Spółdzielcza Grupa Bankowa

Bank Spółdzielczy w Sandomierzu

Rok założenia 1926

Przewodnik dla klienta

„Małych, średnich i dużych przedsiębiorstw”

Spis treści

1. Logowanie do systemu

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

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

W tym celu należy przejść na stronę www.sandomierz.cui.pl lub poprzez stronę banku.

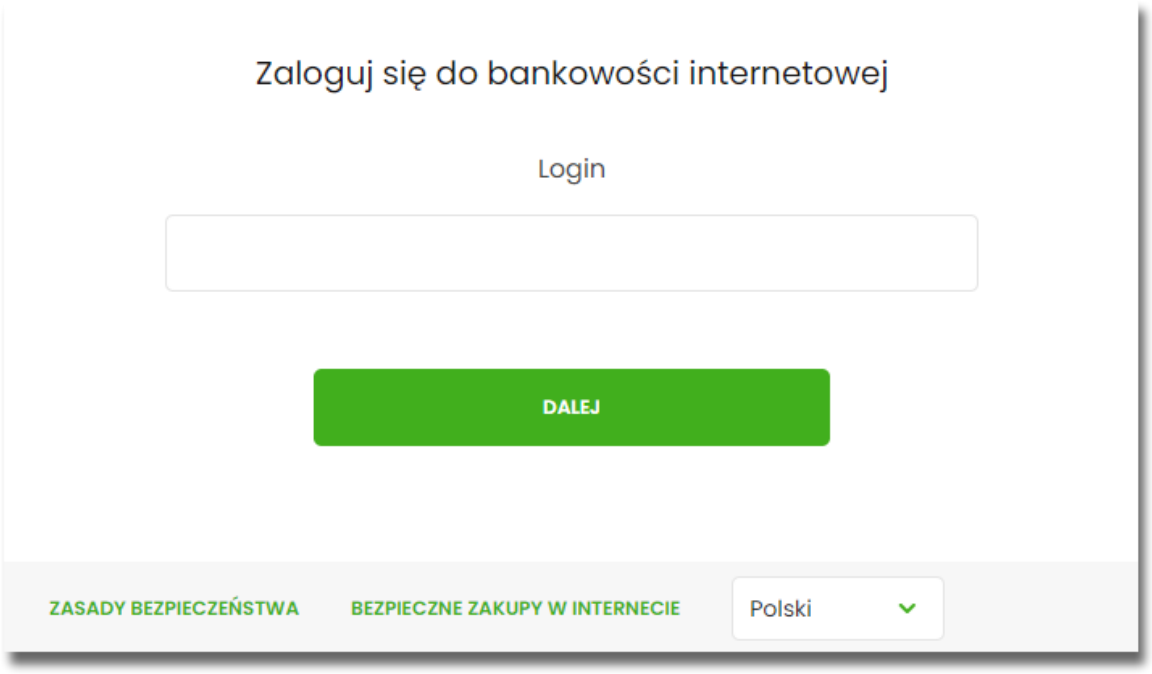
1.1. Logowanie do systemu za pomocą aplikacji mobilnej BSGo

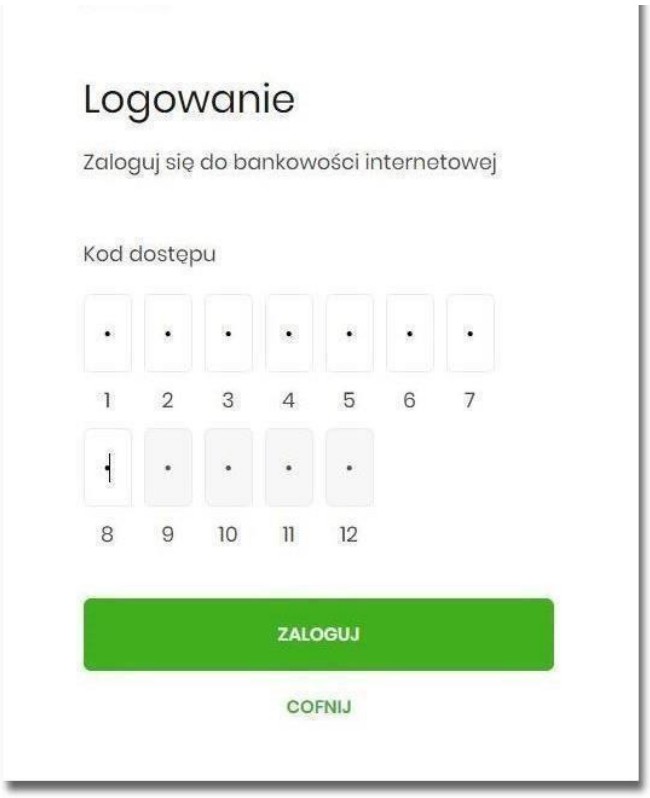
Użytkownik ma możliwość zalogowania się do systemu Asseco EBP za pomocą aplikacji mobilnej BSGo pobranej ze sklepu - Google Play (Android), App Store (iOS) i zainstalowanej na urządzeniu mobilnym.

1.2. Pierwsze logowanie wraz z rejestracją urządzenia

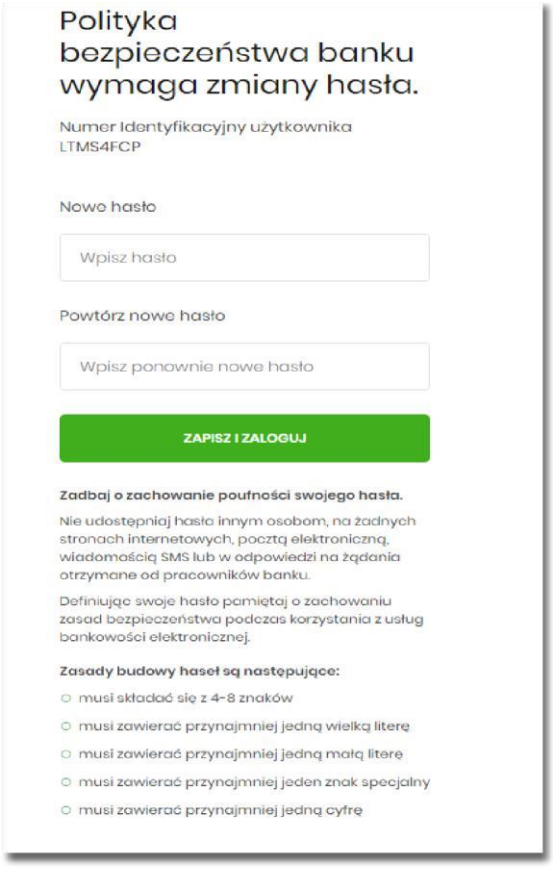
Proces pierwszego logowania za pomocą aplikacji BSGo do Asseco EBP w przypadku gdy Użytkownik nie posiada aktywnego sparowanego urządzenia autoryzującego przebiega w następujący sposób:

Użytkownik wprowadza numer identyfikacyjny oraz otrzymane za pomocą sms hasło tymczasowe,





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



Użytkownik wpisuje nazwę urządzenia autoryzującego (np. nazwę telefonu) i wybiera przycisk [ZALOGUJ],

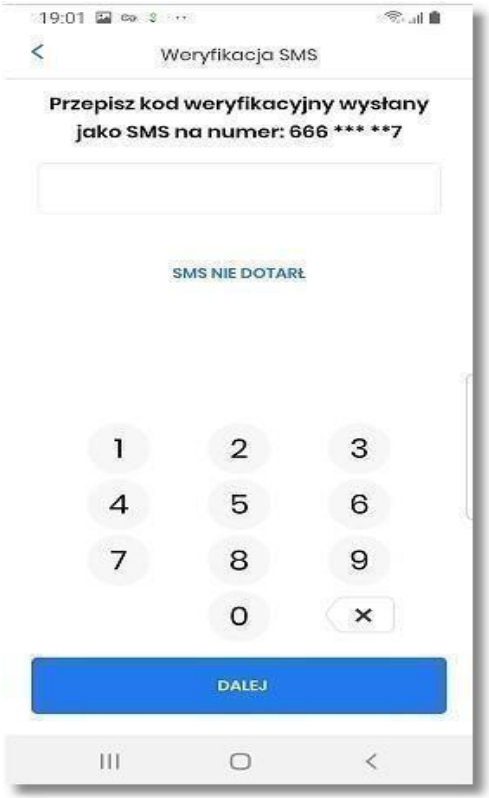
System Asseco EBP prezentuje kod parowania urządzenia autoryzującego który należy wpisać w aplikacji mobilnej BSGo.

.

Użytkownik otwiera zainstalowaną aplikację BSGo 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]

Następnie Użytkownik wpisuje kod weryfikacyjny, przesłany za pomocą SMS,



Użytkownik nadaje PIN, który będzie służył do logowania do aplikacji BSGo oraz autoryzacji zdarzeń. PIN musi składać się z 5-8 cyfr. Należy go wpisać dwukrotnie.

Po prawidłowym nadaniu PIN-u, system umożliwia użytkownikowi ustawienie metody logowania.

Metody logowania udostępniane przez system to:

- Kod PIN - dla systemu android oraz iOS,
- metody biometryczne:

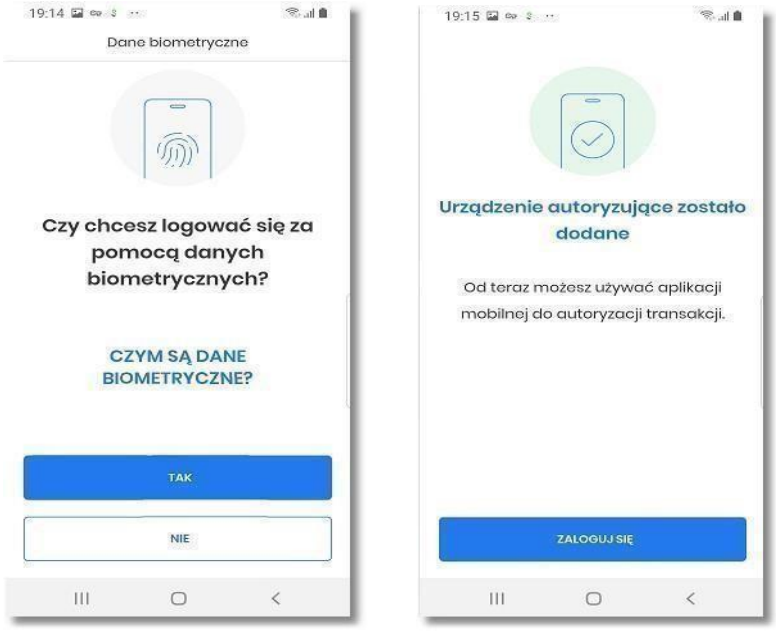
◦ Odcisk palca - dla systemu android oraz iOS,

◦ Face Id - dla systemu iOS,

Opcja 'Odcisk palca' oraz 'Face Id' może być wybrana, gdy urządzenie zostało uprzednio skonfigurowane do takiej obsługi.

