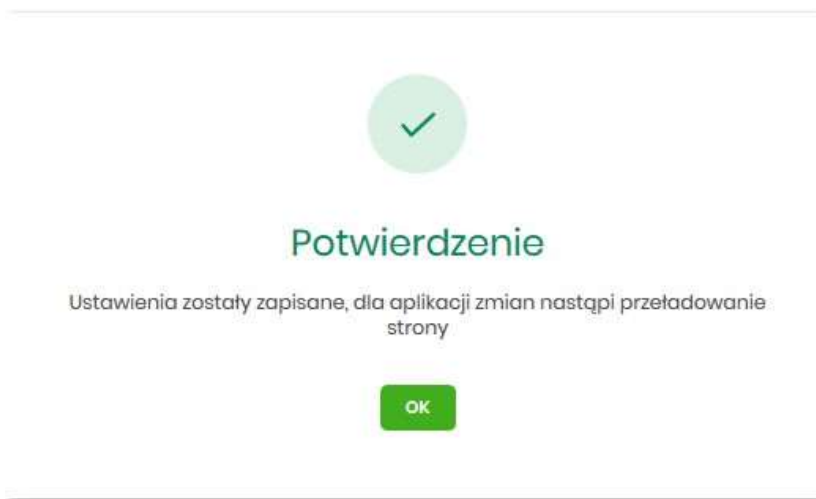
RACHUNEK	UPRAWNIENIA	
Rach.Bież.Podmiotów 28 8642 0002 2001 8400 7357 0001	<input checked="" type="checkbox"/> Może przeglądać	<input checked="" type="checkbox"/> Może obciążać
Rach.Bież.Podmiotów 71 8642 0002 2001 8400 7357 0003	<input checked="" type="checkbox"/> Może przeglądać	<input checked="" type="checkbox"/> Może obciążać

**ZAPISZ ZMIANY**

W dolnej części formularza UPRAWNIENIA UŻYTKOWNIKÓW dostępny jest akcja:

- [ZAPISZ ZMIANY] – pozwalająca na zapisanie wprowadzonych zmian.

Po naciśnięciu [ZAPISZ ZMIANY] system zapisuje wprowadzone zmiany, oraz prezentuje komunikat potwierdzający zapisanie wprowadzonych przez użytkownika zmian.



Zmiana uprawnień, nie wymaga zatwierdzenia przez użytkownika za pomocą dostępnej metody autoryzacji.

Dla rachunków VAT opcja *Obciążanie* nie jest dostępna do edycji.

Może być sytuacja w której użytkownik posiada uprawnienia do obciążania rachunku natomiast nie posiada uprawnienia do oglądania. W takiej sytuacji rachunek nie jest prezentowany na liście rachunków, nie mamy dostępu do wyciągów, historii itd. Użytkownik ma natomiast możliwość realizacji przelewów z tego rachunku, rachunek jest widoczny w polu *wyboru rachunku do obciążenia*.

Zmiany uprawnień wymagają przelogowania użytkownika, którego dotyczą zmiany.

## 10.11. Filtrowanie adresów IP

Opcja *Ustawienia* → *Filtrowanie adresów IP* umożliwia konfigurację usługi filtrowania adresów IP w zakresie użytkowników uprawnionych do logowania się do systemu EBP w kontekście firmy i indywidualnym.

Włączenie funkcjonalności filtrowania adresów IP jest możliwe tylko na poziomie globalnym (na firmie) przez administratora, natomiast zarządzanie i konfiguracja kontroli adresów IP jest możliwa na dwóch poziomach:

- globalnym – po zalogowaniu użytkownika do systemu EBP w kontekście firmowym,
- indywidualnym – po zalogowaniu użytkownika do systemu EBP w kontekście indywidualnym.

Formularz KONFIGURACJA DOSTĘPU prezentowany w kontekście firmowym

Konfiguracja dostępu

Każda zmiana wprowadzona u danego klienta wymaga autoryzacji!

Użytkownik: JAN TESTOWY

Konfiguracja dostępu aktywna

ZARZĄDZAJ NOWA KONFIGURACJA

NAZWA WŁASNA	ADRES IP	STATUS KONFIGURACJI	STATUS DOSTĘPU
Konfiguracja maska	*55.55*	Włączony	UDZIELONO DOSTĘPU
Konfiguracja zakres ip	172.168.0.0 172.168.1.142	Włączony	ZABRONIONO DOSTĘPU

Formularz KONFIGURACJA DOSTĘPU prezentowany w kontekście indywidualnym

Konfiguracja dostępu

Każda zmiana wprowadzona u danego klienta wymaga autoryzacji!

Konfiguracja dostępu aktywna

ZARZĄDZAJ NOWA KONFIGURACJA

NAZWA WŁASNA	ADRES IP	STATUS KONFIGURACJI	STATUS DOSTĘPU
Konfiguracja maska	*55.55*	Włączony	UDZIELONO DOSTĘPU
Konfiguracja zakres ip	172.168.0.0 172.168.1.142	Włączony	ZABRONIONO DOSTĘPU

Na formularzu KONFIGURACJA DOSTĘPU prezentowane są następujące dane:

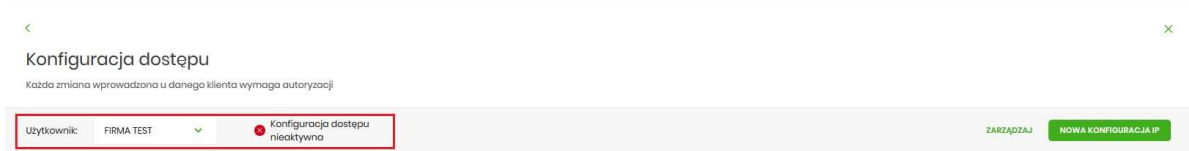
- Użytkownik – (pole prezentowane tylko dla administratora po zalogowaniu użytkownika do systemu w kontekście firmowym, w kontekście indywidualnym niedostępne), rozwijana lista prezentująca użytkowników uprawnionych do logowania się do systemu EBP w kontekście firmy oraz umożliwia wybór użytkownika w zakresie którego będzie wprowadzana konfiguracja:
  - Firma – globalne zarządzanie konfiguracją adresów IP,
  - Użytkownik – lista uprawnionych użytkowników, którzy mogą logować się do systemu EBP w kontekście tej firmy.



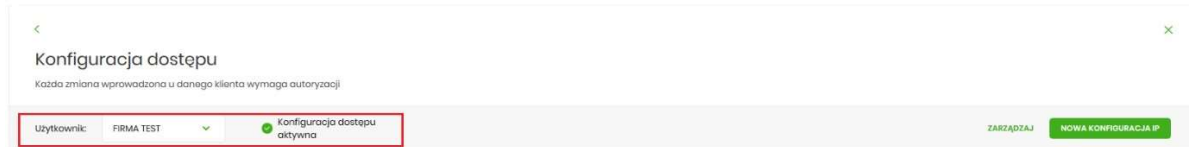
- Znacznik aktywna/nieaktywna – wskaźnik informujący o globalnym włączeniu lub wyłączeniu funkcjonalności filtrowania adresów IP.

