



BS w Bartoszychach

Grupa BPS

BANKOWOŚĆ INTERNETOWA

Asseco EBP

metody logowania i autoryzacji zleceń

SPIS

ROZDZIAŁ 1. WPROWADZENIE	2
ROZDZIAŁ 2. KORZYSTANIE Z PRZEGLĄDAREK INTERNETOWYCH POD KĄTEM PRACY W SYSTEMIE.....	3
ROZDZIAŁ 3. LOGOWANIE DO SYSTEMU.....	4
I. LOGOWANIE DO SYSTEMU ZA POMOCĄ APLIKACJI MOBILNEJ ASSECO MAA	7
II. LOGOWANIE DO SYSTEMU ASSECO EBP PRZY POMOCY KARTY MIKROPROCESOROWEJ	17
III. LOGOWANIE DO SYSTEMU ASSECO EBP PRZY POMOCY HASŁA MASKOWANEGO + KODU SMS	20
ROZDZIAŁ 4. METODY AUTORYZACJI ZLECEŃ.....	27
I. MOBILNY PODPIS.....	27
II. KARTA MIKROPROCESOROWA.....	28
III. KOD PIN + KOD SMS	31

*Bankowość internetowa Asseco CBP/EBP
Bank Spółdzielczy w Bartoszychach, listopad 2020*

Rozdział 1. Wprowadzenie

Asseco 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 Asseco 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 **Asseco 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 Asseco 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 2. Korzystanie z przeglądarek internetowych pod kątem pracy w systemie

Z uwagi na kompatybilność systemu Asseco 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.

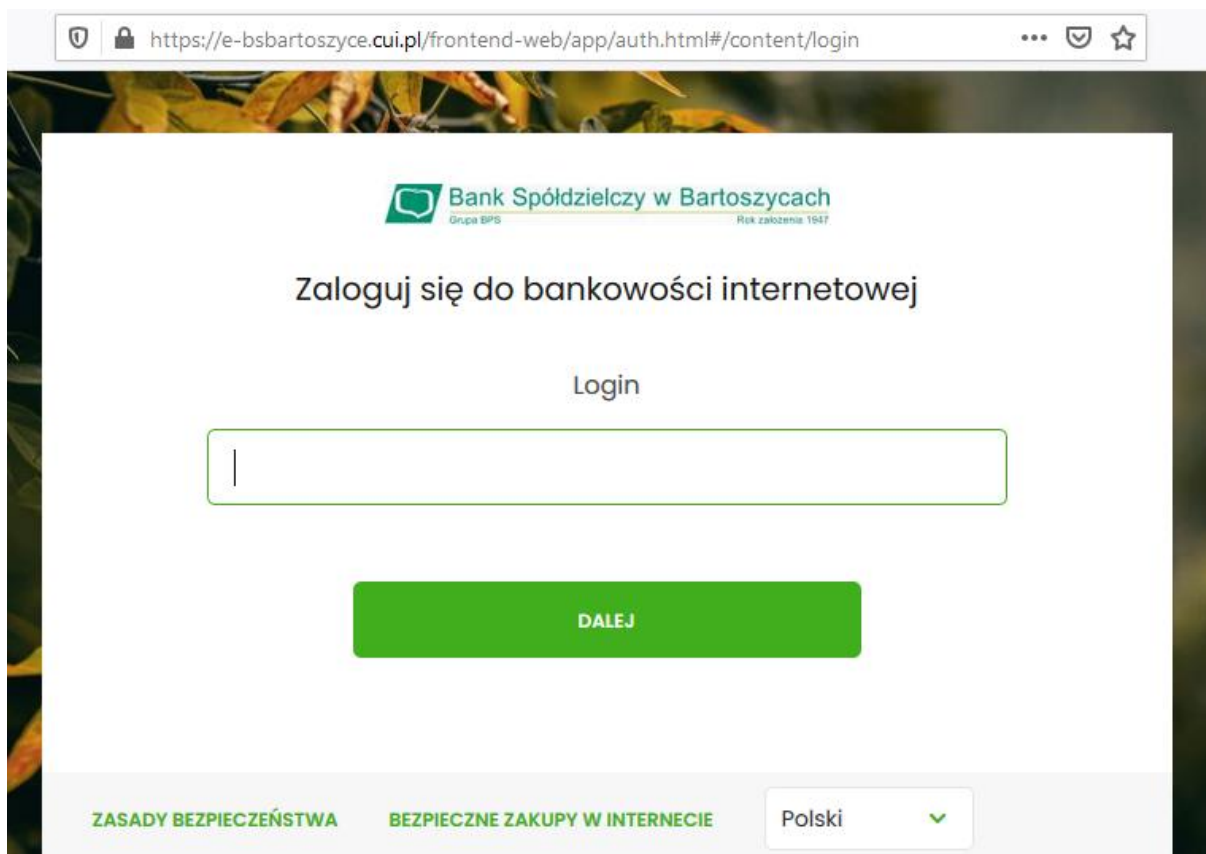
Rozdział 3. Logowanie do systemu

Uruchomienie aplikacji

W celu uruchomienia aplikacji należy:

- 1) Uruchomić przeglądarkę internetową
- 2) Wpisać, lub wybrać z listy adres strony:

<https://e-bsbartoszyce.cui.pl>



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.

Polski

Angielski

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 Asseco EBP zostaje wyświetlany pulpit z **miniaplikacjami**. Dostępność miniaplikacji na pulpicie jest uzależniona od **kontekstu** w jakim użytkownik zalogował się do systemu Asseco 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:



Kontrola usługi filtrowania IP w procesie logowania użytkownika

Funkcjonalność kontroli adresów IP dostępna jest tylko dla użytkowników logujących się do systemu Asseco 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 Asseco 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 Asseco EBP została wyłączona globalna kontrola adresów IP, wówczas logowanie użytkownika do systemu Asseco 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 Asseco EBP.

System umożliwia wprowadzenie konfiguracji adresów IP na dwóch poziomach:

- **globalnym** – po zalogowaniu użytkownika do systemu Asseco EBP w *kontekście firmowym*,
- **indywidualnym** – po zalogowaniu użytkownika do systemu Asseco 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 Asseco 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 Asseco 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 Asseco EBP. Adres IP zabroniony oznacza adres IP, z którego nie będzie możliwości dostępu do systemu Asseco EBP przez użytkownika, dla którego taki adres został zdefiniowany.

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

I. Logowanie do systemu za pomocą aplikacji mobilnej Asseco MAA

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

Pierwsze logowanie wraz z rejestracją urządzenia

W celu zmiany sposobu logowania na wniosek użytkownika (np. w Oddziale Banku), operator w Banku ustawia Priorytetowe urządzenie do logowania na *Mobilny podpis* oraz wysyła nowe tymczasowe **hasło MAA**. Wygenerowane hasło tymczasowe zostaje wysłane za pomocą SMS na numer telefonu użytkownika. Hasło wymagane jest przy logowaniu do systemu Asseco EBP (pierwszy krok uwierzytelniania). Użytkownik otrzymuje hasło po wpisaniu numeru identyfikacyjnego. Hasło ważne jest przez określony czas (np. 15 min).