W celu wyboru metody system prezentuje formularz Dane biometryczne udostępniający zestaw akcji:

- [CZYM SĄ DANE BIOMETRYCZNE] - umożliwia wyświetlenie użytkownikowi komunikatu informacyjnego,
- [TAK] – umożliwia włączenie metody biometrycznej w procesie logowania:
- [NIE] – umożliwia rezygnacje z metody biometrycznej, tym samy logowanie do aplikacji hybrydowej odbywać się będzie przy pomocy ustawionego kodu PIN,



Po dokonaniu aktywacji aplikacji i ustaleniu sposobu logowania za pomocą PIN-u lub danych biometrycznych, użytkownikowi wyświetlany jest ekran informujący o dodaniu urządzenia autoryzującego.

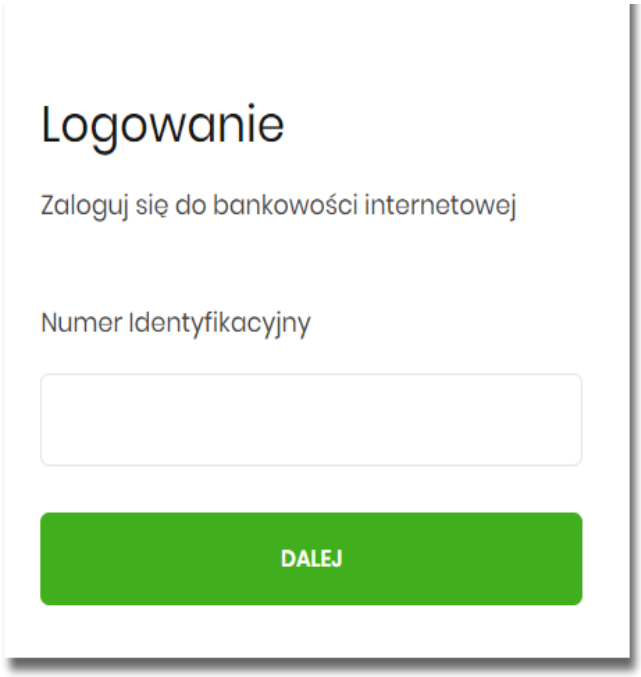
Użytkownik zostaje zalogowany do bakowości internetowej w systemie Asseco EBP oraz może ponownie zalogować się do aplikacji BSGo.

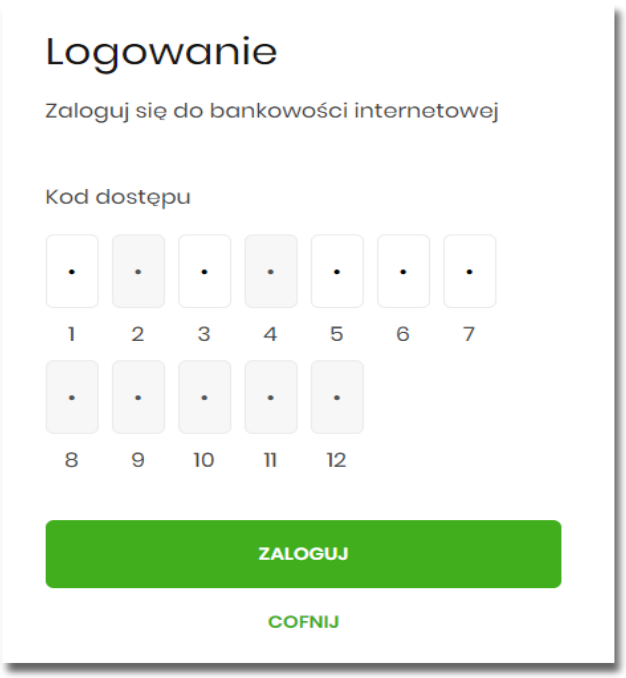
1.3. Logowanie po rejestracji urządzenia

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

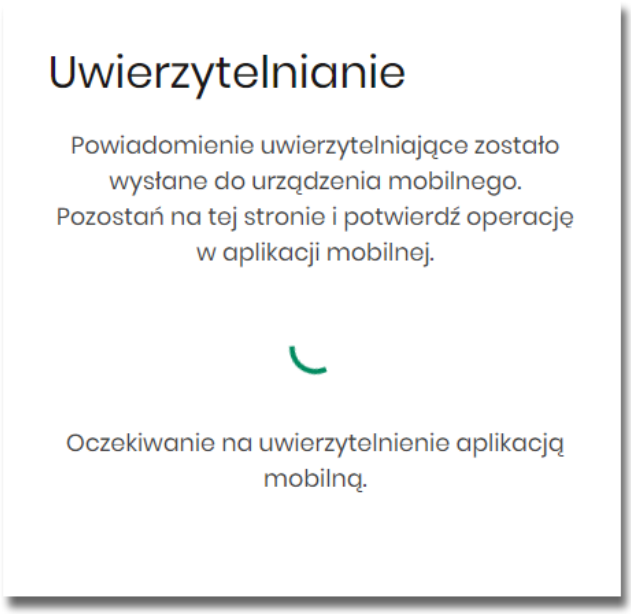
Proces logowania za pomocą aplikacji do systemu Asseco EBP przebiega w następujący sposób:

Użytkownik wpisuje numer identyfikacyjny i hasło (ustawione przez Użytkownika) i wybiera przycisk [ZALOGUJ],





System Asseco EBP prezentuje ekran informujący o wysłaniu dyspozycji logowania do aplikacji Asseco MAA,



- system Asseco EBP wysyła do aplikacji BSGo powiadomienie PUSH o nowej dyspozycji logowania,

- aplikacja wyświetla na urządzeniu mobilnym baner powiadomienia PUSH z informacją o oczekującym powiadomieniu,
- Użytkownik wybiera baner powiadomienia PUSH, które uruchamia aplikację mobilną lub bezpośrednio uruchamia aplikację z systemu operacyjnego urządzenia mobilnego, • Użytkownik loguje się do aplikacji,

Po zalogowaniu się do aplikacji zobaczymy ekran z możliwością akceptacji lub odrzucenia. Wybieramy „akceptuj”. Po czym otrzymamy powiadomienie o udanej autoryzacji oraz Użytkownik zostaje zalogowany do systemu Asseco EBP,

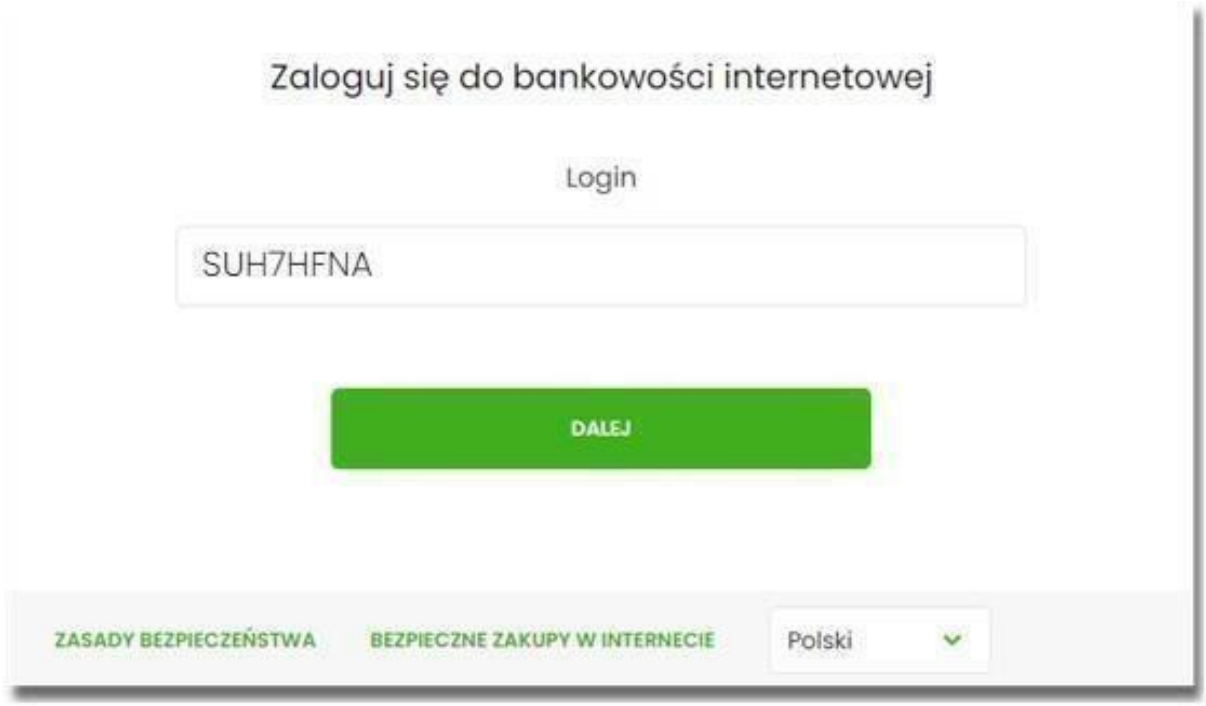
2. Logowanie do systemu Asseco EBP przy pomocy karty mikroprocesorowej