## ZNACZNIK AKTYWNOŚCI/NIEAKTYWNOŚCI DLA KONTEKSTU FIRMOWEGO

### Konfiguracja nieaktywna

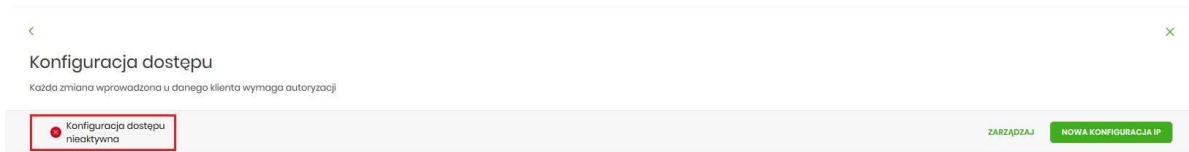


### Konfiguracja aktywna

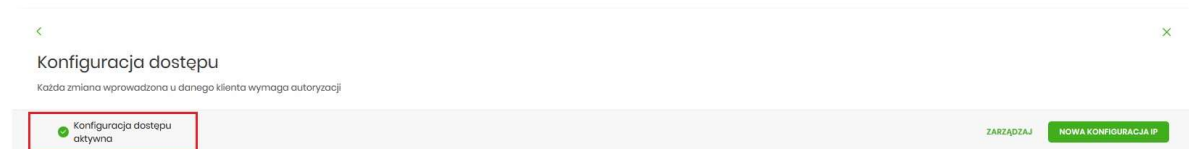


## ZNACZNIK AKTYWNOŚCI/NIEAKTYWNOŚCI DLA KONTEKSTU INDYWIDUALNEGO

### Konfiguracja nieaktywna



### Konfiguracja aktywna



- Nazwa własna – nazwa adresu IP nadana przez użytkownika podczas parametryzacji,
- Adres IP – adresy IP, z których nawiązywane będą połączenia do systemu EBP,
- Status Konfiguracji – prezentowane wartości:

- Włączony – włączona kontrola adresu IP podczas logowania użytkownika do systemu EBP w kontekście tej firmy,
- Wyłączony – wyłączona kontrola adresu IP podczas logowania użytkownika do systemu EBP w kontekście tej firmy,
- Status dostępu – status dostępu do systemu EBP ze wskazanego adresu IP:
  - Udzielono dostępu – możliwość zalogowania się do systemu EBP z tego adresu IP,
  - Zabroniono dostępu – brak możliwości zalogowania się do systemu EBP z tego adresu IP.

Dodatkowo prezentowany jest określony zestaw akcji:

- [ZARZĄDZAJ] – w zależności od wyboru użytkownika (w polu *Użytkownik*), będzie możliwe:
  - Dla FIRMY:
    - globalne włączenie funkcjonalności filtrowania adresów IP,
    - definiowanie częstotliwości kontroli oraz adresów IP na poziomie globalnym.
  - Dla UŻYTKOWNIKA
    - definiowanie częstotliwości kontroli oraz adresów IP na poziomie indywidualnym.
- [NOWA KONFIGURACJA] – opcja w zależności od wyboru użytkownika (w polu *Użytkownik*), będzie umożliwiała:
  - Dla FIRMY:
    - definicja adresów IP na poziomie globalnym (dla wszystkich użytkowników), z których użytkownicy będą albo nie będą mogli się zalogować do systemu EBP w kontekście tej firmy,
  - Dla UŻYTKOWNIKA
    - definicja adresów IP na poziomie globalnym (dla wybranego użytkownika), z których użytkownik będzie albo nie będzie mógł się zalogować do systemu EBP w kontekście firmy.

Z poziomu formularza KONFIGURACJA DOSTĘPU użytkownik będzie miał możliwość wykonania akcji, za pomocą następujących przycisków:



•

– edycja, umożliwia zmianę wprowadzonej konfiguracji, •



– usunięcie, umożliwia usunięcie wprowadzonej konfiguracji.

W górnej części formularza dostępne są przyciski:



- 

– umożliwiający powrót do formularza USTAWIENIA,



- 

– umożliwiający przejście do głównego menu.

### 10.11.1. Edycja konfiguracji adresów IP

Po wyborze przycisku [EDYCJA] zostanie zaprezentowany formularz EDYCJA KONFIGURACJI, umożliwiający wprowadzenie zmian konfiguracji adresów IP.

Edytuj konfigurację

Nazwa własna: aaa

Filtr IP: Maska adresu IP

Maskaz: • SS SS •

Kraj: Polska (PL)

Kontynent: Brak

Status:  Włączony  
 Wyłączony

Status dostępu:  Udzielono dostępu  
 Zabroniono dostępu

ZAPISZ

Na formularzu EDYCJA KONFIGURACJI dostępne do edycji są następujące parametry:

- Nazwa własna – nazwa adresu IP nadana przez administratora/użytkownika podczas parametryzacji,
- Filtr IP – dostępne wartości:
  - Zakres adresów IP ◦
  - Maska adresów IP
- Filtr IP od do – pole prezentowane po wyborze w opcji *Filtr IP* wartości Zakres adresów IP, należy podać w polach odpowiednie wartości dla adresu IP,

- Maska – pole prezentowane po wyborze w opcji *Filtr IP* wartości Maska adresu IP, należy zdefiniować adres IP z wykorzystaniem znaków:
  - "\*" - oznaczający dowolny ciąg cyfr w adresie IP,
  - "\$" - oznaczający jedną dowolną cyfrę w adresie IP.

- Kraj – dostępna lista wartości,
- Kontynent – dostępna lista wartości,
- Status – dostępne wartości:
  - Włączony – włączona kontrola dla wskazanego zakresu adresów IP albo adresu IP, podczas logowania użytkownika do systemu EBP,
  - Wyłączony – włączona kontrola dla wskazanego zakresu adresów IP albo adresu IP, podczas logowania użytkownika do systemu EBP,

- Status dostępu – dostępne wartości:
  - Udzielono dostępu – oznacza, że użytkownik logujący się z tego adresu IP albo ze wskazanego zakresu adresów IP, będzie mógł uzyskać dostęp do systemu EBP,
  - Zabroniono dostępu – oznacza, że użytkownik logujący się z tego adresu IP albo ze wskazanego zakresu adresów IP, nie będzie mógł uzyskać dostęp do systemu EBP.

Zmiany uprawnień należy zatwierdzić przyciskiem [ZAPISZ].



Wprowadzone zmiany ,będą wymagały potwierdzenia użytkownika za pomocą dostępnej metody autoryzacji.

W górnej części formularza ZARZĄDZANIE KONFIGURACJĄ DOSTĘPU, dostępne są przyciski:



•

– umożliwiający powrót do formularza KONFIGURACJA DOSTĘPU,

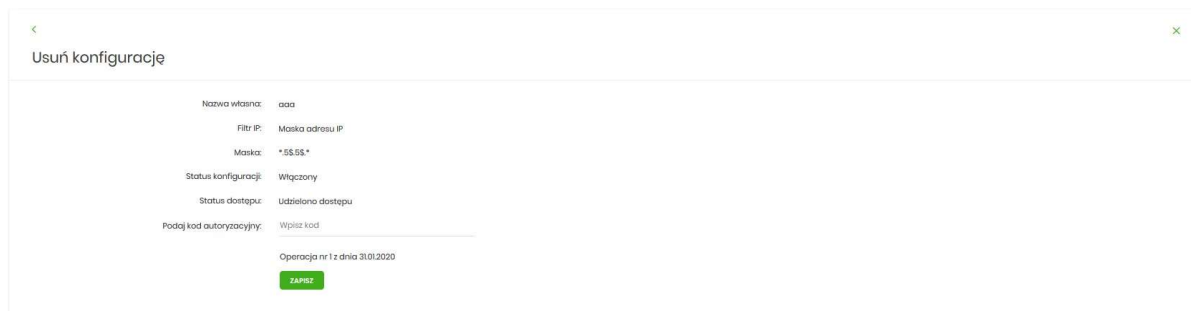


•

– umożliwiający przejście do głównego menu.