Użytkownik powinien je zmienić przed upływem okresu ważności podczas logowania do systemu Asseco EBP.

Proces pierwszego logowania za pomocą aplikacji Asseco MAA do Asseco 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,

The image displays two screenshots of the Asseco MAA mobile application interface. The left screenshot shows the login screen with the title 'Zaloguj się do bankowości internetowej' and a 'Login' input field. Below the field is a green button labeled 'DALEJ'. At the bottom, there are links for 'ZASADY BEZPIECZEŃSTWA' and 'BEZPIECZNE ZAKUPY W INTERECIE', along with a language selector set to 'Polski'. The right screenshot shows the password entry screen with the title 'Logowanie' and the subtitle 'Zaloguj się do bankowości internetowej'. It features a numeric keypad for entering a 7-digit 'Kod dostępu'. Below the keypad is a green button labeled 'ZALOGUJ' and a 'COFNIJ' button.

- 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],

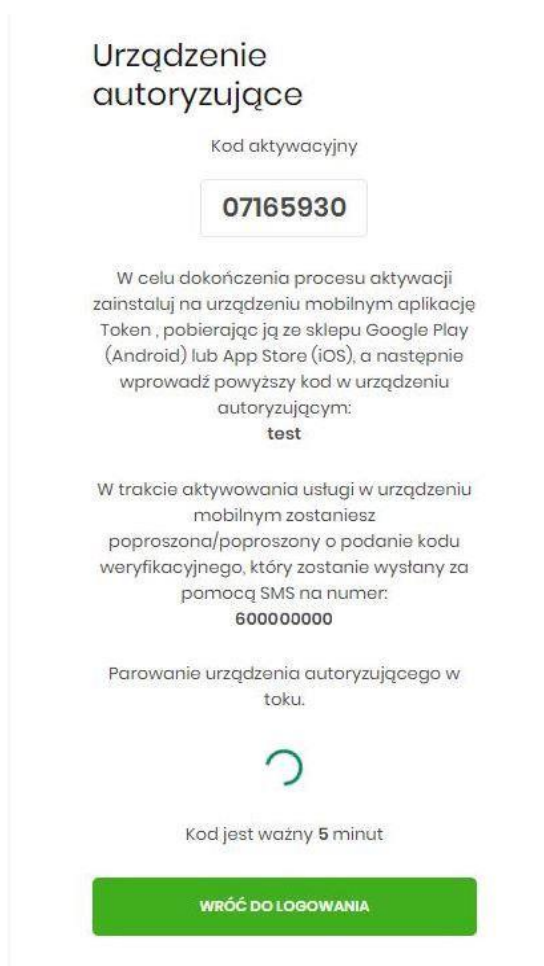
Urządzenie autoryzujące

Nazwa urządzenia

ZALOGUJ

COFNIJ

- system *Asseco EBP* za pośrednictwem systemu *GUARDIAN* generuje oraz prezentuje kod parowania urządzenia autoryzującego oraz komunikat jakie dane są wymagane do wprowadzenia przez użytkownika w aplikacji mobilnej *Asseco MAA* w celu potwierdzenia parowania. Po wpisaniu kodu aktywacyjnego w aplikacji *Asseco MAA* użytkownik otrzyma **SMS**, w celu potwierdzenia logowania do aplikacji *Asseco MAA*. Kroki do przejścia w aplikacji *Asseco MAA* zostały opisane w rozdziale ***Proces parowania urządzenia podczas pierwszego logowania w aplikacji MAA.***



W procesie rejestracji urządzenia autoryzującego podczas logowania użytkownika do systemu *Asseco 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.

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 Asseco 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 Asseco EBP i przechodzi do kolejnego okna za pomocą przycisku [DALEJ] w aplikacji Asseco MAA,
- następnie użytkownik wpisuje kod weryfikacyjny, przesłany za pomocą **SMS**,
(Rys.)

Asseco
KOD AKTYWACYJNY

Kod wygenerowany został w bankowości internetowej

Wprowadź kod aktywacyjny

1	2	3
4	5	6
7	8	9
	0	⊗

DALEJ

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 Asseco MAA oraz autoryzacji zdarzeń. PIN powinien składać się z 5-8 cyfr,
- następnie ponownie wprowadza PIN,

Asseco
NADAJ PIN

PIN służyć będzie do logowania oraz autoryzacji zdarzeń

..... ?

1	2	3
4	5	6
7	8	9
	0	⊗

DALEJ

Asseco
ZWERYFIKUJ PIN

Wprowadź ponownie PIN nadany w poprzednim kroku

.....

1	2	3
4	5	6
7	8	9
	0	⊗

DALEJ

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




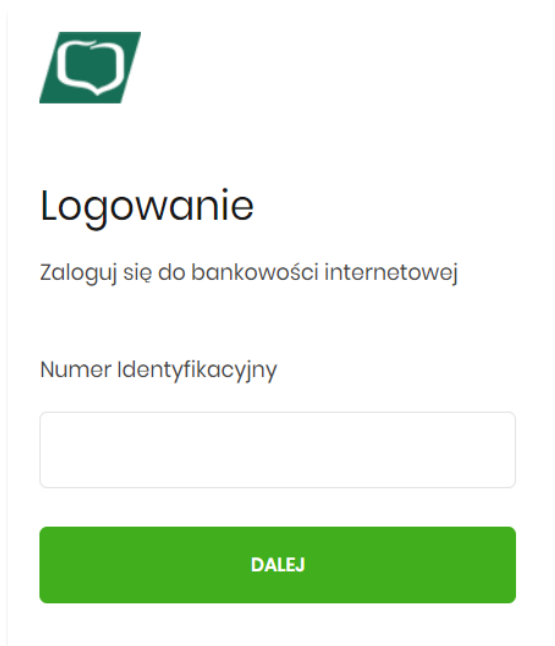
Użytkownik zostaje zalogowany do bazy danych internetowej w systemie **Asseco EBP** oraz może zalogować się do aplikacji **Asseco MAA**.

Logowanie po rejestracji urządzenia

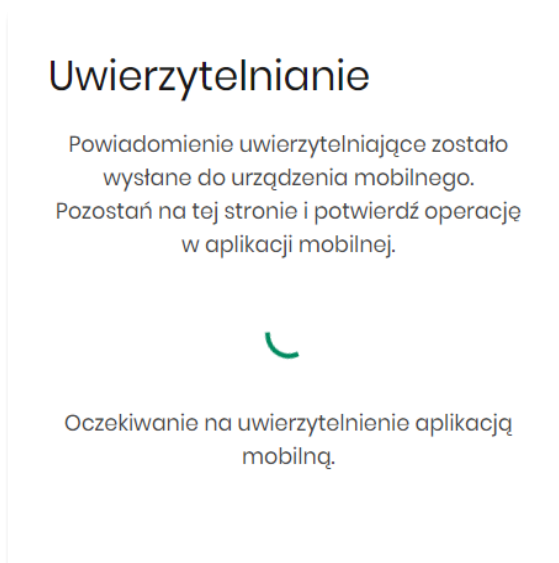
Użytkownik ma możliwość zalogowania się do systemu *Asseco EBP* za pomocą aplikacji mobilnej *Asseco MAA*, jeżeli posiada sparowane aktywne urządzenie oraz hasło stałe.