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

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

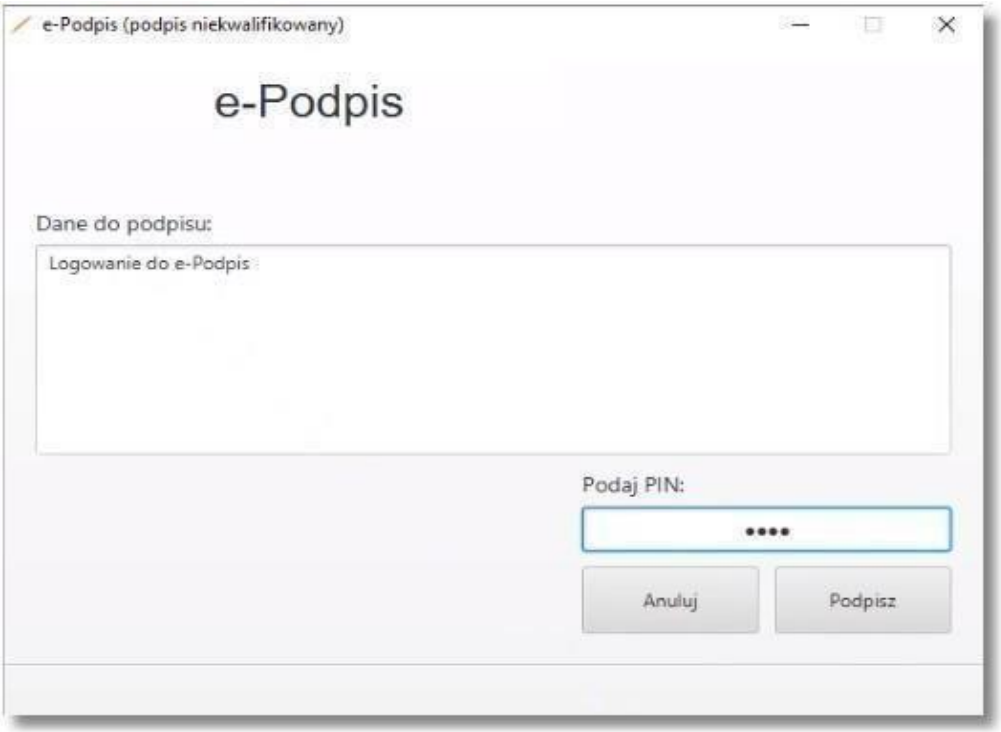
Proces pierwszego logowania za pomocą karty mikroprocesorowej do Asseco EBP przebiega w następujący sposób:

Użytkownik na formatce logowania wprowadza identyfikator i przechodzi do drugiego kroku naciskając przycisk [DALEJ].

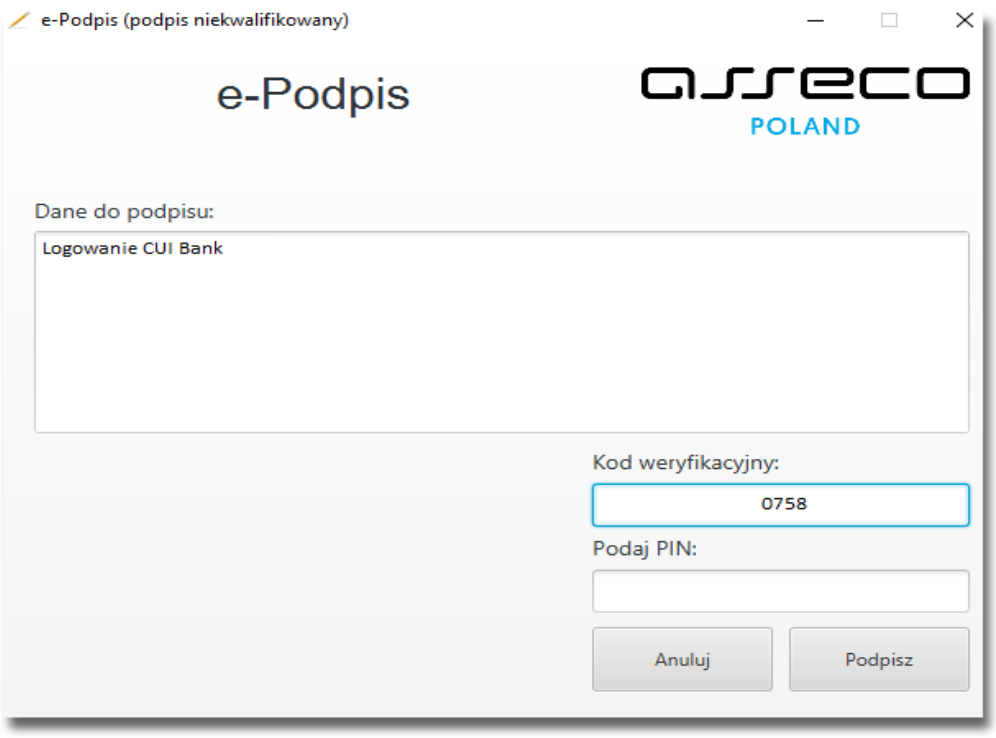


Na drugim kroku logowania, zostaje zaprezentowana formatka oczekiwania na podpis z aplikacji ePodpis. Wybór opcji [ZALOGUJ ZA POMOCĄ E-PODPISU] pozwala na pobranie, a następnie instalację aplikacji ePodpis.

Po zainstalowaniu i uruchomieniu aplikacji e-Podpis, użytkownik powinien zostać w niej uwierzytelniony. W tym celu, na formatce e-Podpisu, użytkownik wpisuje PIN karty mikroprocesorowej, a następnie wybiera przycisk [PODPISZ].



Jeśli proces uwierzytelnienia w aplikacji e-Podpis zakończył się pomyślnie, użytkownik loguje się do systemu Asseco EBP, podając na formatce e-Podpisu kod weryfikacyjny z formatki logowania oraz PIN do karty.



Po poprawnym wprowadzeniu kodu weryfikacyjnego oraz PINu, użytkownik zostaje zalogowany do systemu Asseco EBP.

2.2. Kolejne logowanie do systemu Asseco EBP przy pomocy karty mikroprocesorowej

Jeśli aplikacja e-Podpis jest uruchomiona i użytkownik jest do niej zalogowany, wówczas proces logowania do system Asseco EBP za pomocą karty mikroprocesorowej przebiega następująco:

Użytkownik na formatce logowania wprowadza identyfikator i przechodzi do drugiego kroku naciskając przycisk [DALEJ].

Na drugim kroku logowania, zostaje zaprezentowana formatka oczekiwania na podpis oraz formatka z aplikacji e-Podpis z danymi do podpisu.

Użytkownik podaje na formatce e-Podpisu kod weryfikacyjny z formatki logowania oraz PIN do karty.

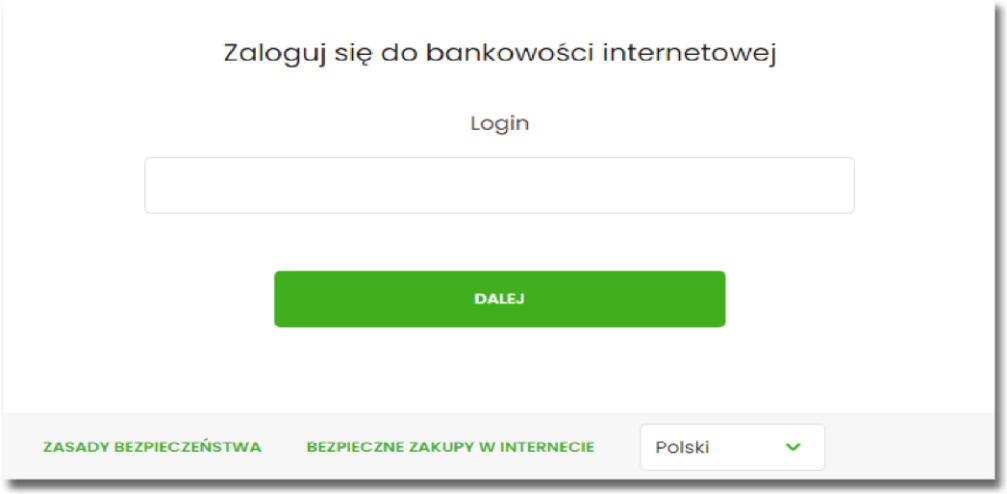
Po poprawnym wprowadzeniu kodu weryfikacyjnego oraz PINu, użytkownik zostaje zalogowany do systemu Asseco EBP.

3. 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.

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

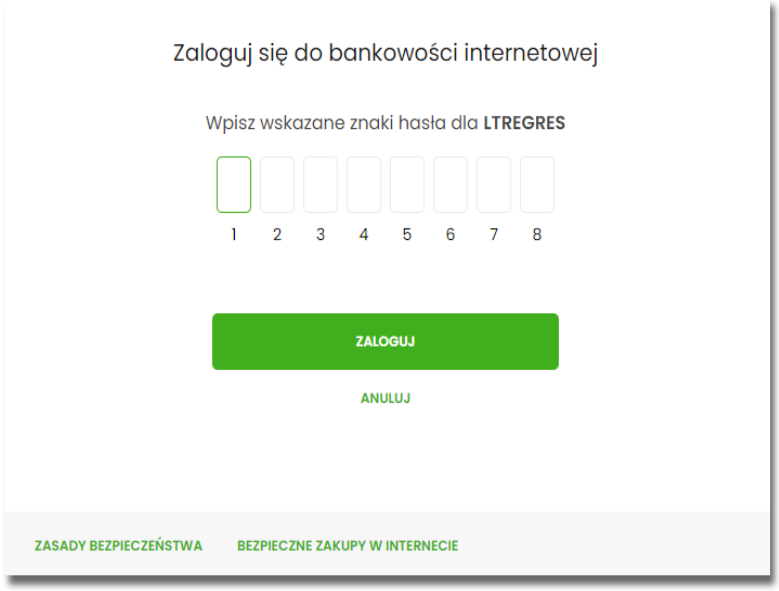
Po uruchomieniu systemu Asseco EBP wyświetlane jest okno logowania:



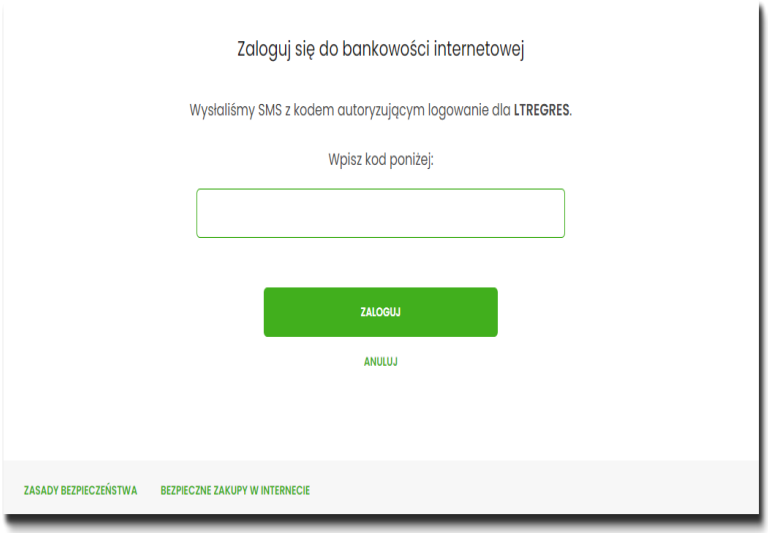
Pierwsze logowanie odbywa się w następujących krokach:

Wprowadzenie identyfikatora Użytkownika i naciśnięciu przycisku [DALEJ]. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tą wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami,

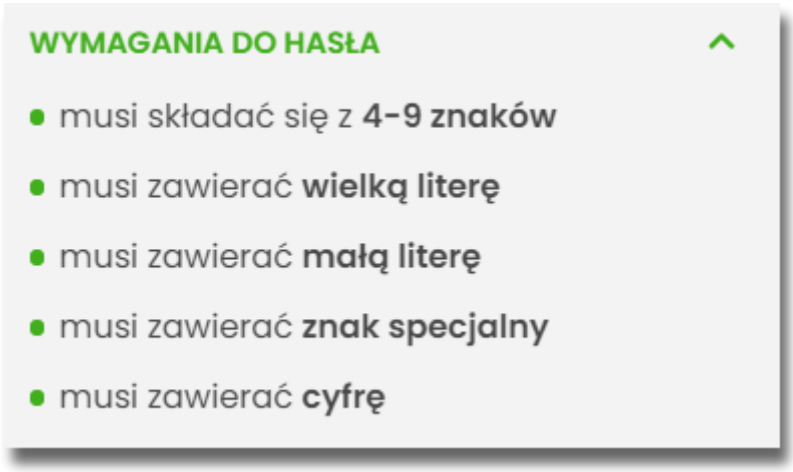
Wprowadzenie hasła, które zostało przesłane w wiadomości sms (hasło tymczasowe) i potwierdzeniu przyciskiem [ZALOGUJ],

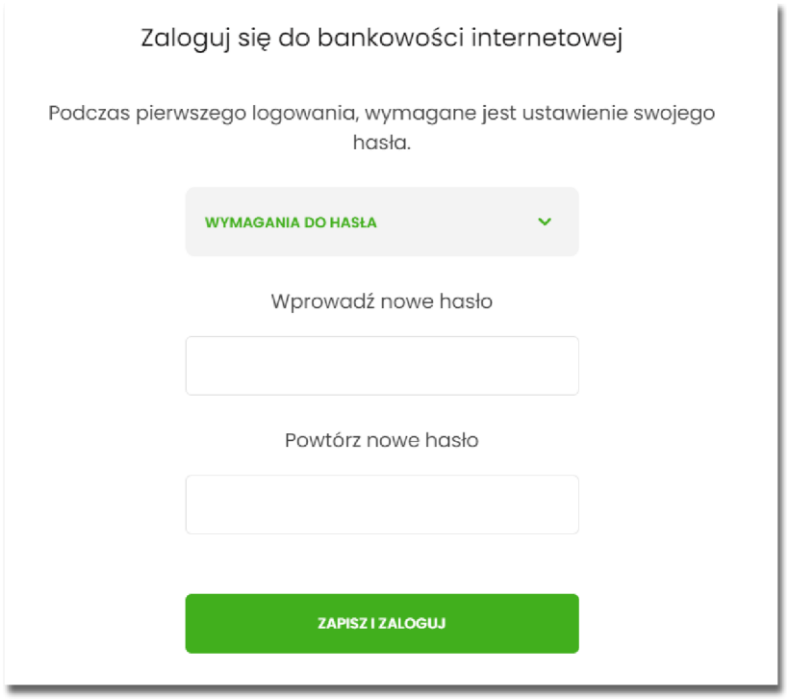


Potwierdzenie logowania otrzymanym kodem sms i naciśnięcie przycisku [ZALOGUJ],



Ustawienie nowego hasła do logowania z zachowaniem zasad bezpieczeństwa (zasady są dostepne na liście rozwijalnej WYMAGANIA DO HASŁA), oraz potwierdzenie za pomocą przycisku [ZAPISZ I ZALOGUJ]:





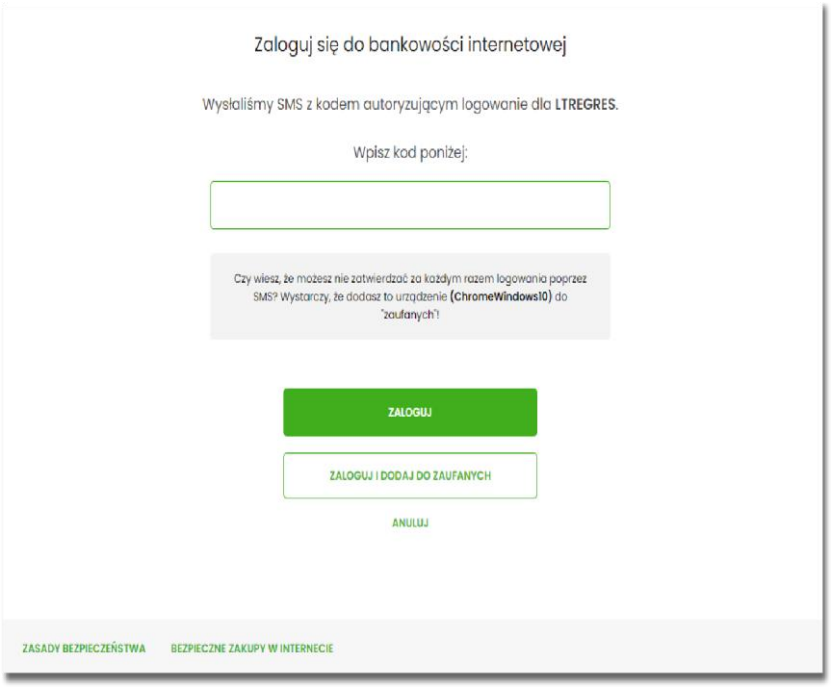
Po poprawnym ustawieniu nowego hasła, Użytkownik zostanie zalogowany do systemu Asseco EBP.

3.2. Dodanie urządzenia zaufanego podczas logowania.

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



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

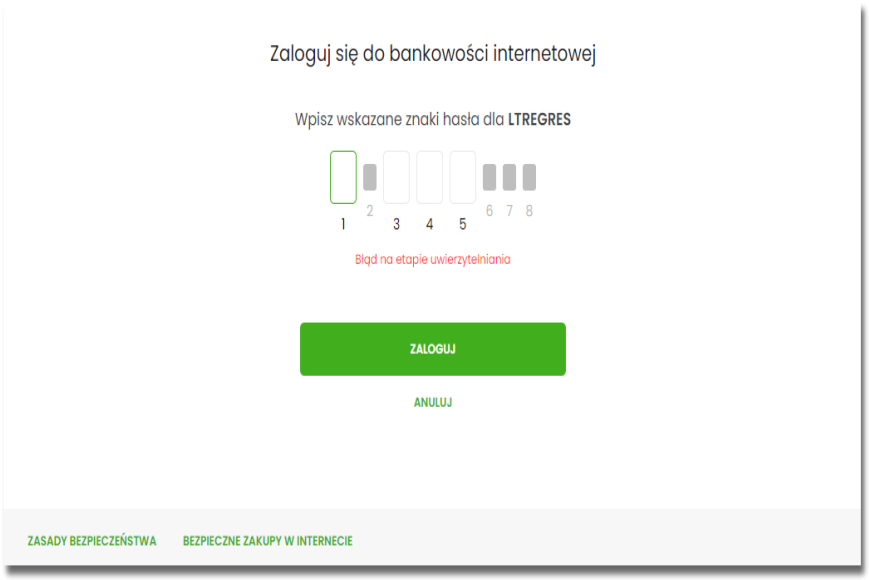
3.3. Kolejne logowanie do systemu Asseco EBP przy pomocy hasła maskowanego + kodu SMS (bez dodania urządzenia do zaufanych)

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

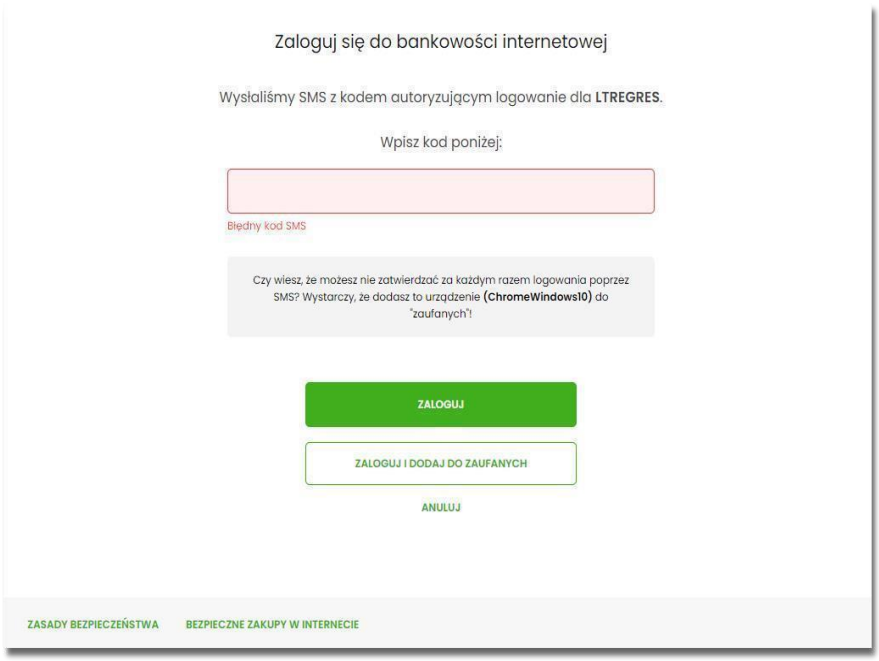
- identyfikator Użytkownika i nacisnąć przycisk [DALEJ],
- hasło i potwierdzić przyciskiem [ZALOGUJ],
- otrzymany kod SMS, potwierdzający logowanie i nacisnąć przycisk [ZALOGUJ].