### 10.11.2. Usunięcie konfiguracji adresów IP

Po wyborze przycisku [USUŃ] zostanie zaprezentowany formularz USUNIĘCIE KONFIGURACJI, umożliwiający usunięcie konfiguracji adresów IP.

A screenshot of a web form titled "Usuń konfigurację". The form contains the following fields: "Nazwa własna:" with the value "oaa"; "Filtr IP:" with the value "Maska adresu IP"; "Maska:" with the value "\*55.55\*"; "Status konfiguracji:" with the value "Włączony"; "Status dostępu:" with the value "Udzielono dostępu"; and "Podaj kod autoryzacyjny:" with the value "Wpisz kod". At the bottom, there is a green "ZAPISZ" button and a small text "Operacja nr 1 z dnia 31.01.2020".

Usunięcie konfiguracji będzie wymagało potwierdzenia użytkownika, za pomocą dostępnej metody autoryzacji.

### 10.11.3. Włączenie funkcjonalności kontroli adresów IP na poziomie globalnym

Włączenie funkcjonalności na poziomie globalnym, dostępne jest tylko dla administratora/użytkownika FIRMA, w opcji [ZARZĄDZAJ].

Na formularzu ZARZĄDZANIE KONFIGURACJĄ DOSTĘPU dostępny jest parametr *Zarządzaj konfiguracją dostępu*, za pomocą którego administratora/użytkownika może globalnie włączyć/wyłączyć funkcjonalność:

- AKTYWNY – przesunięcie suwaka w prawo umożliwia włączenie funkcjonalności filtrowania adresów IP dla wszystkich użytkowników logujących się do systemu EBP w kontekście tej firmy,
- NIEAKTYWNA – przesunięcie suwaka w lewo umożliwia globalne wyłączenie funkcjonalności kontroli adresów IP dla wszystkich użytkowników logujących się do systemu EBP w kontekście tej firmy.

#### Wyłączona funkcjonalność kontroli adresów IP

#### Włączona funkcjonalność kontroli adresów IP

Zmiana konfiguracji będzie wymagała potwierdzenia użytkownika za pomocą dostępnej metody autoryzacji.

W zależności od ustawienia parametru *Zarządzaj konfiguracją dostępu* na formularzu KONFOGURACJA DOSTĘPU system zaprezentuje informację o statusie funkcjonalności:

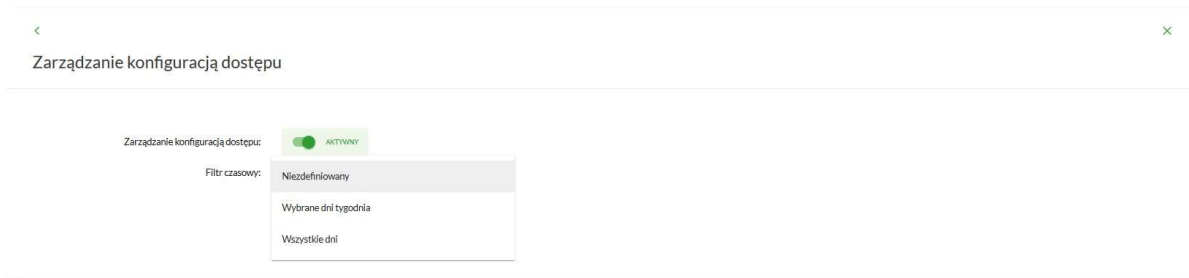
- Konfiguracja dostępu nieaktywna,

- Konfiguracja dostępu aktywna,



#### 10.11.4. Zarządzaj konfiguracją dostępu

Aby przejść do formularza ZARZĄDZANIE KONFIGURACJĄ DOSTĘPU, należy na formularzu KONFIGURACJA DOSTĘPU, wybrać użytkownika w polu *Użytkownik*, następnie nacisnąć przycisk [ZARZĄDZAJ].



Na formularzu dostępne są następujące parametry:

- Zarządzaj konfiguracją dostępu – parametr pozwala na włączenie albo wyłączenie funkcjonalności filtrowania adresów IP (zgodnie z opisem w punkcie 10.10.4), globalnie albo indywidualnie,
- Filtr czasowy – pozwala na konfigurację częstotliwości filtrowania adresów IP, dostępne wartości:
  - Niezdefiniowany – brak kontroli adresów IP podczas logowania użytkownika do systemu EBP (w zależności od wyboru użytkownika na formularzu KONFIGURACJA DOSTĘPU definicja globalnie albo indywidualnie),
  - Wybrane dni tygodnia – wybranie tej opcji pozwala na:
    - ustawienie dni tygodnia przez zaznaczenie checkbox przy danym dniu,
    - określenie godzin ( od do) w których system ma kontrolować adresy IP (w zależności od wyboru użytkownika na formularzu KONFIGURACJA DOSTĘPU definicja globalnie albo indywidualnie), w zaznaczonym dniu tygodnia (pole wymagalne gdy wskazano konkretny dzień),

<

## Zarządzanie konfiguracją dostępu

Filtr czasowy: Wybrane dni tygodnia

Poniedziałek:  Godziny: 00:00 - 00:00

Wtorek:  Godziny: 00:00 - 00:00

Środa:  Godziny: 00:00 - 00:00

Czwartek:  Godziny: 00:00 - 00:00

Piątek:  Godziny: 00:00 - 00:00

Sobota:  Godziny: 00:00 - 00:00

Niedziela:  Godziny: 00:00 - 00:00

**ZAPISZ**

- Wszystkie dni – po wybraniu tej opcji system pozwala na określenie godzin (od do) w zakresie których będą kontrolowane adresy IP (w zależności od wyboru użytkownika na formularzu KONFIGURACJA DOSTĘPU globalnie albo indywidualnie),

Zarządzanie konfiguracją dostępu:  AKTYWNY

Filtr czasowy: Wszystkie dni

Godziny: 00:00 - 00:00

**ZAPISZ**

Zmiany należy zatwierdzić przyciskiem [ZAPISZ].

**ZAPISZ**

Wprowadzone zmiany, będą wymagały potwierdzenia użytkownika za pomocą dostępnej metody autoryzacji.

W górnej części formularza ZARZĄDZANIE KONFIGURACJĄ DOSTĘPU, dostępne są przyciski:



•

– umożliwiający powrót do formularza KONFIGURACJA DOSTĘPU,



•

– umożliwiający przejście do głównego menu.

### 10.11.5. Nowa konfiguracja

Opcja umożliwia wprowadzenie konfiguracji adresów IP: globalnie dla firmy (wybór na formularzu KONFIGURACJA DOSTĘPU użytkownika Firma) i indywidualnie dla każdego uprawnionego użytkownika do tej firmy, w zależności od tego kto został wskazany na formularzu KONFIGURACJA DOSTĘPU w polu *Użytkownik*.