Proces logowania za pomocą aplikacji mobilnej *Asseco MAA* do systemu *Asseco 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 operatora w Banku) i wybiera przycisk [ZALOGUJ],



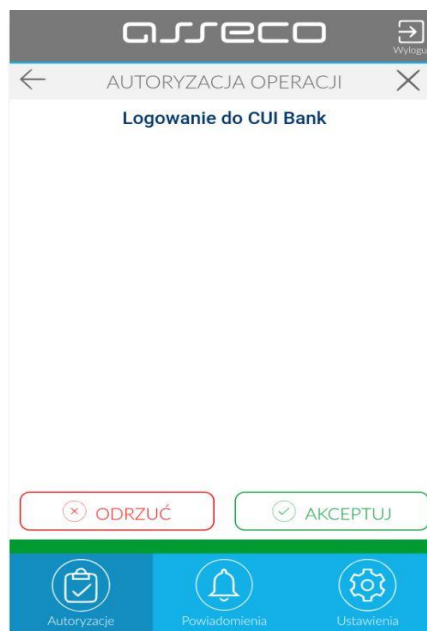
- system *Asseco EBP* prezentuje ekran informujący o wysłaniu dyspozycji logowania do aplikacji *Asseco MAA*,



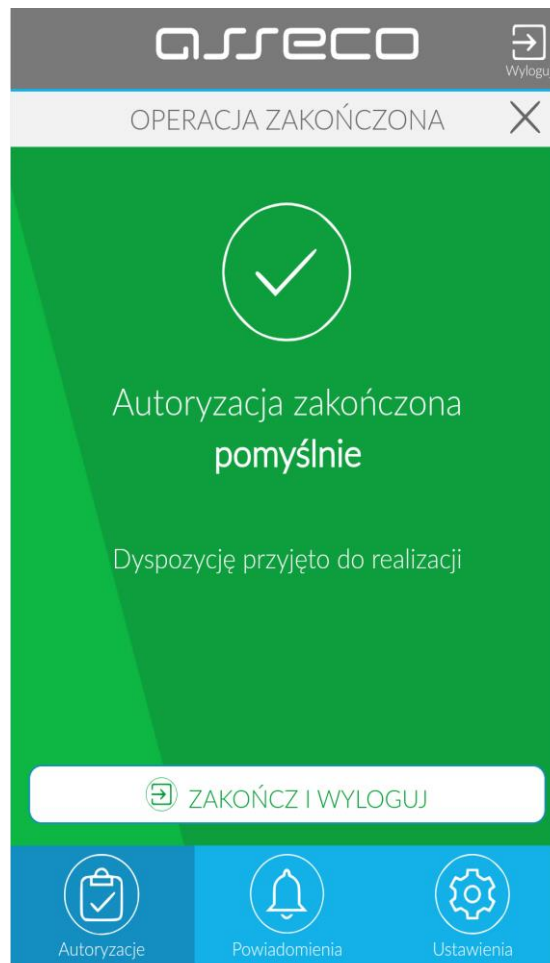
- system Asseco EBP za pośrednictwem systemu GUARDIAN wysyła do aplikacji Asseco MAA powiadomienie PUSH o nowej dyspozycji logowania,
- aplikacja Asseco MAA wyświetla na urządzeniu mobilnym baner powiadomienia PUSH z informacją o oczekującym powiadomieniu,
- użytkownik wybiera baner powiadomienia PUSH,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



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



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

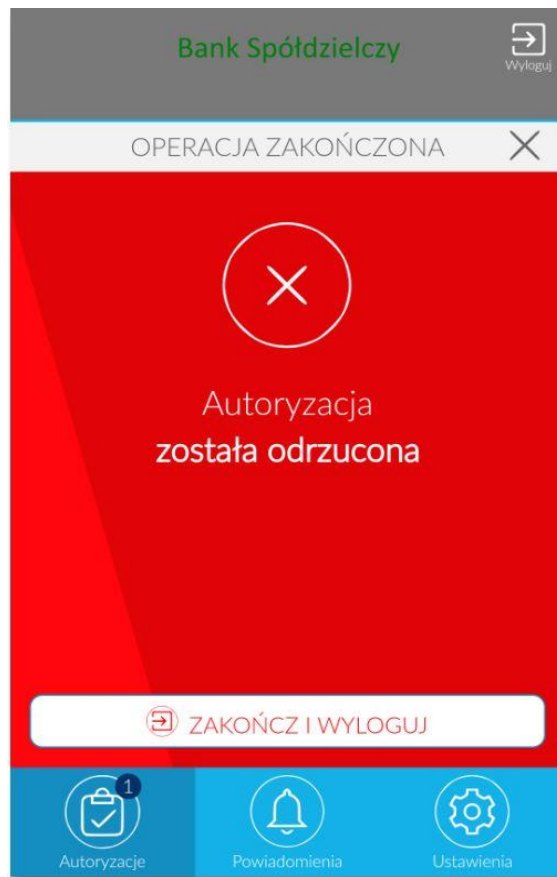


W przypadku, gdy użytkownik nie potwierdził autoryzacji dyspozycji logowania w określonym czasie po wskazaniu dyspozycji w aplikacji mobilnej Asseco MAA, wówczas zostanie zaprezentowany następujący komunikat:

- *Upłynął czas akceptacji dyspozycji.*

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

- *Autoryzacja została odrzucona.*



W procesie logowania do systemu *Asseco EBP* za pomocą aplikacji mobilnej *Asseco 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 *Asseco MAA*.

II. Logowanie do systemu Asseco EBP przy pomocy karty mikroprocesorowej

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

Pierwsze logowanie do systemu *Asseco EBP* za pomocą karty mikroprocesorowej wraz z rejestracją urządzenia

Proces pierwszego logowania za pomocą karty mikroprocesorowej do *Asseco 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
SG4EPQBUV

ZALOGUJ SIĘ ZA POMOCĄ E-PODPISU

COFNIJ

ZASADY BEZPIECZEŃSTWA
BEZPIECZNE ZAKUPY W INTERNECIE

ASSECO

Pamiętaj o podstawowych zasadach bezpieczeństwa.