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.*



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



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

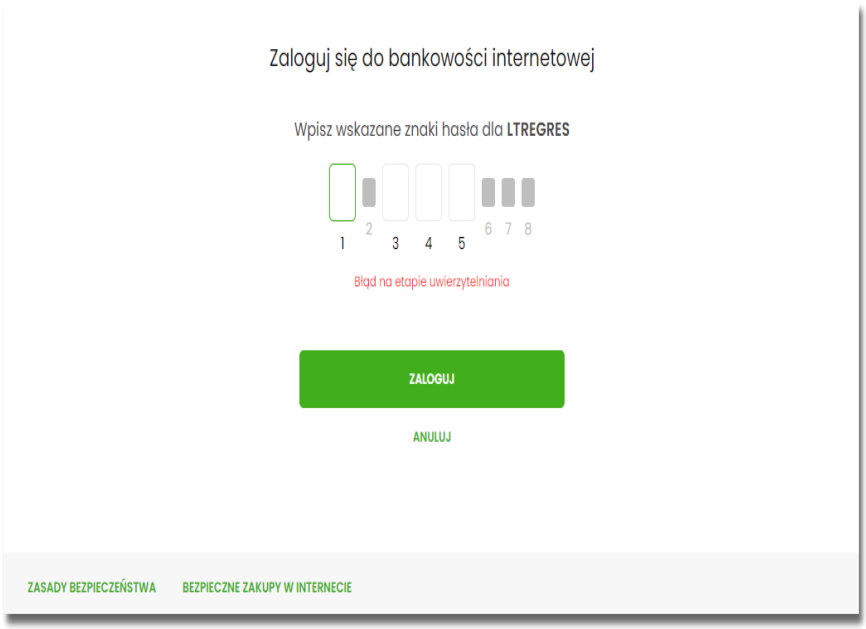
Podczas kolejnego logowania do systemu Asseco EBP, Użytkownik musi wprowadzić:

- 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 zweryfikauje, 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.*



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

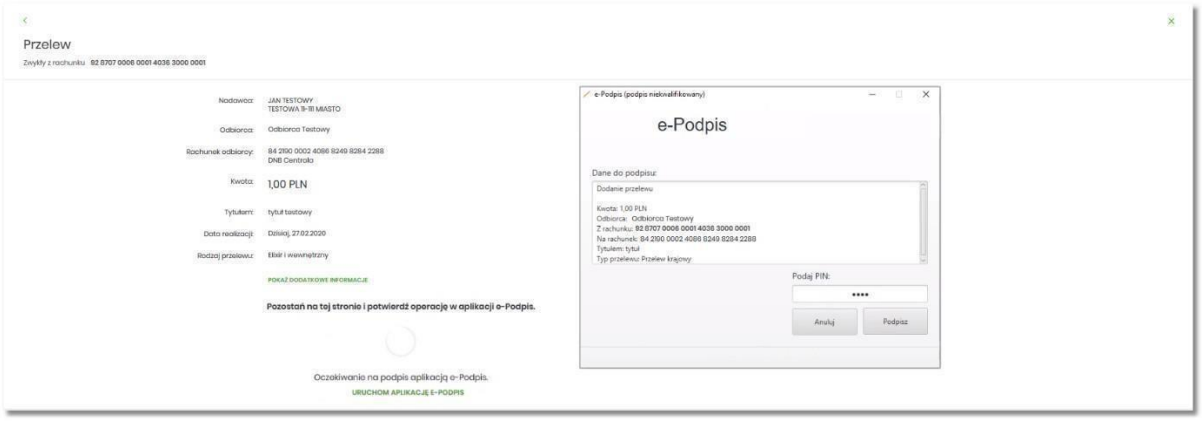
4.1. Mobilny podpis

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

4.2. Karta mikroprocesorowa

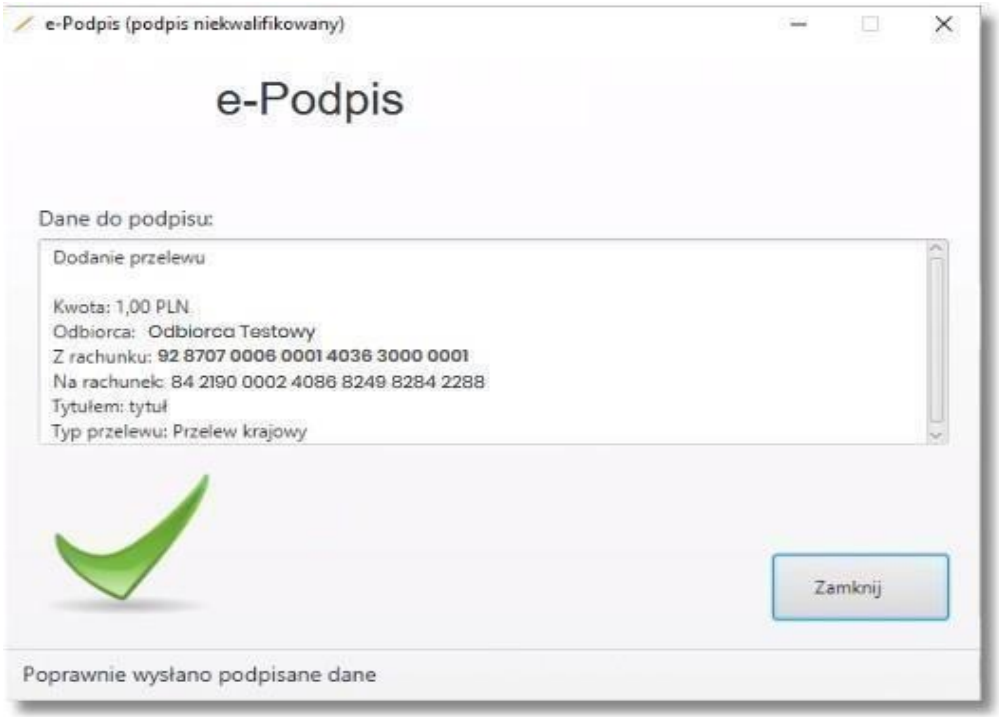
Autoryzacja dyspozycji przy pomocy karty mikroprocesorowej.

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.



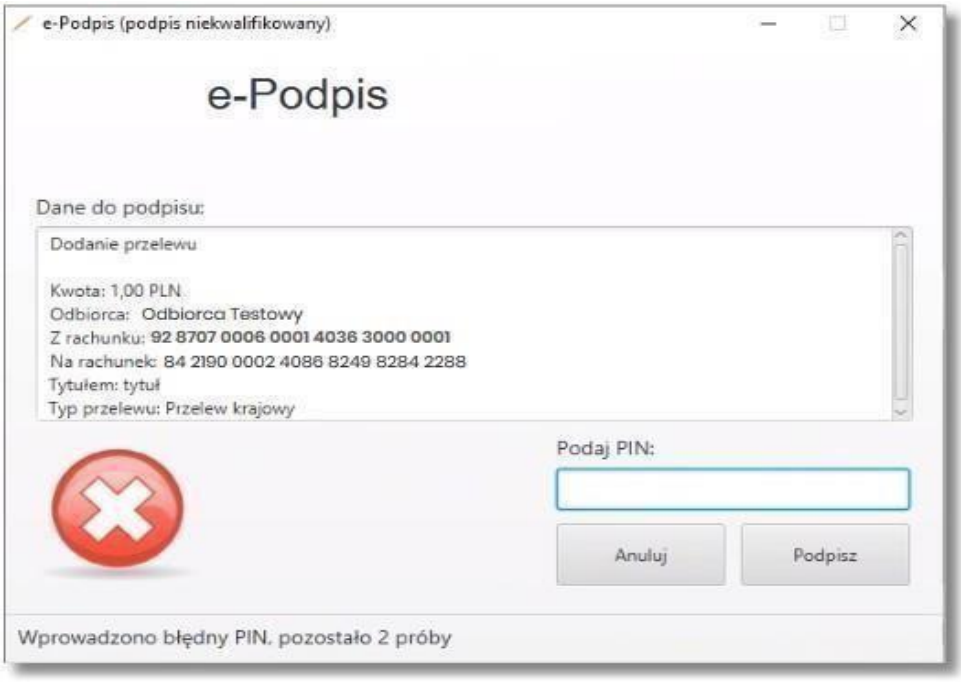
Po wprowadzeniu kodu PIN i naciśnięciu [PODPISZ] system prezentuje formularz z informacją o poprawnej autoryzacji dyspozycji.

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.

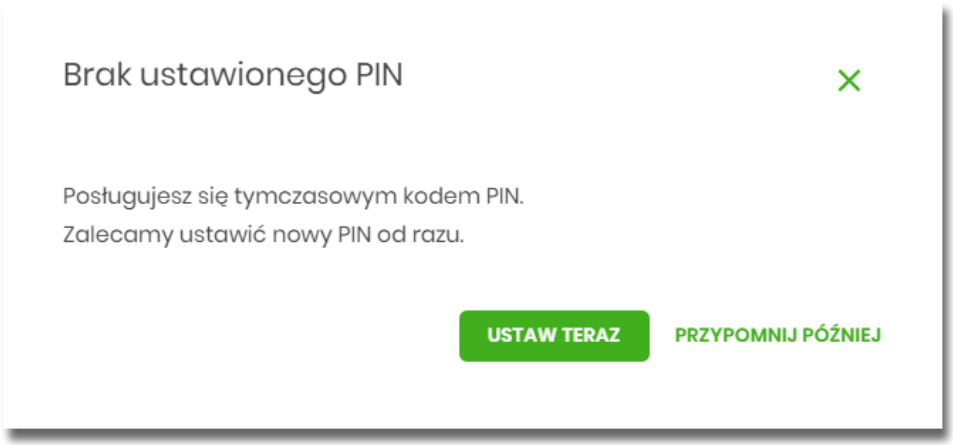
Po odrzuceniu dyspozycji za pomocą przycisku [ANULUJ], system prezentuje następujący komunikat:

4.3. Kod PIN + kod SMS

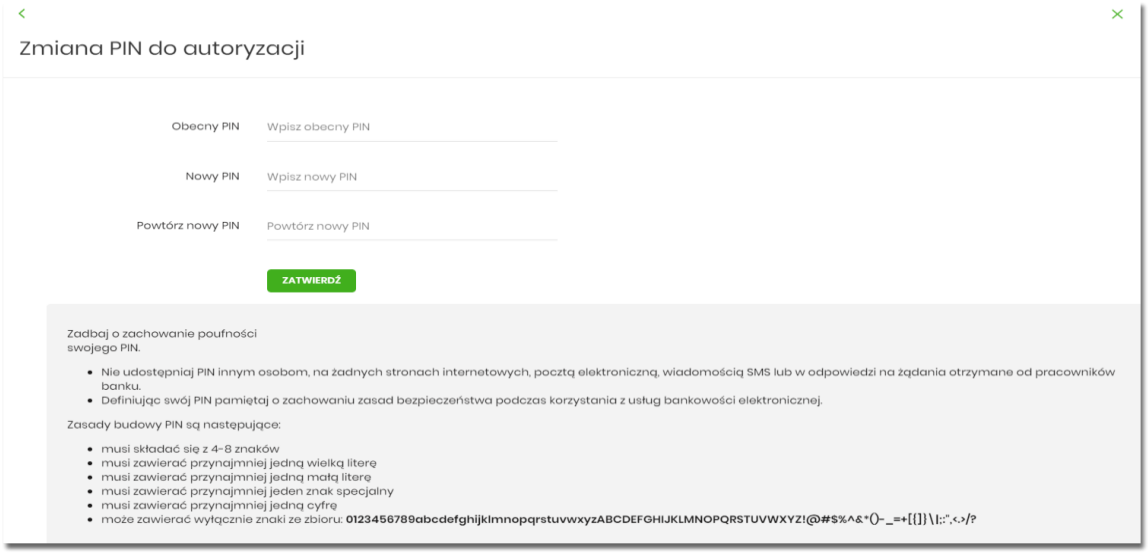
W przypadku Użytkowników posiadających przypisaną metodę autoryzacji Kod PIN + Kod SMS, autoryzacja zleceń następuje po wprowadzeniu poprawnego kodu PIN oraz przesłanego kodu SMS.

Operator w module Asseco BackOffice wyszukuje osobę i 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 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).



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

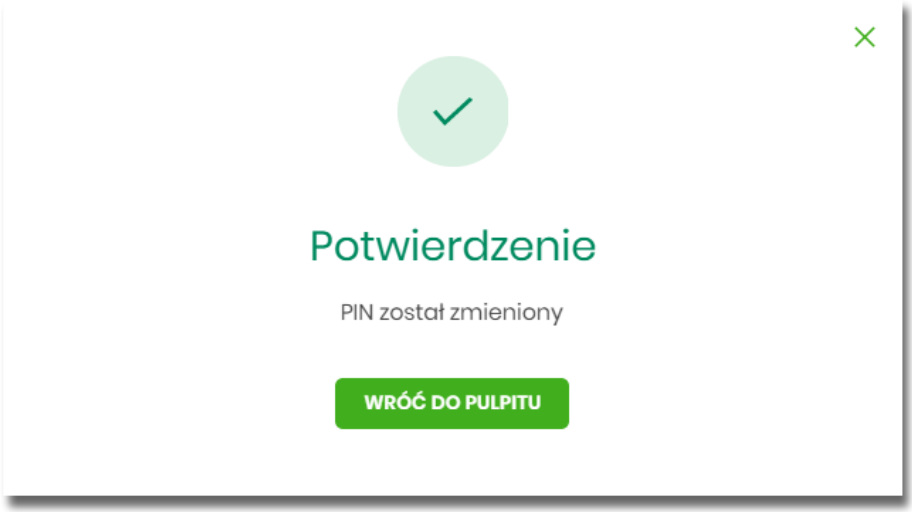
Nowy PIN musi być zgodny z zasadami bezpieczeństwa zgodnie z informacją w dolnej części formularza, tzn.:

- 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!@#$%^&*()-

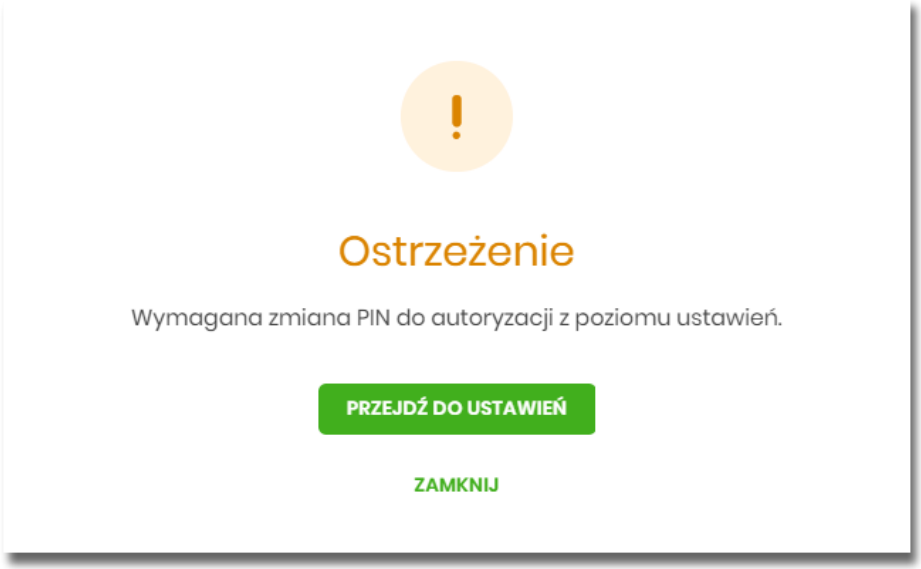
_=+[\{]}\|;:",<.>/?.

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.

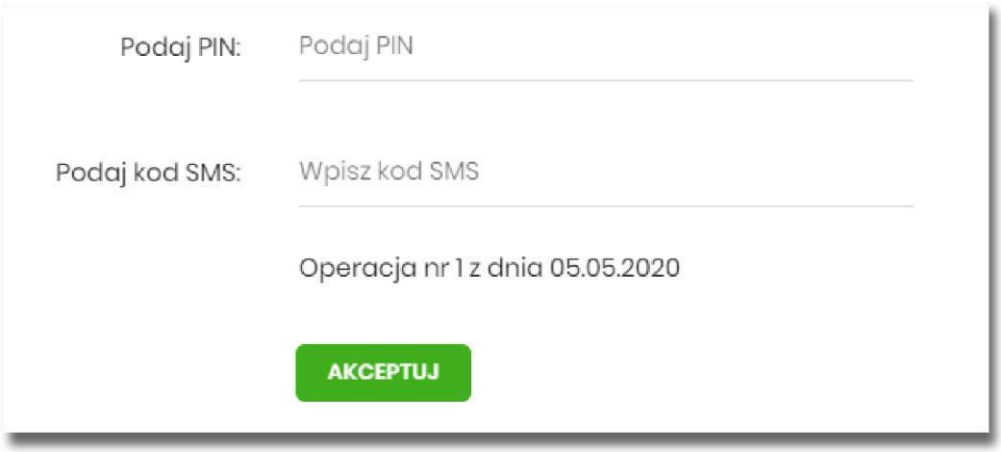
Jeśli Użytkownik nie zmieni PIN do autoryzacji bezpośrednio po zalogowaniu i przejdzie do wykonania przelewów, to przy wejściu Użytkownika na formularz potwierdzenia przelewu, system wymusza zmianę PINu, prezentując odpowiedni komunikat:



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

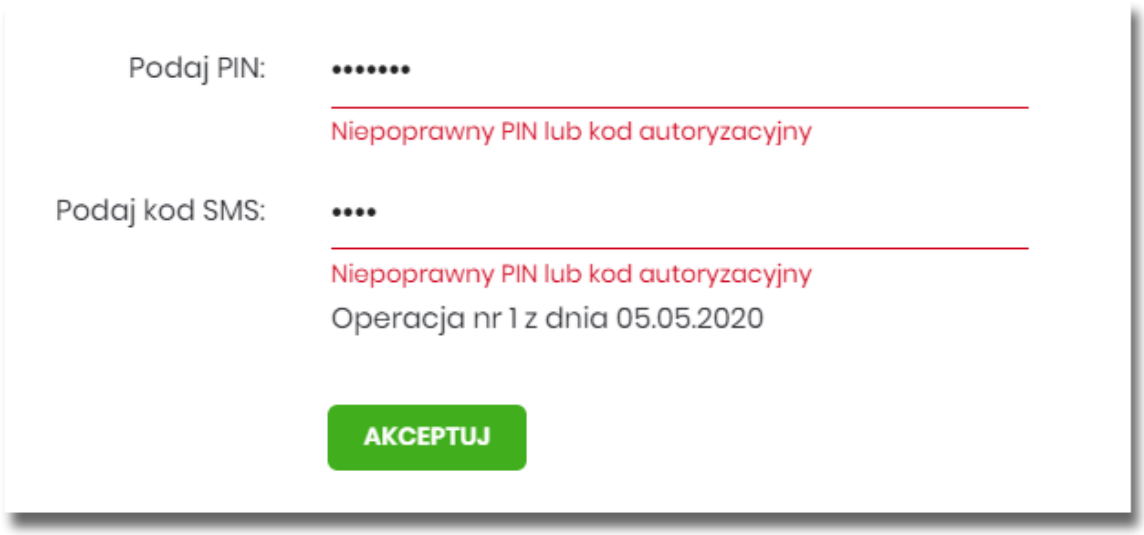
Po zmianie PIN'u tymczasowego, aby zautoryzować dyspozycję Użytkownik będzie musiał:

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



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

W przypadku wprowadzenia błędnego PIN'u albo kodu SMS, system wyświetli odpowiedni komunikat:



5. Wielopodpis

System Asseco EBP umożliwia weryfikację wymaganych podpisów podczas akceptacji dyspozycji przelewu przez Użytkownika w zależności od zdefiniowanych schematów akceptacji.

Użytkownik ma możliwość akceptacji jednoosobowej przelewów bądź akceptacji wieloosobowej (zgodnie z obowiązującym schematem akceptacji).

Konfiguracja schematów akceptacji realizowana jest po stronie modułu BackOffice.