W przypadku gdy zostanie wprowadzona globalna konfiguracja a brak konfiguracji indywidualnej dla użytkownika, wówczas podczas logowania użytkownika do systemu EBP będą weryfikowane ustawienia globalne. W sytuacji gdy została wprowadzona zarówno konfiguracja globalna jak i indywidualna, wówczas podczas logowania użytkownika do systemu EBP w kontekście firmy będą weryfikowane ustawienia indywidualne zdefiniowane dla tego użytkownika z pominięciem ustawień globalnych.

Adres IP dozwolony oznacza adres IP, z którego użytkownik (dla którego taki adres został zdefiniowany), będzie mógł uzyskać dostęp do systemu EBP. Adres IP zabroniony oznacza adres IP, z którego użytkownik (dla którego taki adres został zdefiniowany) nie będzie miał dostępu do systemu EBP przez użytkownika.

Aby przejść do formularza NOWA KONFIGURACJA należy na formularzu KONFIGURACJA DOSTĘPU wybrać użytkownika (w zależności od wyboru użytkownika konfiguracja będzie globalna albo indywidualna) w polu *Użytkownik*, następnie nacisnąć przycisk [NOWA KONFIGURACJA].

Nowa konfiguracja

Nazwa własna:

Filtr IP:

Kraj:

Kontynent:

Status:  Włączony  
 Wyłączony

Status dostępu:  Udzielono dostępu  
 Zabroniono dostępu

Na formularzu dostępna są następujące parametry:

- Nazwa własna – nazwa adresu IP nadana przez administratora/użytkownika podczas parametryzacji,
- Filtr IP – dostępne wartości:
  - Zakres adresów IP ◦
  - Maska adresów IP
- Filtr IP od do – pole prezentowane po wyborze w opcji *Filtr IP* wartości Zakres adresów IP, należy podać w polach odpowiednie wartości dla adresu IP,

Filtr IP:

Od:

Do:

- Maska – pole prezentowane po wyborze w opcji *Filtr IP* wartości Maska adresu IP, należy zdefiniować adres IP z wykorzystaniem znaków:
  - "\*" - oznaczający dowolny ciąg cyfr w adresie IP,
  - "\$" - oznaczający jedną dowolną cyfrę w adresie IP.

Filtr IP:

Maska:

- Kraj – dostępna lista wartości, • Kontynent – dostępna lista wartości,
- Status – dostępne wartości:

- Włączony – włączona kontrola dla wskazanego zakresu adresów IP albo adresu IP, podczas logowania użytkownika do systemu EBP,
- Wyłączony – włączona kontrola dla wskazanego zakresu adresów IP albo adresu IP, podczas logowania użytkownika do systemu EBP,

Status:  Włączony  
 Wyłączony

- Status dostępu – dostępne wartości:

- Udzielono dostępu – oznacza, że użytkownik logujący się z tego adresu IP albo ze wskazanego zakresu adresów IP, będzie mógł uzyskać dostęp do systemu EBP,
- Zabroniono dostępu – oznacza, że użytkownik logujący się z tego adresu IP albo ze wskazanego zakresu adresów IP, nie będzie mógł uzyskać dostęp do systemu EBP.

Status dostępu:  Udzielono dostępu  
 Zabroniono dostępu

Zmiany uprawnień należy zatwierdzić przyciskiem [ZAPISZ].



Wprowadzone zmiany, będą wymagały potwierdzenia użytkownika za pomocą dostępnej metody autoryzacji.

W górnej części formularza ZARZĄDZANIE KONFIGURACJĄ DOSTĘPU, dostępne są przyciski:



- 

– umożliwiający powrót do formularza KONFIGURACJA DOSTĘPU,



- 

– umożliwiający przejście do głównego menu.

## 10.12. Historia logowań

W opcji *Ustawienia* → *Historia logowań* użytkownik ma możliwość przeglądania poprawnych i niepoprawnych logowań do systemu EBP.

DATA ZDARZENIA	ZDARZENIE	ADRES IP
22.01.2020, 09:45:06	Poprawne logowanie	10.130.0.1
22.01.2020, 09:44:47	Niepoprawne logowanie	10.130.0.1
22.01.2020, 09:20:38	Poprawne logowanie	10.130.0.1
22.01.2020, 09:20:08	Niepoprawne logowanie	10.130.0.1
22.01.2020, 09:10:26	Poprawne logowanie	10.130.0.1
22.01.2020, 09:09:52	Niepoprawne logowanie	10.130.0.1
15.01.2020, 11:14:54	Poprawne logowanie	10.130.0.1
15.01.2020, 10:56:09	Poprawne logowanie	10.130.0.1
15.01.2020, 10:02:19	Poprawne logowanie	10.130.0.1
15.01.2020, 09:52:13	Poprawne logowanie	10.130.0.1

W górnej części ekranu, znajduje się informacja o ostatnim poprawnym i niepoprawnym logowaniu do systemu EBP.



Na formularzu HISTORIA LOGOWAŃ znajdują się następujące informacje:

- Data zdarzenia – data logowania (data w formacie RRRR.MM.DD GG:MM:SS),
- Zdarzenie – status logowania, dostępne wartości:
  - Poprawne logowanie,
  - Niepoprawne logowanie,
- Adres IP – adres IP z jakiego nastąpiło logowanie lub próba logowania do systemu EBP.

W celu zawężenia prezentacji listy logowań, system umożliwi zastosowanie filtru zaawansowanego za pomocą przycisku [POKAŻ FILTRY].

Ostatnie: 30 dni Zakres dat: 29.12.2019 - 28.01.2020 Typ zdarzenia: Wybierz

POKAŻ FILTRY

FILTRUJ

Użytkownik ma możliwość ustawiania filtru zaawansowanego dla następujących pól:

- Ostatnie – liczba dni poprzedzających datę bieżącą, dla których ma zostać zaprezentowana historia logowań, domyślnie 30 dni,
- Zakres dat – zakres dat, od do, dla których ma zostać wyświetlona historia logowań, od miesiąca wstecz do daty bieżącej (alternatywa dla pola Ostatnie). Kliknięcie w obszar pól z datami otwiera okno kalendarza, za pomocą którego można określić zakres dat.



- Typ zdarzenia – typ wyszukiwanego zdarzenie (wybór konkretnego zdarzenia z listy wartości) dostępne wartości:
  - Poprawne logowanie,
  - Niepoprawne logowanie.

Lista historii logowań jest stronicowana, użytkownik ma możliwość przejścia do kolejnych stron za pomocą przycisków nawigacji znajdujących się w dolnej części formularza.



Zastosowanie filtra zaawansowanego aktywuje się za pomocą przycisku [FILTRUJ].

W górnej części formularza HISTORIA LOGOWAŃ znajdują się przyciski:



– umożliwiający powrót do formularza USTAWIENIA,



- umożliwiającą przejście do głównego menu.