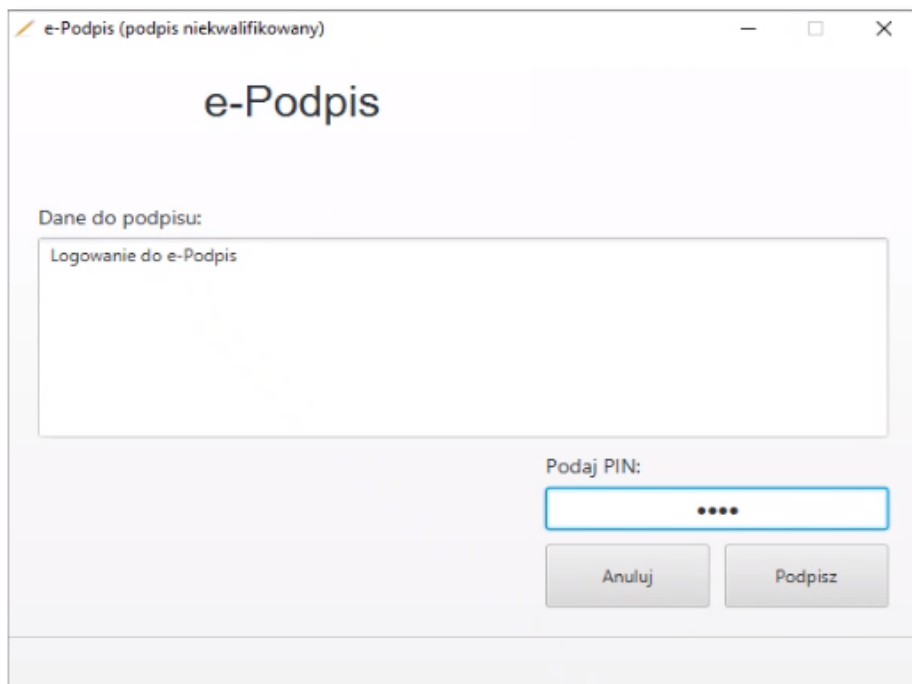
Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę Symantec

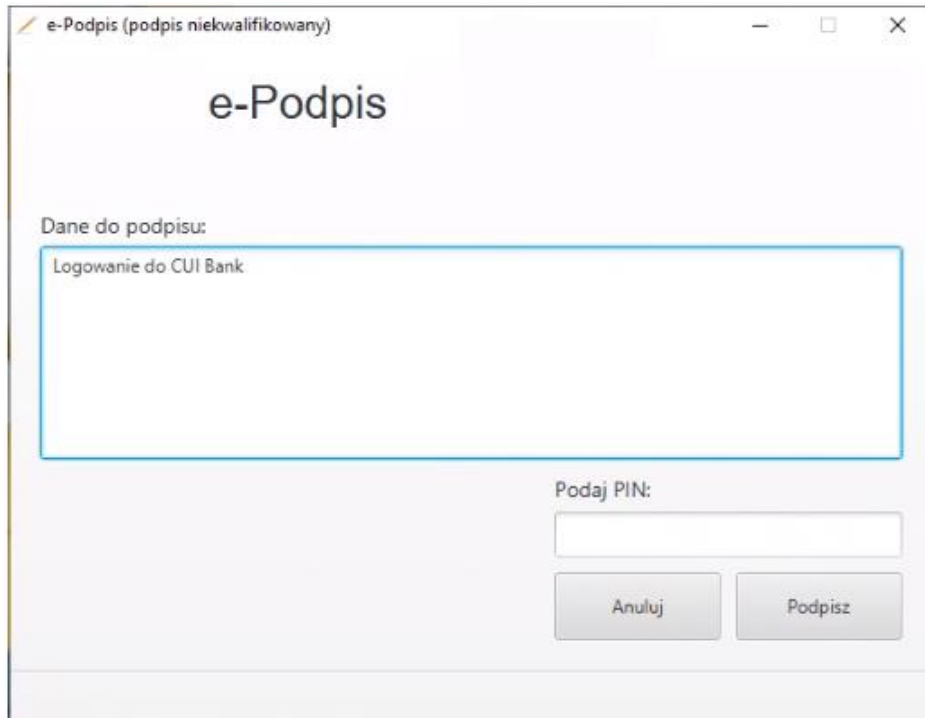
Pamiętaj!
Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na komputerach użytkowników.

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**.



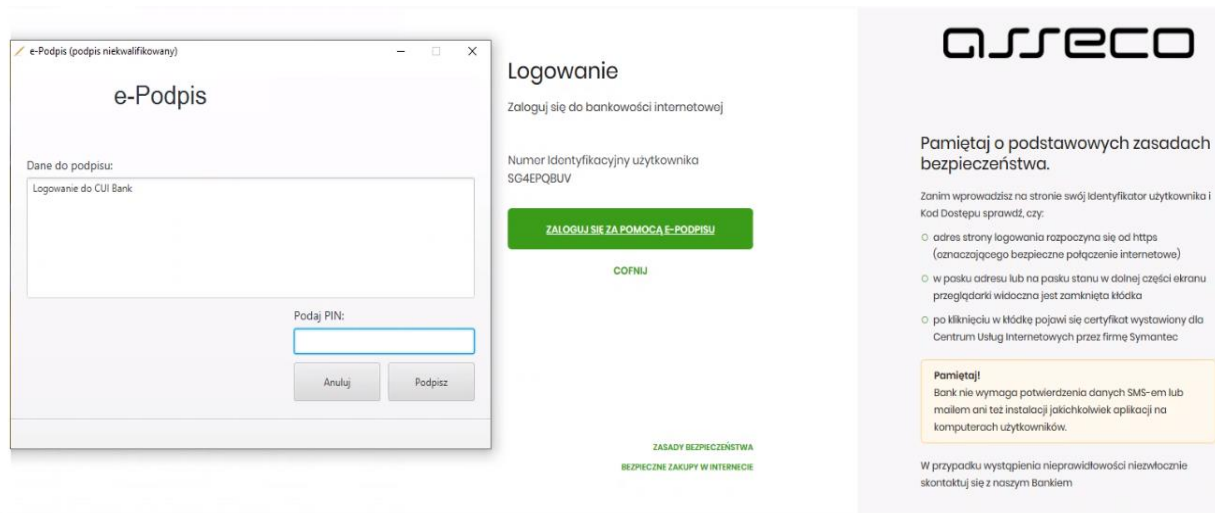
- użytkownik wpisuje PIN, następnie naciska przycisk [PODPISZ], system sprawdza aplikacja sprawdza poprawność wprowadzonych.
- po poprawnej weryfikacji wprowadzonego PIN-u, system na stronie logowania do systemu Asseco EBP prezentuje ekran do wprowadzenia PIN karty mikroprocesorowej.



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

Kolejne logowanie do systemu Asseco EBP za pomocą karty mikroprocesorowej

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



Po poprawnym wprowadzeniu PIN system loguje użytkownika do systemu Asseco EBP.