Wielopodpis dotyczy autoryzacji:

- przelewu zwykłego,
- przelewu własnego,

Jeśli schemat podpisu został zdefiniowany system prezentuje akcje na formularzu nowego przelewu:

- **Formularz wprowadzenia danych – krok 1: dostępne są akcje:**
  - [DALEJ] – przejście do kroku 2,
  - [DODAJ DO LISTY ZLECEŃ]– przycisk umożliwia zapisanie przelewu do *Koszyka zleceń* lub na *Listę zleceń* w statusie *Nowy*.
- **Formularz potwierdzenia i autoryzacji danych – krok 2: dostępne są akcje**:
  - dla schematu wymagającego podpisu jednej osoby:

- [AKCEPTUJ i WYŚLIJ] – przejście do autoryzacji, przelew po autoryzacji przekazywany jest do realizacji w systemie transakcyjnym. Przelew widoczny jest na liście przelewów w statusie *Aktywne*.
- [AKCEPTUJ] – przejście do autoryzacji (prezentacja sekcji do autoryzacji), przelew dodawany jest do Koszyka zleceń w przypadku kontekstu indywidualnego lub na Listę zleceń w przypadku kontekstu firmowego w statusie *Gotowy do przekazania*,
- [DODAJ DO KOSZYKA] dla klienta indywidualnego lub [DODAJ DO LISTY ZLECEŃ] dla klienta firmowego – przejście do potwierdzenia (o wymogu autoryzacji decyduje parametr systemowy), przelew trafia do Koszyka zleceń lub na Listę zleceń w statusie *Nowy*.

◦ dla schematu wymagającego podpisu więcej niż jednej osoby:

- [AKCEPTUJ] – przejście do autoryzacji (prezentacja sekcji do autoryzacji), przelew dodawany jest do listy zleceń w statusie *W akceptacji*,
- [DODAJ DO KOSZYKA] dla klienta indywidualnego lub [DODAJ DO LISTY ZLECEŃ] dla klienta firmowego – przejście do potwierdzenia (o wymogu autoryzacji decyduje parametr systemowy), przelew trafia do Koszyka zleceń lub na Listę zleceń w statusie Nowy.

6. Blokowanie kanałów dostępu

W przypadku utraty karty mikroprocesorowej, urządzenia autoryzującego lub ujawnienia osobom trzecim danych logowania prosimy o kontakt w godzinach pracy banku pod numerem telefonu:

15-833-20-20 wew. 160

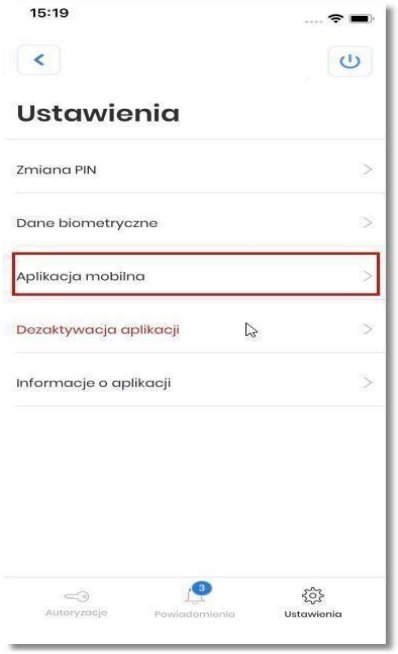
7. Uruchomienie rozszerzonych funkcji aplikacji BSGo.

W momencie udostępnienia Klientom rozszerzonych funkcjonalności aplikacji BSGo, zostanie Użytkownikowi zaprezentowany ekran z możliwością włączenia dodatkowych opcji nowej bankowości.

Użytkownik może dokonać wyboru poprzez kliknięcie w opcję:

- **[Przejdź]** - użytkownik uzyska dostęp do funkcjonalności tożsamych z bankowością internetową.
- …kliknij **[tutaj]** - użytkownik przekierowany zostanie do aplikacji tylko w kontekście tokena mobilnego.

W przypadku gdy użytkownik zdecyduje się pozostać przy dotychczasowych funkcjonalnościach aplikacji, będzie mógł w każdym momencie uruchomić rozszerzoną wersje aplikacji wybierając menu ***'Ustawienia'*** → ***'Aplikacja mobilna'***.



Następnie użytkownik na ekranie **'Aplikacja mobilna'** wybiera opcję **[WŁĄCZ].**

8. Limity w aplikacji BSGo.

Limit pojedynczej transakcji:

Wartość standardowa	Wartość maksymalna
5.000,00 zł	Limit ustawiony w bankowości internetowej lub limit standardowy pojedynczej transakcji w ciągu dnia określony w załączniku nr 3 do „Regulaminu świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów instytucjonalnych”.

Limit wszystkich transakcji w ciągu dnia:

Wartość standardowa	Wartość maksymalna
5.000,00 zł	Limit ustawiony w bankowości internetowej lub limit standardowy wszystkich transakcji w ciągu dnia określony w załączniku nr 3 do Regulaminu świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów instytucjonalnych”.

9. Rodzaje wniosków w bankowości elektronicznej.

- Wniosek o aktywację karty
- Wniosek o zmianę środka dostępu
- Wniosek o zmianę sposobu dostarczania wyciągów
- Wniosek o zmianę limitów karty
- Wniosek o zmianę danych osobowych
- Wniosek o zmianę limitów operacji dokonywanych za pośrednictwem bankowości elektronicznej
- Wniosek o aktywację/ zmianę PUSH i SMS
- Wniosek o odroczenie spłaty rat kredytowych

- Wniosek o udzielenie/ odwołanie pełnomocnictwa
- Wniosek o zablokowanie/ cofnięcie dostępu Użytkownika do usług bankowości elektronicznej przez posiadacza rachunku
- Wniosek definiowany przez Użytkownika poprzez tytuł oraz pole tekstowe wraz z możliwością dodania załącznika.
- Wniosek o dokonanie / odwołanie zastrzeżenia dokumentu tożsamości

10. Środki bezpieczeństwa

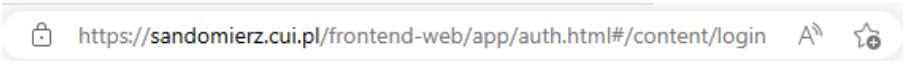
10.1. Uważaj na fałszywe wiadomości e-mail

Bank Spółdzielczy w Sandomierzu nigdy nie wysyła do swoich klientów wiadomości mailowych z prośbami o podanie poufnych informacji (uzupełnienie formularzy). Nie należy zatem odpowiadać na takie wiadomości i nie uruchamiać zawartych w nich linków. Złodzieje często podszywają się pod bankowców i fałszują korespondencję, a nawet witryny internetowe, które do złudzenia przypominają oryginalne z Banku. Wiadomości e-mail wysyłają do tysięcy osób w nadziei na złapanie naiwnego Klienta, który dobrowolnie poda wrażliwe dane takie jak hasło i login do serwisu bankowości internetowej. Działania takie określa się terminem „phishing", który pochodzi od słowa „fishing" – łowienie. Dlatego każdą tego typu informację należy bezwzględnie zignorować i **pod żadnym pozorem nie korzystać** z linków przesłanych w wiadomości e-mail. Takie działanie jest przestępstwem internetowym. W takiej sytuacji najlepiej **poinformować** o tym Bank. Zalecamy jednak **unikać** odbierania **poczty elektronicznej** na stacji roboczej, na której korzystamy z usług bankowości elektronicznej. To pozwoli ograniczyć ryzyko zainfekowania naszego urządzenia złośliwym oprogramowaniem, które potencjalnie może pochodzić z zainfekowanej wiadomości e-mail. Należy zwrócić **szczególną uwagę** na załączniki, które mogą zawierać złośliwe oprogramowanie lub skrypty umożliwiające pobranie ich z sieci Internet. Załączniki powinny być przeskanowane **przed otwarciem** przez oprogramowanie **antywirusowe** zainstalowane na stacji roboczej lub urządzeniu mobilnym. Zalecamy korzystanie z usług serwerów poczty e-mail wyposażonych w system antyspamowy oraz antywirusowy dla kont pocztowych.
System taki może spowodować, że wybrane wiadomości e-mail zostaną oznaczone jako stwarzające potencjalne zagrożenie i w efekcie mogą zostać odrzucone.

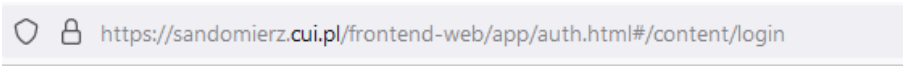
10.2. Sprawdź adres strony logowania do CUI

Do logowania do systemu należy używać wyłącznie adresu podanego przez Bank wpisując go do paska adresu przeglądarki internetowej lub skorzystać **bezpośrednio** ze strony naszego Banku.
W Banku Spółdzielczym w Sandomierzu dla klientów korzystających z bankowości internetowej CUI prawidłowy adres strony logowania to https://sandomierz.cui.pl/frontend-web/app/auth.html#/content/login . Do wyszukiwania adresów nie powinno używać się wyszukiwarki internetowej. Dla poprawy bezpieczeństwa nie należy umieszczać strony logowania wśród „ulubionych" stron przeglądarki internetowej. Przestępcy tworzą bowiem oprogramowanie, które jest w stanie wykorzystać luki w systemie i podmienić stronę na fałszywą. O tym, że znajdujemy się na właściwej stronie internetowej, informuje nas pasek adresu. Adres musi zaczynać się od https:// a przeglądarka powinna zweryfikować połączenie wyświetlając symbol zamkniętej kłódki. **Bardzo ważne** jest i należy **zawsze** sprawdzić, czy adres strony jest **właściwy** i nie zawiera tzw. „literówek". Poprawne adresy wyglądają następująco:

Dla przeglądarki Microsoft Edge:



Dla przeglądarki Firefox:



Dla przeglądarki Chrome:

Klikając w symbol zatrzaśniętej kłódki możemy zweryfikować czy certyfikat strony wystawiony jest przez:

Nazwa pospolita (CN)	Certum Extended Validation CA SHA2
Organizacja (O)	Unizeto Technologies S.A.
Jednostka organizacyjna (OU)	Certum Certification Authority

Wystawiony dla:

Nazwa pospolita (CN)	sandomierz.cui.pl
Organizacja (O)	Bank Spółdzielczy w Sandomierzu
Jednostka organizacyjna (OU)	<brak w certyfikacie>

Brak "zatrzaśniętej kłódki" oznacza, że mamy do czynienia z niebezpiecznym połączeniem, w którym dane nie są szyfrowane - w związku z tym nie powinniśmy podejmować prób logowania na taką stronę.