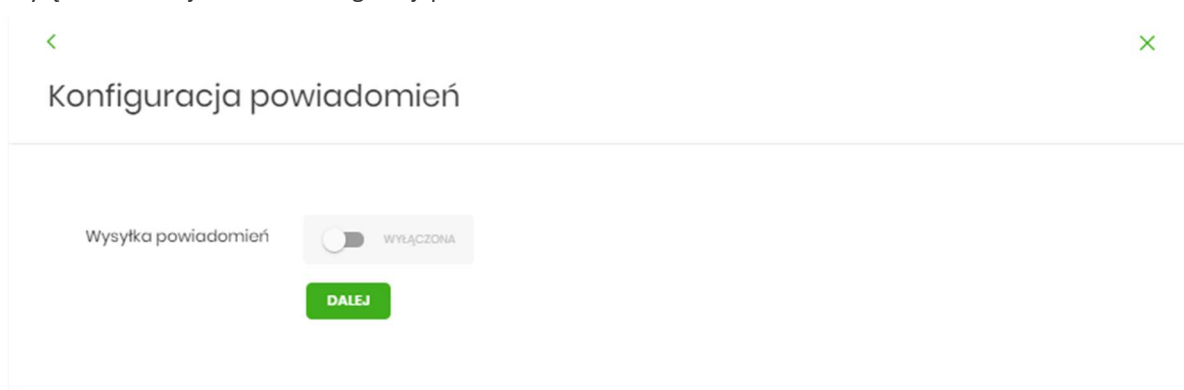
## 10.13. Konfiguracja powiadomień

W opcji *Ustawienia* → *Konfiguracja powiadomień* użytkownik ma możliwość włączenia i konfiguracji powiadomień dla kontekstu indywidualnego.

Na formularzu KONFIGURACJA POWIADOMIEŃ dostępny jest parametr *Wysyłka powiadomień*, umożliwiającą użytkownikowi włączenie/wyłączenie konfiguracji powiadomień:

- WŁĄCZONA – przesunięcie suwaka w prawo umożliwia włączenie funkcjonalności,
- WYŁĄCZONA – przesunięcie suwaka w lewo umożliwia wyłączenie funkcjonalności.

Wyłączona funkcjonalność konfiguracji powiadomień



The screenshot shows a mobile application interface for 'Konfiguracja powiadomień'. At the top, there is a back arrow on the left and a close 'X' icon on the right. Below the title, there is a toggle switch for 'Wysyłka powiadomień' which is currently in the 'WYŁĄCZONA' (off) position. Below the toggle is a green button labeled 'DALEJ'.

Włączona funkcjonalność konfiguracji powiadomień

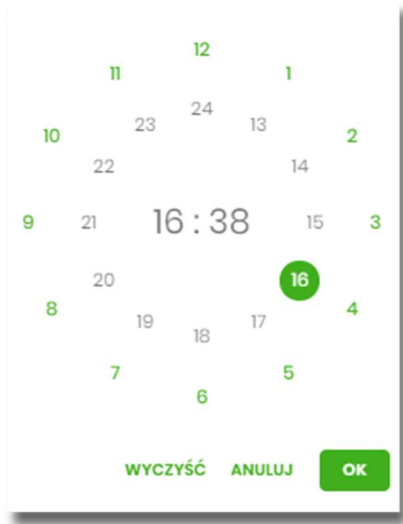


The screenshot shows the same 'Konfiguracja powiadomień' form, but the toggle switch for 'Wysyłka powiadomień' is now in the 'WŁĄCZONA' (on) position. Below the toggle, there are two input fields: 'Godziny wysyłki powiadomień' and 'Od: 00:00 Do: 00:00'.

Aby użytkownik miał możliwość zarządzania uprawnieniami, musi zostać włączony parametr Konfiguracja powiadomień. Po włączeniu usługi na formularzu KONFIGURACJA POWIADOMIEŃ system udostępni parametry, umożliwiające konfigurację powiadomień, podzielone na następujące sekcje:

- Parametry ogólne:
  - **Godzina wysyłki powiadomień** – zakres godzin, od do, w których mają być wysyłane powiadomienia. Kliknięcie w obszar pól z godzinami otwiera okno zegara, za pomocą którego można określić zakres godzin,





W oknie zegara dostępne są następujące przyciski:

- Wyczyść – po naciśnięciu następuje usunięcie wybranej przez użytkownika godziny, oraz zamknięcie zegara i powrót do formularza KONFIGURACJA POWIADOMIEŃ,
  - Anuluj – po naciśnięciu następuje anulowanie wybranej godziny oraz zamknięcie zegara i powrót do formularza KONFIGURACJA POWIADOMIEŃ,
  - Cofnij – przycisk jest dostępny w momencie wskazania przez użytkownika godziny. Po naciśnięciu następuje anulowanie wybranej godziny i minuty, wówczas system na formularzu zegara prezentuje aktualny czas, oraz użytkownik ma możliwość wyboru innej godziny i minuty.
  - OK – przycisk potwierdza wybór godziny i następuje powrót do formularza KONFIGURACJA POWIADOMIEŃ.
- Konfiguracja powiadomień dla wybranych funkcjonalności, w podziale na:
    - Rachunki,
    - Lokaty,
    - Logowanie,
    - Przelewy.

RACHUNKI	LOKATY	LOGOWANIE	PRZELEWY
<b>Zmiana salda</b>	Powiadomienie wysyłane każdorazowo w momencie zmiany salda na rachunku <input type="checkbox"/> SMS <input type="checkbox"/> PUSH		
<b>Debet na rachunku</b>	Powiadomienie wysyłane każdorazowo w momencie zmiany salda na rachunku, gdy ta powoduje powstanie debetu <input type="checkbox"/> SMS <input type="checkbox"/> PUSH		
<b>Cykliczna informacja o stanie salda</b>	Powiadomienie wysyłane w wybrane dni niezależnie od tego, czy nastąpiła zmiana salda. <input type="checkbox"/> SMS <input type="checkbox"/> PUSH		
<b>DALEJ</b>			

W dolnej części formularza KONFIGURACJA POWIADOMIEŃ dostępne są:

- Informacja prezentowana na formularzu zawsze po włączeniu parametru *Wysyłka powiadomień*,

*Zmiana konfiguracji powiadomień SMS może mieć wpływ na koszty obsługi rachunku, szczegółowa informacja jest dostępna w Taryfie prowizji i opłat.*

- Przycisk [DALEJ] – zmiana konfiguracji wymaga zatwierdzenia przez użytkownika, za pomocą dostępnej metody autoryzacji. Po naciśnięciu przycisku [DALEJ], system prezentuje formularz KONFIGURACJA POWIADOMIEŃ z podsumowaniem wprowadzonej konfiguracji powiadomień oraz oczekuje na zatwierdzenie zmian.