III. Logowanie do systemu Asseco EBP przy pomocy hasła maskowanego + kodu SMS

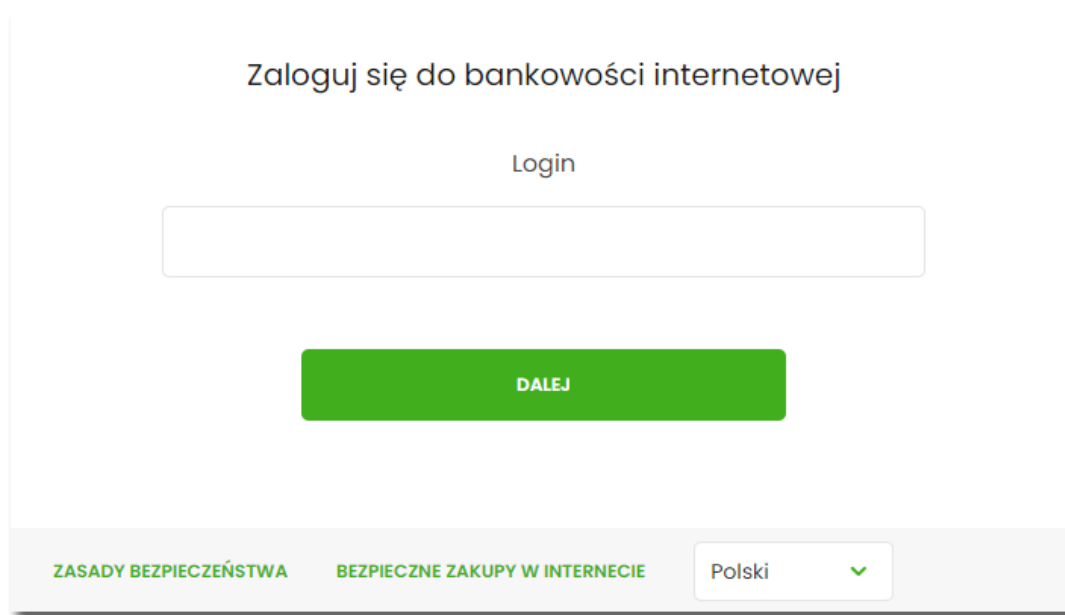
Użytkownik ma możliwość zalogowania się do systemu Asseco EBP za pomocą hasła maskowanego + kodu SMS.

Pierwsze logowanie do systemu Asseco EBP przy pomocy hasła maskowanego + kodu SMS

W celu zmiany sposobu logowania na wniosek użytkownika (np. w Oddziale Banku), operator w Banku ustawia *Priorytetowe urządzenie do logowania* na *Hasło maskowane + kod sms* oraz wysyła nowe hasło. Wygenerowane hasło tymczasowe zostaje wysłane za pomocą **SMS** na numer telefonu użytkownika. Hasło wymagane jest przy logowaniu do systemu *Asseco EBP* (pierwszy krok uwierzytelniania). **Użytkownik otrzymuje hasło po wpisaniu numeru identyfikacyjnego**. Hasło ważne jest przez określony czas (np. 15 min).

Użytkownik powinien je zmienić przed upływem okresu ważności podczas logowania.

Po uruchomieniu systemu *Asseco EBP* wyświetlane jest okno logowania:



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 tę 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],

Zaloguj się do bankowości internetowej

Wpisz wskazane znaki hasła dla LTREGRES

1 2 3 4 5 6 7 8

ZALOGUJ

ANULUJ

ZASADY BEZPIECZEŃSTWA BEZPIECZNE ZAKUPY W INTERNECIE

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

Zaloguj się do bankowości internetowej

Wysłaliśmy SMS z kodem autoryzującym logowanie dla LTREGRES.

Wpisz kod poniżej:

ZALOGUJ

ANULUJ

ZASADY BEZPIECZEŃSTWA BEZPIECZNE ZAKUPY W INTERNECIE

- 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

Zaloguj się do bankowości internetowej

Podczas pierwszego logowania, wymagane jest ustawienie swojego hasła.

Wprowadź nowe hasło

Powtórz nowe hasło

ZAPISZ I ZALOGUJ

Wymagania do hasła:

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

ZASADY BEZPIECZEŃSTWA BEZPIECZNE ZAKUPY W INTERNECIE

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

Dodanie urządzenia zaufanego podczas logowania.

Użytkownik ma możliwość dodania urządzenia zaufanego, dzięki czemu będzie mógł się zalogować do systemu bez podania SMS.

Podczas logowania do systemu *Asseco EBP*, użytkownik musi wprowadzić:

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

Zaloguj się do bankowości internetowej

Wysłałiliśmy SMS z kodem autoryzującym logowanie dla LTREGRES.

Wpisz kod poniżej:

Czy wiesz, że możesz nie zatwierdzać za każdym razem logowania poprzez SMS? Wystarczy, że dodasz to urządzenie (**ChromeWindows10**) do "zaufanych".

ZALOGUJ

ZALOGUJ I DODAJ DO ZAUFANYCH

ANULUJ

ZASADY BEZPIECZEŃSTWA BEZPIECZNE ZAKUPY W INTERNECIE

W przypadku wprowadzenia poprawnych danych, użytkownik zostanie zalogowany do systemu *Asseco EBP*, natomiast urządzenie zostanie zapisane do urządzeń zaufanych.

Po zalogowaniu (podaniu danych uwierzytelniających) do aplikacji *Asseco EBP* weryfikowany jest status użytkownika w kontekście akceptacji i jeśli dane użytkownika są zmieniane lub weryfikowane (przez operatora w Banku) wówczas dalsza praca z systemem nie jest możliwa, a użytkownik otrzymuje komunikat:

Praca w systemie nie jest obecnie możliwa. Zlecone przez Ciebie zmiany w dostępie są obecnie wprowadzane w Banku. Spróbuj ponownie później bądź skontaktuj się ze swoim Doradcą lub Teleserwisem.

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

Podczas kolejnego logowania do systemu Asseco 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 *Asseco EBP*, natomiast w przypadku wprowadzenia błędnych danych, system zaprezentuje odpowiedni komunikat. W przypadku wprowadzenia:

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

Zaloguj się do bankowości internetowej

Wpisz wskazane znaki hasła dla LTREGRES

1 2 3 4 5 6 7 8

Błąd na etapie uwierzytelniania

ZALOGUJ

ANULUJ

ZASADY BEZPIECZEŃSTWA BEZPIECZNE ZAKUPY W INTERECIE

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

Zaloguj się do bankowości internetowej

Wysłaliśmy SMS z kodem autoryzującym logowanie dla LTREGRES.

Wpisz kod poniżej:

Błędny kod SMS

Czy wiesz, że możesz nie zatwierdzać za każdym razem logowania poprzez SMS? Wystarczy, że dodasz to urządzenie (ChromeWindows10) do "zaufanych"!

ZALOGUJ

ZALOGUJ I DODAJ DO ZAUFANYCH

ANULUJ

ZASADY BEZPIECZEŃSTWA BEZPIECZNE ZAKUPY W INTERECIE

Po zalogowaniu (podaniu danych uwierzytelniających) do aplikacji *Asseco EBP* weryfikowany jest status użytkownika w kontekście akceptacji i jeśli dane użytkownika są zmieniane lub weryfikowane (przez operatora w Banku) wówczas dalsza praca z systemem nie jest możliwa, a użytkownik otrzymuje komunikat:

Praca w systemie nie jest obecnie możliwa. Zlecone przez Ciebie zmiany w dostępie są obecnie wprowadzane w Banku. Spróbuj ponownie później bądź skontaktuj się ze swoim Doradcą lub Teleserwisem.