10.3. Stosuj się do procedur Banku

Logując się na stronę Banku należy stosować się do procedur obowiązujących w Banku. Zasady bezpiecznego korzystania z bankowości elektronicznej zawarte są w niniejszym przewodniku, który jest także zamieszczony na stronie internetowej Banku:

10.4. Aktualizuj przeglądarkę internetową i system operacyjny

Przeglądarka internetowa to program, który służy do otwierania stron internetowych, także tych do logowania do systemu bankowości internetowej. Należy zatem zadbać o to, by na naszym komputerze regularnie dokonywać aktualizacji oprogramowania. Zaleca się również używać firewalla. Hakerzy wyszukują luk w programach, za pomocą których mogą wykraść niezbędne informacje. Należy także pamiętać o **regularnej aktualizacji** sytemu operacyjnego. Dostawcy oprogramowania na bieżąco monitorują poziom bezpieczeństwa i publikują aktualizacje uzupełniające luki w oprogramowaniu. Nowoczesna przeglądarka internetowa jest **niezbędnym** elementem zapewniającym bezpieczne korzystanie z systemu bankowości internetowej. Nie zastąpi jednak ludzkiej **czujności**, dlatego **nie instaluj** oprogramowania z **nieznanych** źródeł. Takie aplikacje mogą zawierać oprogramowanie szpiegujące, szyfrujące, czy złośliwe.
PAMIĘTAJ! **Urządzenie mobilne** takie jak smartfon, tablet, itp. również posiada zainstalowany system operacyjny i podlega tym samym zasadom, co komputer lub laptop.

PAMIĘTAJ! dbając o bezpieczeństwo na swoim komputerze możesz nie tylko bezpiecznie korzystać z bankowości internetowej, ale również chronisz dane na nim przechowywane.

10.5. Korzystaj z oprogramowania antywirusowego

Równie niezbędne jak bezpieczna przeglądarka internetowa jest zainstalowanie programu antywirusowego zapobiegającego instalacji wirusów oraz innego szkodliwego oprogramowania. Zalecamy, aby **nie korzystać** z **darmowych** programów antywirusowych. Oprogramowanie zainstalowane na komputerze czy też urządzeniu mobilnym **powinno** posiadać **płatną licencję**. Warto przy tym korzystać z programów polecanych przez **ekspertów**, ponieważ nie wszystkie aplikacje dostępne w sieci spełniają niezbędne standardy. Należy pamiętać, że instalowanie aplikacji pobranych z niesprawdzonych stron internetowych bardzo często kończy się zainfekowaniem komputera przez oprogramowanie szpiegujące. Warto także raz na kilka dni **skanować** antywirusem komputer i dbać o **aktualne** bazy wirusów.

10.6. Loguj się na własnym komputerze lub własnym urządzeniu mobilnym

Zaletą bankowości internetowej jest to, że dostęp do własnego konta możemy mieć z dowolnego komputera podpiętego do sieci. Tu jednak zaleca się duża ostrożność – powinniśmy korzystać przede wszystkim z naszego własnego stanowiska komputerowego lub naszego własnego urządzenia mobilnego. Nie powinniśmy także logować się na ogólnie dostępnych komputerach, np. w kafejkach internetowych, miejscach hotelowych, kioskach internetowych, itd. Nie mamy bowiem gwarancji, że komputery te są „czyste". Mogą tam być zainstalowane programy szpiegujące, które potrafią przechwycić dane do logowania czy numery kart. Jeśli jednak musimy skorzystać z obcego komputera należy pamiętać, by zawsze wylogować się z serwisu transakcyjnego. **Nie należy** dokonywać płatności i logować się do serwisów bankowości elektronicznej podając swoje hasło w punktach bezpłatnego publicznego dostępu do Internetu - w tzw. **hot-spotach**, np. na lotniskach, dworcach kolejowych, stacjach paliw, hotelach, itd. Takie sieci charakteryzują się często niskim poziomem bezpieczeństwa co jest dodatkowym czynnikiem stwarzającym **zagrożenie**.

10.7. Chroń środki dostępu do usługi internetowej

Nie zapisuj danych do logowania (identyfikatorów, haseł, itd.) - zarówno w formie tradycyjnej, elektronicznej jak również bezpośrednio w przeglądarce internetowej, gdyż w ten sposób stwarzasz zagrożenie przejęcia ich przez osoby postronne. Bez znaczenia jest tutaj forma - taka informacja zawsze może zostać przejęta przez niepowołaną osobę, dla przykładu, jeśli jest to urządzenie przenośne, takie jak notebook, tablet, czy telefon komórkowy, może zostać skradzione.

Staraj się także **okresowo zmieniać** hasło dostępu do konta.
Po zalogowaniu na stronie bankowości elektronicznej – w ustawieniach profilu Klienta udostępniona jest opcja zmiany hasła logowania której można dokonać w dowolnym momencie. Telefon z zainstalowanym Tokenem mobilnym lub karty chipowe do

zatwierdzania transakcji internetowych trzymaj w bezpiecznym miejscu – nie zostawiaj na przykład w biurku w pracy. Pamiętaj, że są to dane, które mogą posłużyć do zlecenia przelewu z Twojego konta. Sprawdzaj także daty i godziny ostatniego logowania na rachunek, które znajdują się w zakładce Historia logowań.

PEŁNOMOCNICTWO DO RACHUNKU

Pamiętaj, aby **nigdy nie udostępniać** środków dostępu do rachunku innym osobom – **niezależnie** od tego, czy jest to osoba Tobie dobrze znana – **nie ma znaczenia**, czy jest to Współmałżonek, Córka, Syn czy Rodzic. **Twoje** środki autoryzacji są przeznaczone **TYLKO** do **Twojego** użytku. Udostępnianie danych logowania jest **niedopuszczalne**. Jeżeli istnieje potrzeba, aby także ktoś inny miał dostęp do Twojego rachunku, należy udać się do placówki Banku i podpisać dokument stanowiący ustalenie **pełnomocnictwa** do Twojego rachunku. **Pełnomocnik** otrzyma swoje **własne** środki dostępu do Twojego rachunku i **tylko** w ten sposób będzie uprawniony do korzystania z niego.

LOGOWANIE DWUETAPOWE

Dodatkowym mechanizmem, który podnosi poziom bezpieczeństwa w bankowości jest logowanie dwuetapowe. To rozwiązanie wymaga **dwuskładnikowego uwierzytelnienia**, którym jest hasło ustawione przez Klienta oraz potwierdzenie pinem w aplikacji BSGo lub kod SMS.

ZAUFANE URZĄDZENIE

Jest to mechanizm, który pozwala zdefiniować urządzenie, na którym system nie będzie wymagał drugiego składnika uwierzytelnienia, jakim jest zatwierdzenie logowania a aplikacji BSGo lub kod SMS podczas logowania do bankowości. Procedura dodania urządzenia zaufanego odbywa się **podczas logowania**. System rejestruje urządzenie na liście urządzeń zaufanych, którymi można zarządzać w ustawieniach zabezpieczeń w menu **ZAUFANE URZĄDZENIA.** Logowanie z innego komputera – nie dodanego do listy urządzeń zaufanych wymaga mechanizmu dwuskładnikowego uwierzytelnienia. Warto pamiętać, iż system rozpoznaje także wersję przeglądarki internetowej, z której dodano urządzenie zaufane i przy próbie logowania z innej przeglądarki ponownie wymaga dwuskładnikowego uwierzytelnienia.

10.8. Ustaw silne hasło

Poprzez silne hasło rozumiemy ciąg znaków o odpowiednim stopniu złożoności. W bankowości internetowej CUI mamy możliwość nadania ciągu hasła o długości od 410-24 znaków.

Hasło:

- musi zawierać przynajmniej jedną wielką literę
- musi zawierać przynajmniej jedną małą literę

- musi zawierać przynajmniej jedną cyfrę
- nie może zaczynać się od zera
- nie może zawierać polskich znaków

Im hasło jest bardziej skomplikowane i trudniejsze do zapamiętania dla potencjalnego przestępcy, tym bardziej możemy czuć się bezpieczni. **Unikaj** stosowania nazw własnych, takich jak imiona, nazwiska, nazwy miejscowości, daty urodzenia, nazwy firmy itp. - jest to zawsze dodatkowe ułatwienie przy próbie złamania dostępu. **Stosuj unikalne** hasła, tzn. inne dla każdego z serwisów, z których korzystasz.

Pięciokrotne błędne wpisanie hasła powoduje blokadę dostępu do bankowości.

HASŁO MASKOWANE

Hasło maskowane to bezpieczny sposób wprowadzania hasła, polegający na wpisaniu do systemu jedynie losowo wyznaczonych znaków. Jest to dodatkowe zabezpieczenie przed udostępnieniem go osobom niepowołanym. **Pamiętaj**, że po błędnej próbie logowania system **nie zmienia** sekwencji wymaganych znaków hasła – prosi o podanie **tych samych** znaków hasła, których wymagał poprzednim razem. Gdyby system żądał wpisania innych znaków niż przy błędnej próbie, nie kontynuuj próby logowania i skontaktuj się z Bankiem, np.:

Pierwsza próba logowania:

Druga próba logowania:

1 + 2 sekwencja wpisania hasła = przestępca przejmuje całe hasło do bankowości

Podobnie, gdyby system wymagał wpisania wszystkich znaków w poszczególne pola hasła maskowanego, również nie podejmuj logowania i skontaktuj się z Bankiem.

10.9. Zwiększ kontrolę nad swoim kontem

W bankowości CUI mamy możliwość zgłoszenia zastrzeżenia dostępu do rachunku poprzez kontakt z Bankiem w godzinach jego pracy. Zadzwoń pod nr 15 833 20 20 a następnie wybierz 160 na swoim urządzeniu. Tym sposobem zostaniesz przekierowany do pracownika Banku.

POWIADOMIENIA SMS oraz PUSH

Bardzo ważną kwestię dotyczącą bezpieczeństwa w środowisku bankowości elektronicznej stanowi także usługa **powiadomień o logowaniu**, która poinformuje Cię za pomocą wiadomości SMS lub powiadomienia w aplikacji BSGo o logowaniu do systemu bankowości elektronicznej.

FILTRY LOGOWANIA

System bankowości elektronicznej CUI umożliwia dodatkowo skonfigurowanie **filtrów logowania**, które dopuszczą logowanie do Twojego konta **tylko** z określonych przez Ciebie adresów IP. Dla bankowości CUI klient musi złożyć wniosek w Banku

LIMITY

Dodatkowym zabezpieczeniem, które możesz wprowadzić jest **limit** jednorazowy oraz dzienny który uniemożliwia zlecenie transakcji przewyższających wyznaczoną całkowitą sumę.

INFORMACJA DLA KLIENTA

Wszelkie informacje dotyczące bankowości internetowej znajdziesz na stronie internetowej: https://www.bssandomierz.com.pl/ Jest to **oficjalna strona** informacyjna dla Klientów.