<>

## Konfiguracja powiadomień

---

**Wszystka powiadomień**  WŁĄCZONA

Godziny wysyłki powiadomień    Od: 09:30    Do: 14:50

Godzina wysyłki powiadomień cyklicznych    10:45

---

**RACHUNKI**

**Zmiana salda**     SMS     PUSH  
Kwota zmiany salda, powyżej której wysłane będzie powiadomienie  
100,00    PLN

**Debet na rachunku**     SMS     PUSH

**Cykliczna informacja o stanie salda**     SMS     PUSH

---

**LOKATY**

**Przypomnienie o zapadalności lokaty**     SMS     PUSH

---

**LOGOWANIE**

**Nieudane logowanie do bankowości internetowej**     SMS     PUSH

**Udane logowanie do bankowości internetowej**     SMS     PUSH

---


**PRZELEWY**

**Zmiana statusu przelewu**     SMS     PUSH

**Zrealizowanie przelewu**     SMS     PUSH

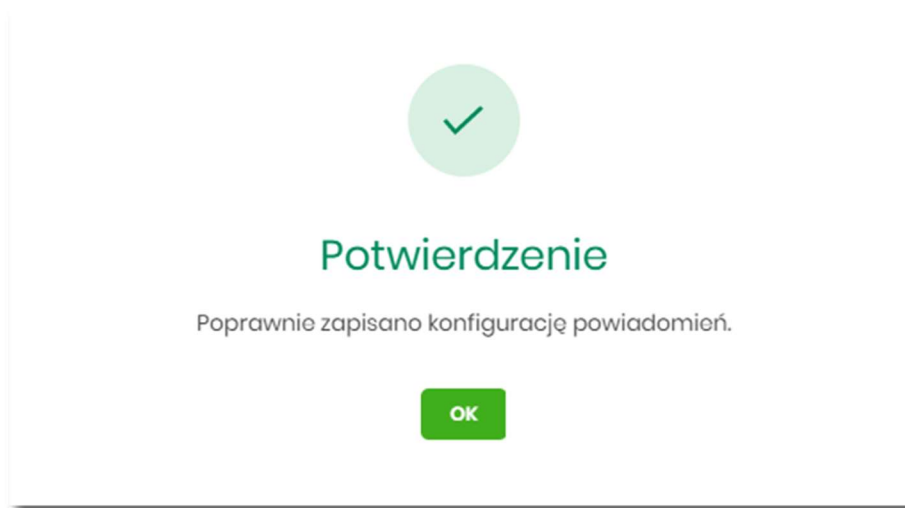
**Odrzucenie przelewu**     SMS     PUSH

Powiadomienie autoryzacyjne zostało wysłane do urządzenia mobilnego.  
**Pozostań na tej stronie i potwierdź operację w aplikacji mobilnej.**



Oczekiwanie na podpis aplikacją mobilną.

Po poprawnej autoryzacji, system wyświetli okno z potwierdzeniem:



Na potwierdzeniu dostępny jest przycisk [OK], po naciśnięciu którego system przechodzi do formularza KONFIGURACJA POWIADOMIEŃ.

### 10.13.1. Konfiguracja powiadomień dla rachunków

Wybranie zakładki RACHUNKI umożliwia użytkownikowi konfigurację powiadomień dotyczących rachunków.

RACHUNKI	LOKATY	LOGOWANIE	PRZELEWY
<b>Zmiana salda</b>	Powiadomienie wysyłane każdorazowo w momencie zmiany salda na rachunku		
	<input type="checkbox"/> SMS <input type="checkbox"/> PUSH		
<b>Debet na rachunku</b>	Powiadomienie wysyłane każdorazowo w momencie zmiany salda na rachunku, gdy ta powoduje powstanie debetu		
	<input type="checkbox"/> SMS <input type="checkbox"/> PUSH		
<b>Cykliczna informacja o stanie salda</b>	Powiadomienie wysyłane w wybrane dni niezależnie od tego, czy nastąpiła zmiana salda.		
	<input type="checkbox"/> SMS <input type="checkbox"/> PUSH		
<b>DALEJ</b>			

W zakładce RACHUNKI użytkownik ma możliwość konfiguracji następujących parametrów:

- Zmiany salda – powiadomienie wysyłane każdorazowo w momencie zmiany salda na rachunku, dostępne do konfiguracji są następujące parametry:
  - SMS – wysyłanie powiadomień za pomocą SMS,
  - PUSH – wysyłanie powiadomień za pomocą PUSH.

Użytkownik ma możliwość jednocześnie zaznaczenia dwóch checkboxów, po zaznaczeniu przynajmniej jednego checkboxa, system zaprezentuje dodatkowy parametr:

- Kwota zmiany salda, powyżej której wysłane będzie powiadomienie:

**Zmiana salda** Powiadomienie wysyłane każdorazowo w momencie zmiany salda na rachunku

SMS  PUSH

Kwota zmiany salda, powyżej której wysłane będzie powiadomienie

100,00 PLN

W przypadku, gdy użytkownik nie wypełni kwoty, system zaprezentuje dodatkową informację: *Powiadomienie będzie wysyłane niezależnie od kwoty.*

**Zmiana salda** Powiadomienie wysyłane każdorazowo w momencie zmiany salda na rachunku

SMS  PUSH

Kwota zmiany salda, powyżej której wysłane będzie powiadomienie

*\* Powiadomienie będzie wysyłane niezależnie od kwoty*

0 PLN

- **Debet na rachunku** - powiadomienie wysyłane każdorazowo w momencie zmiany salda na rachunku, gdy to powoduje powstanie debetu, dostępne do konfiguracji są następujące parametry:
  - SMS – wysyłanie powiadomień za pomocą SMS,
  - PUSH – wysyłanie powiadomień za pomocą PUSH.

Użytkownik ma możliwość jednocześnie zaznaczenia dwóch checkboxów.

- **Cykliczna informacja o stanie salda** - powiadomienie wysyłane w wybrane dni niezależnie od tego, czy nastąpiła zmiana salda, dostępne do konfiguracji są następujące parametry:
  - SMS – wysyłanie powiadomień za pomocą SMS,
  - PUSH – wysyłanie powiadomień za pomocą PUSH.

Użytkownik ma możliwość jednocześnie zaznaczenia dwóch checkboxów. Po zaznaczeniu przynajmniej jednego checkboxa, system prezentuje dodatkową informację *Powiadomienie wysyłane o godzinie 09:00*, godzina prezentowana w informacji, jest uzależniona od ustawienia parametru *Godzina wysyłki powiadomień*.

Godzina wysyłki powiadomień cyklicznych 00:00

*W przypadku wybrania wysyłki powiadomienia cyklicznego należy określić godzinę jego wysyłki*

- Dodatkowo system prezentuje listę dni tygodnia, użytkownik może wskazać konkretne lub wszystkie dni w których będą wysyłane powiadomienia.

#### Cykliczna informacja o stanie salda

Powiadomienie wysyłane w wybrane dni niezależnie od tego, czy nastąpiła zmiana salda.

SMS  PUSH

*Powiadomienie wysyłane o godzinie 10:45*

Dni wysyłki powiadomień

PONIEDZIAŁEK

WTOREK

ŚRODA

CZWARTEK

PIĄTEK

SOBOTA

NIEDZIELA

### 10.13.2. Konfiguracja powiadomień dla lokat

Wybranie zakładki LOKATY umożliwia użytkownikowi konfigurację powiadomień dotyczących lokat.