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

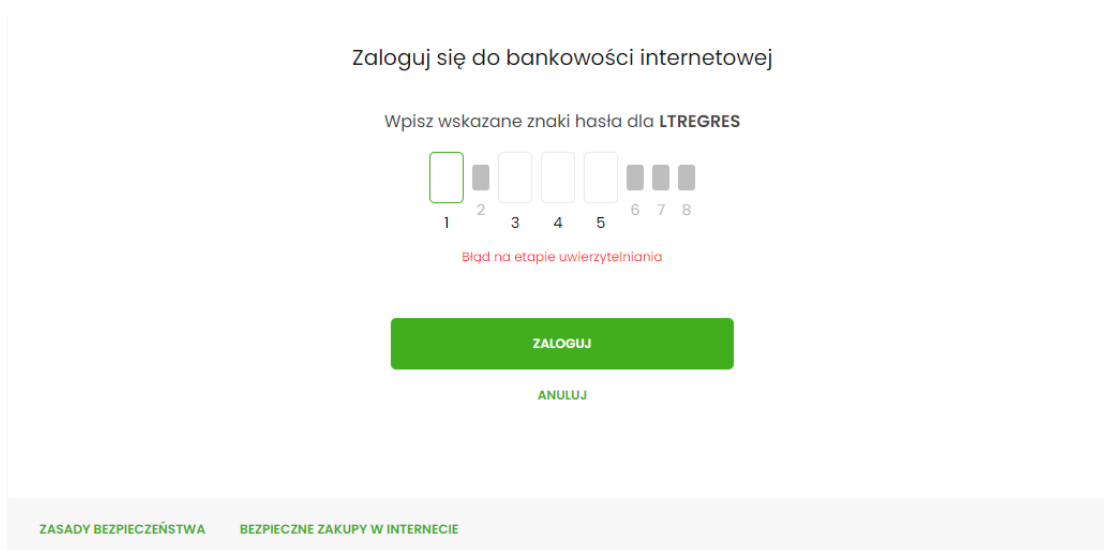
Podczas kolejnego logowania do systemu Asseco EBP, użytkownik musi wprowadzić:

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

W przypadku wprowadzenia poprawnych danych, użytkownik zostanie od razu zalogowany do systemu *Asseco EBP*, ponieważ system zweryfikuje, czy Użytkownik loguje się za pomocą dodanego **urządzenie zaufanego** na podstawie nazwy i wersji systemu operacyjnego oraz rodzaju przeglądarki internetowej.

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 for 'Zaloguj się do bankowości internetowej'. It prompts the user to 'Wpisz wskazane znaki hasła dla LTREGRES' and displays eight input fields numbered 1 to 8. Field 1 is active. Below the fields, a red error message reads 'Błąd na etapie uwierzytelniania'. At the bottom, there are two buttons: a green 'ZALOGUJ' button and a smaller green 'ANULUJ' button. The footer contains the text 'ZASADY BEZPIECZEŃSTWA' and 'BEZPIECZNE ZAKUPY W INTERNECIE'.

Po zalogowaniu (podaniu danych uwierzytelniających) do aplikacji Asseco EBP weryfikowany jest status użytkownika w kontekście akceptacji i jeśli dane użytkownika są zmieniane lub weryfikowane (przez operatora w Banku) wówczas dalsza praca z systemem nie jest możliwa, a użytkownik otrzymuje komunikat:

Praca w systemie nie jest obecnie możliwa. Zlecone przez Ciebie zmiany w dostępie są obecnie wprowadzane w Banku. Spróbuj ponownie później bądź skontaktuj się ze swoim Doradcą lub Teleserwisem.

Rozdział 4. Metody autoryzacji zleceń

Po uzyskaniu dostępu do aplikacji *Asseco EBP* użytkownik może korzystać z oferowanych mu funkcji aplikacji w celu wykonywania operacji bankowych w ramach udostępnionych mu rachunków bieżących.

W aplikacji *Asseco 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**.

I. Mobilny podpis

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

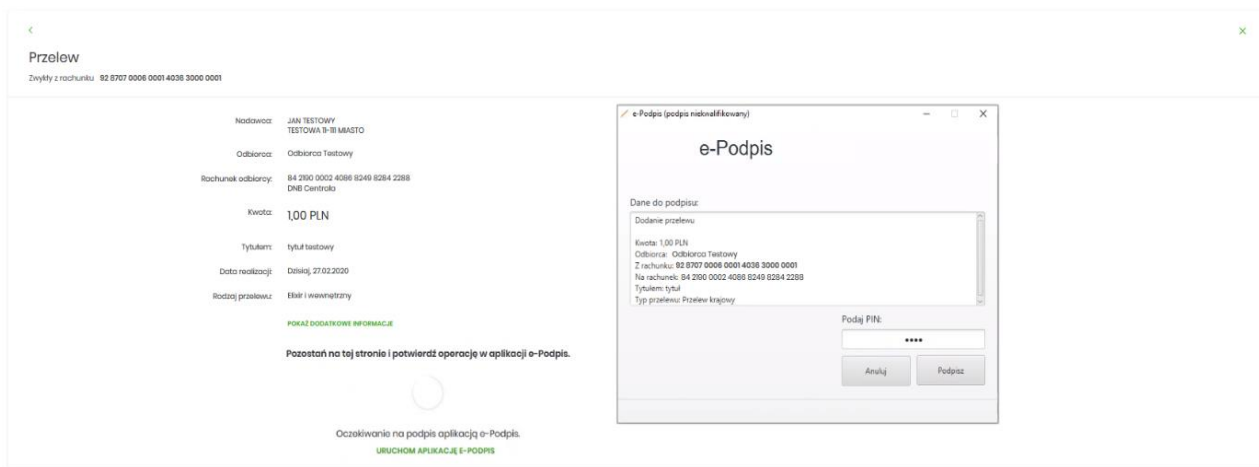
W procesie autoryzacji dyspozycji za pomocą aplikacji mobilnej **Asseco MAA** mogą wystąpić następujące komunikaty informujące o błędzie:

- *Nastąpiło przekroczenie czasu oczekiwania na autoryzację*, w przypadku:
 - braku podpisania dyspozycji w określonym czasie.
- *Autoryzacja została odrzucona*, w przypadku:
 - odrzucenia autoryzacji w aplikacji mobilnej *Asseco 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.

II. Karta mikroprocesorowa

Autoryzacja dyspozycji przy pomocy **karty mikroprocesorowej**.