RACHUNKI **LOKATY** LOGOWANIE PRZELEWY

**Przypomnienie o zapadalności lokaty** Powiadomienie wysyłane na kilka dni przed zaplanowanym terminem zapadalności lokaty

SMS  PUSH

*Powiadomienie wysyłane o godzinie 09:00*

*Zmiana konfiguracji powiadomień SMS może mieć wpływ na koszty obsługi rachunku, szczegółowa informacja jest dostępna w Taryfie prowizji i opłat.*

**DALEJ**

W zakładce LOKATY użytkownik ma możliwość konfiguracji następujących parametrów:

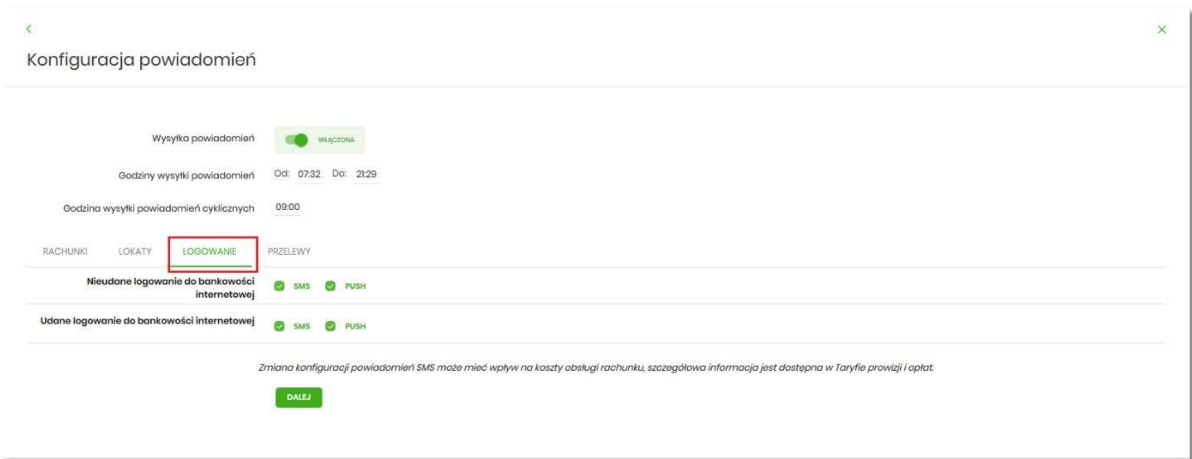
- Przypomnienie o zapadalności lokaty – powiadomienie wysyłane na kilka dni przed planowanym terminem zapadalności lokaty, dostępne do konfiguracji są następujące parametry:
  - SMS – wysyłanie powiadomień za pomocą SMS,
  - PUSH – wysyłanie powiadomień za pomocą PUSH.

Użytkownik ma możliwość jednocześnie zaznaczenia dwóch checkboxów, po zaznaczeniu przynajmniej jednego checkboxa, system prezentuje dodatkową informację *Powiadomienie wysyłane o godzinie 09:00*. Godzina prezentowana w informacji, jest uzależniona od ustawienia parametru *Godzina wysyłki powiadomień cyklicznych*.

Godzina wysyłki powiadomień cyklicznych 10:45

### 10.13.3. Konfiguracja powiadomień dla logowania

Wybranie zakładki LOGOWANIE umożliwia użytkownikowi konfigurację powiadomień dotyczących logowania.



W zakładce LOGOWANIE użytkownik ma możliwość konfiguracji następujących parametrów:

- Nieudane logowanie do bankowości internetowej – powiadomienia wysyłane w momencie nieudanego logowania użytkownika do systemu EBP, dostępne do konfiguracji są następujące parametry:
  - SMS – wysyłanie powiadomień za pomocą SMS,
  - PUSH – wysyłanie powiadomień za pomocą PUSH.

Użytkownik ma możliwość jednocześnie zaznaczenia dwóch checkboxów.

- Udane logowanie do bankowości internetowej – powiadomienia wysyłane w momencie udanego logowania użytkownika do systemu EBP, dostępne do konfiguracji są następujące parametry:
  - SMS – wysyłanie powiadomień za pomocą SMS,
  - PUSH – wysyłanie powiadomień za pomocą PUSH.

Użytkownik ma możliwość jednocześnie zaznaczenia dwóch checkboxów.

#### 10.13.4. Konfiguracja powiadomień dla przelewów

Wybranie zakładki PRZELEWY umożliwi użytkownikowi konfigurację powiadomień dotyczących przelewów.

W zakładce PRZELEWY użytkownik ma możliwość konfiguracji następujących parametrów:

- Zmiany statusu przelewu – powiadomienie wysyłane, gdy status przelewu wprowadzonego w bankowości internetowej ulegnie zmianie, dostępne do konfiguracji są następujące parametry:
  - SMS – wysyłanie powiadomień za pomocą SMS,
  - PUSH – wysyłanie powiadomień za pomocą PUSH.

Użytkownik ma możliwość jednocześnie zaznaczenia dwóch checkboxów. Po ich zaznaczeniu, system zablokuje możliwość wyboru poniższych opcji (checkboxy wyboru zostają wyszarzone) dla parametrów: *Zrealizowanie przelewu* i *Odrzucenie przelewu*.

- Zrealizowanie przelewu – powiadomienie wysyłane, gdy przelew wprowadzony w bankowości internetowej zostanie zrealizowany. Parametr zablokowany, w sytuacji gdy zaznaczono checkbox dla parametru *Zmiany statusu przelewu*, dostępne do konfiguracji są następujące parametry:
  - SMS – wysyłanie powiadomień za pomocą SMS,
  - PUSH – wysyłanie powiadomień za pomocą PUSH.

Użytkownik ma możliwość jednocześnie zaznaczenia dwóch checkboxów. Po zaznaczeniu przynajmniej jednego checkboxa, system zaprezentuje dodatkowy parametr:

- Kwota przelewu, powyżej której wysyłane jest powiadomienie – w przypadku gdy użytkownik nie poda kwoty, system zaprezentuje informację *Powiadomienie będzie wysyłane niezależnie od kwoty*



Kwota przelewu, powyżej której wysyłane jest powiadomienie

\* Powiadomienie będzie wysyłane niezależnie od kwoty

0 PLN

- Odrzucenie przelewu – powiadomienie wysyłane, gdy przelew wprowadzony w bankowości internetowej zostanie odrzucony. Parametr zablokowany, w sytuacji gdy zaznaczono checkbox dla parametru *Zmiany statusu przelewu*, dostępne do konfiguracji są następujące parametry:
  - SMS – wysyłanie powiadomień za pomocą SMS,
  - PUSH – wysyłanie powiadomień za pomocą PUSH.

Użytkownik ma możliwość jednocześnie zaznaczenia dwóch checkboxów.

W sytuacji gdy użytkownik zaznaczył checkbox SMS dla parametrów:

- Zrealizowanie przelewu,
- Odrzucenie przelewu, a następnie zaznaczył checkbox SMS dla parametru *Zmiana statusu przelewu*, wówczas dostępne są ustawienia parametrów:
- Zrealizowanie przelewu,
- Odrzucenie przelewu, zostaną anulowane (odznaczonych checkbox SMS). Tak samo system się zachowa dla checkbox PUSH.

## 10.14. Zmiana hasła telefonicznego

W opcji *Ustawienia* → *Zmiana hasła telefonicznego* użytkownik ma możliwość zmiany hasła do obsługi telefonicznej.

Po wybraniu opcji *Zmiana hasła telefonicznego* prezentowany jest formularz ZMIANA HASŁA TELEFONICZNEGO wraz z polami do wprowadzenia nowego hasła:

Zmiana hasła telefonicznego

Nowe hasło Wpisz nowe hasło

Powtórz nowe hasło Powtórz nowe hasło

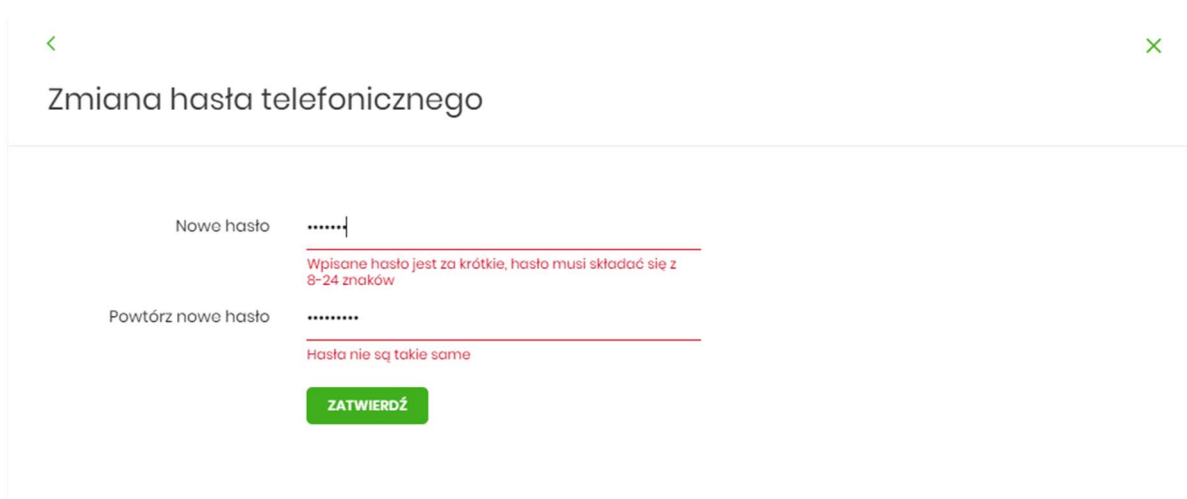
ZATWIERDŹ

- Nowe hasło – użytkownik wprowadza nowe hasło,
- Powtórz nowe hasło – użytkownik ponownie wprowadza nowe hasło.

Akcja:

- [ZATWIERDŹ] – umożliwia zatwierdzenie zmiany hasła.

Hasło obsługi telefonicznej to dowolny ciąg znaków o długości od 8 do 24. W przypadku wprowadzenia niepoprawnego nowego hasła, system zaprezentuje odpowiednią informację:



Po poprawnym wpisaniu nowego hasła oraz zatwierdzeniu, system przejdzie do nowego okna w celu akceptacji zmiany hasła za pomocą dostępnej metody autoryzacji.



Po poprawnej autoryzacji system zaprezentuje następujący komunikat:



## Potwierdzenie

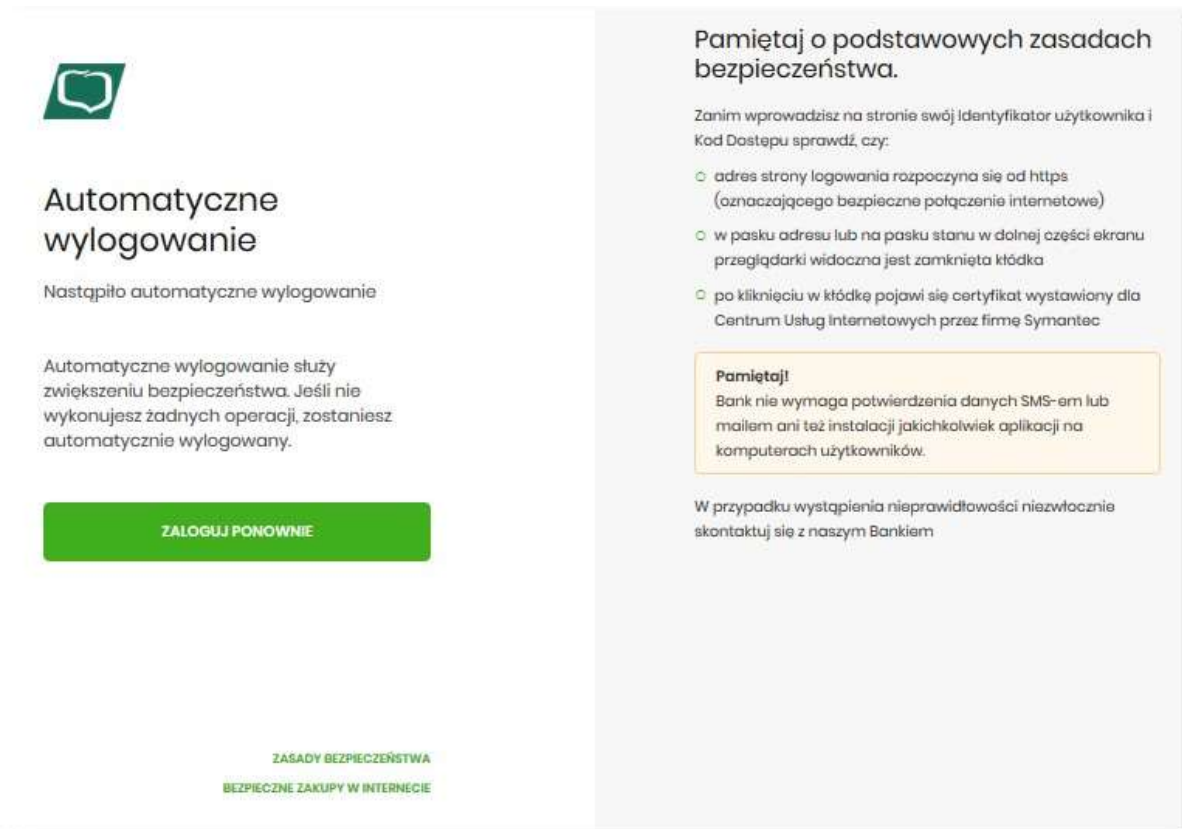
Hasło telefoniczne zostało zmienione

[WRÓĆ DO PULPITU](#)

## Rozdział 11. Zakończenie pracy z systemem

W celu zakończenia pracy z systemem EBP, należy wybrać przycisk [WYLOGUJ], dostępny w górnym pasku menu aplikacji.

Wylogowanie użytkownika z systemu, może także nastąpić po upływie określonego czasu bezczynności użytkownika. Ma to na celu zwiększenie bezpieczeństwa. Jeżeli użytkownik nie wykonuje żadnych operacji przez 10 minut, system automatycznie wyloguje użytkownika z systemu EBP.



The screenshot displays a user interface for the EBP system. On the left, a green logo is positioned above the heading "Automatyczne wylogowanie". Below this, a message states "Nastąpiło automatyczne wylogowanie". A paragraph explains that automatic logout is for security and occurs if no operations are performed for 10 minutes. A prominent green button labeled "ZALOGUJ PONOWNIE" is located below the text. At the bottom left, there are links for "ZASADY BEZPIECZEŃSTWA" and "BEZPIECZNE ZAKUPY W INTERNECIE". On the right side, a grey panel titled "Pamiętaj o podstawowych zasadach bezpieczeństwa." contains a list of security checks: verifying the user ID and password, ensuring the login URL starts with https, checking for a lock icon in the browser's address bar, and noting that a Symantec certificate appears after clicking a lock icon. A yellow box labeled "Pamiętaj!" emphasizes that the bank does not require SMS or mail verification and that no applications should be installed on user computers. At the bottom of this panel, it advises contacting the bank immediately if any irregularities occur.

Automatyczne wylogowanie użytkownika z systemu, może także nastąpić w wyniku zalogowania się do systemu EBP na innym urządzeniu, przy pomocy tego samego numeru identyfikacyjnego.