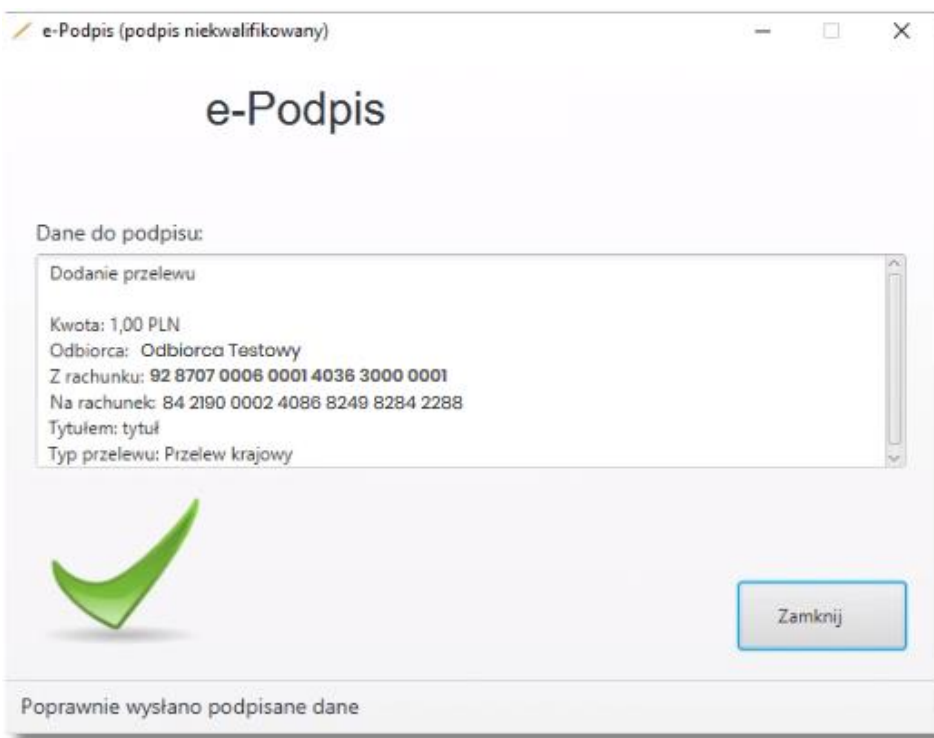
Po wprowadzeniu danych dyspozycji przelewu i naciśnięciu [DALEJ] system prezentuje formularz potwierdzenia wprowadzonych danych wraz oknem do wprowadzenia kodu PIN



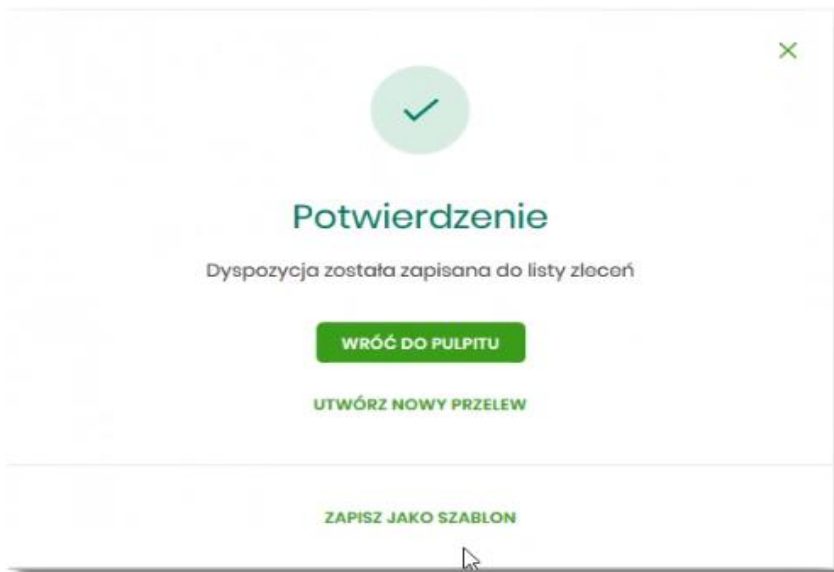
Na formularzu **e-Podpis** dostępne są akcje:

- [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.



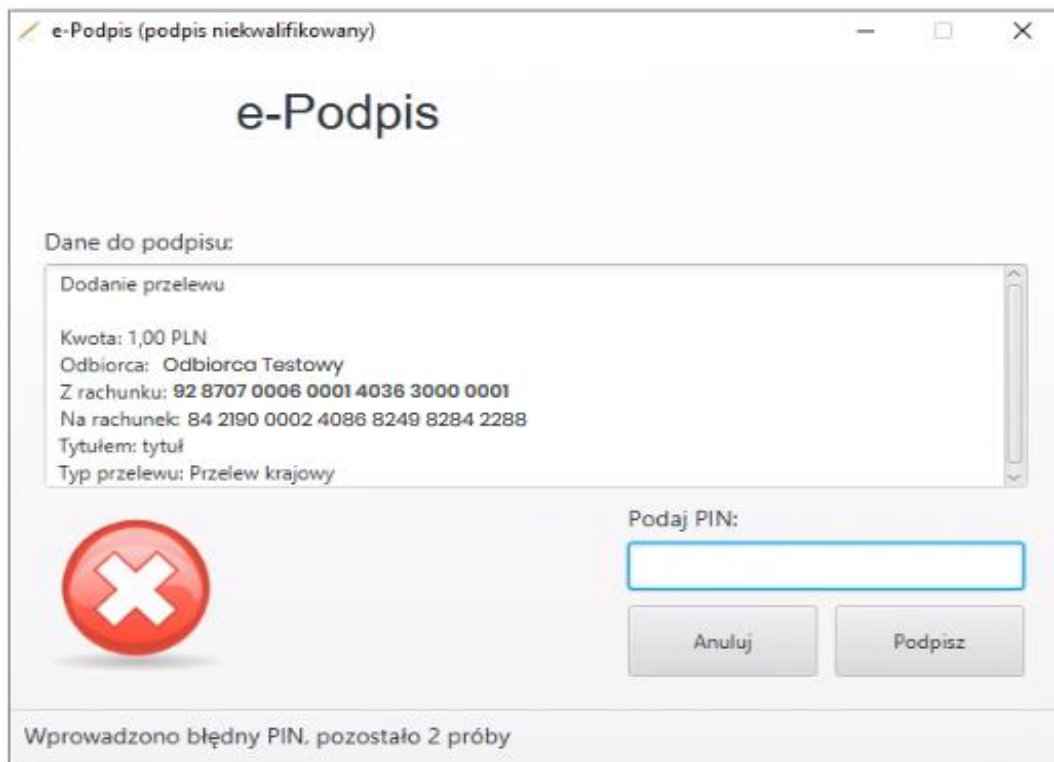
Po naciśnięciu [ZAMKNIJ] system prezentuje formularz z potwierdzeniem realizacji dyspozycji.



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.

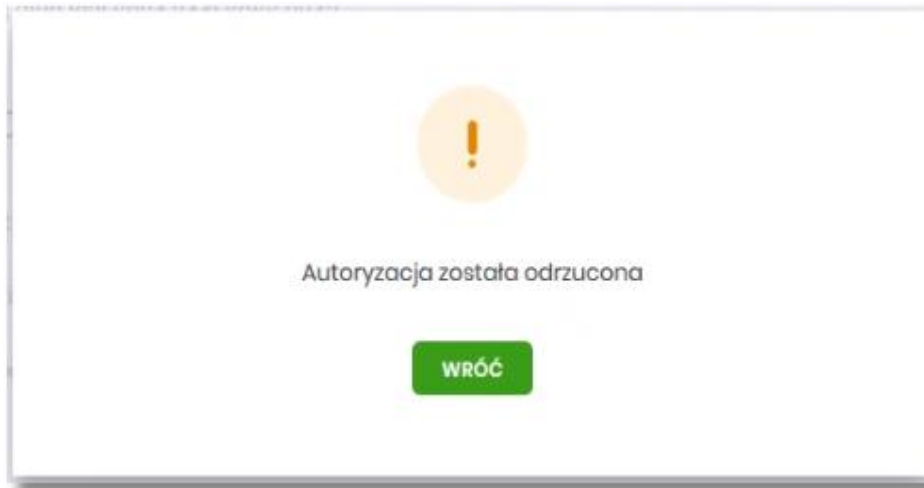
W przypadku gdy użytkownik wprowadzi błędny kod PIN system zaprezentuje komunikat:



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:

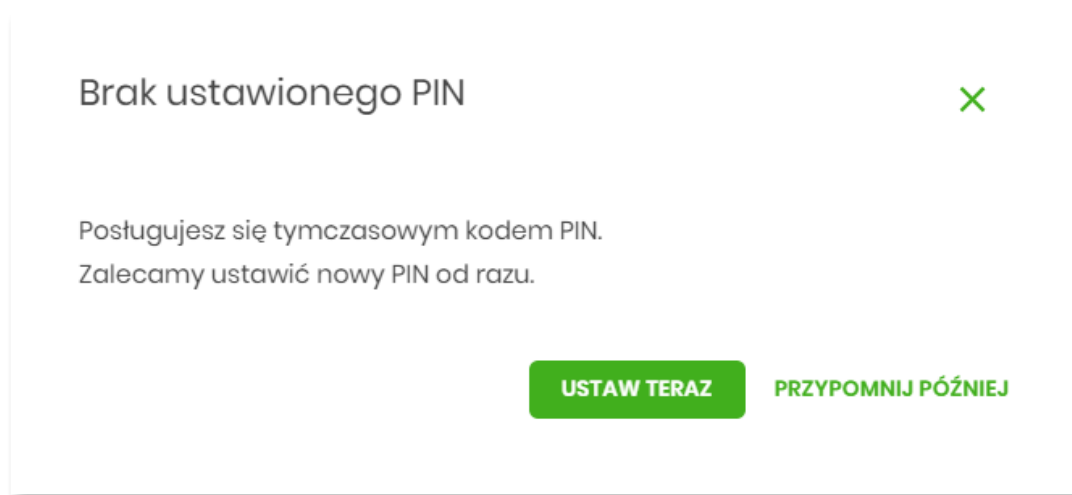


III. Kod PIN + kod SMS

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

Operator w Banku ustawia *Priorytetowe urządzenie do autoryzacji* na *Kod PIN + Kod SMS* oraz ustawia *hasło tymczasowe*. Wygenerowane hasło tymczasowe zostaje wysłane za pomocą SMS na numer telefonu użytkownika.

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 PIN do autoryzacji**.



Wybór przycisku [USTAW TERAZ] powoduje przeniesienie użytkownika do formatki **ZMIANA PIN DO AUTORYZACJI**.

PIN ważny jest przez określony czas (np. 15 min).

<
>

Zmiana PIN do autoryzacji

Obecny PIN

Nowy PIN

Powtórz nowy PIN

ZATWIERDŹ

Zadbaj o zachowanie poufności swojego PIN.

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

Zasady budowy PIN są następujące:

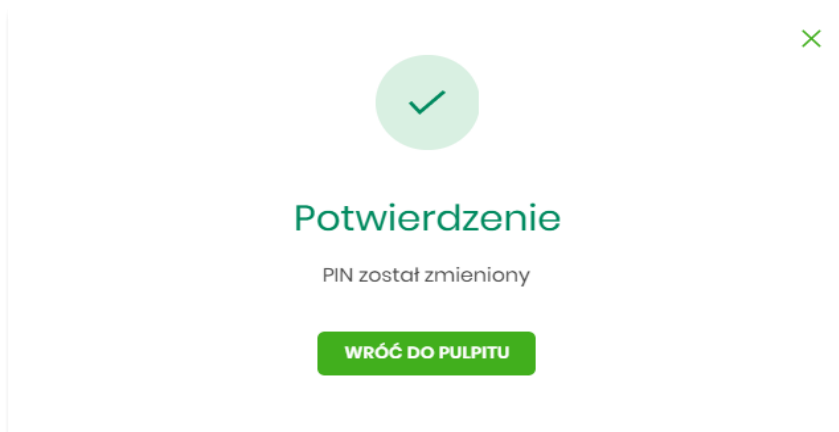
- musi składać się z 4-8 znaków
- musi zawierać przynajmniej jedną wielką literę
- musi zawierać przynajmniej jedną małą literę
- musi zawierać przynajmniej jeden znak specjalny
- musi zawierać przynajmniej jedną cyfrę
- może zawierać wyłącznie znaki ze zbioru: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!@#%&*()-_+[]\|;:","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

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.:

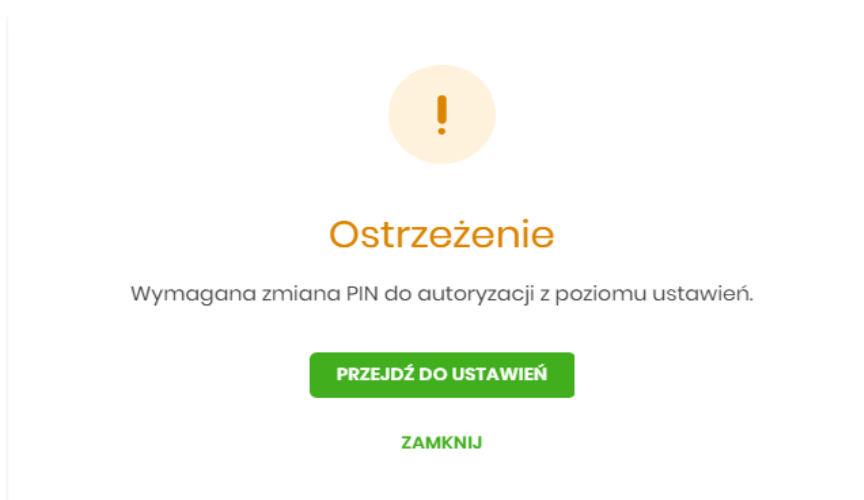
- musi składać się z 4-8 znaków,
- musi zawierać przynajmniej jedną wielką literę,
- musi zawierać przynajmniej jedną małą literę,
- musi zawierać przynajmniej jeden znak specjalny,
- musi zawierać przynajmniej jedną cyfrę,
- może zawierać wyłącznie znaki ze zbioru:
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!@#%&*()-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

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 PIN, prezentując odpowiedni komunikat:



Wybór przycisku [PRZEJDŹ DO USTAWIEŃ] powoduje przeniesienie użytkownika do formatki *ZMIANA PIN DO AUTORYZACJI*.

PIN ważny jest przez określony czas (np. 15 min).

Po zmianie PIN 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 PIN 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