Spółdzielcza Grupa Bankowa

Bank Spółdzielczy w Sandomierzu

Rok założenia 1926

Przewodnik dla klienta

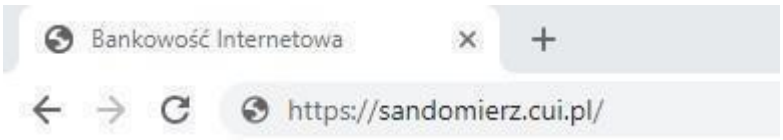
„Klientów indywidualnych”

Spis treści

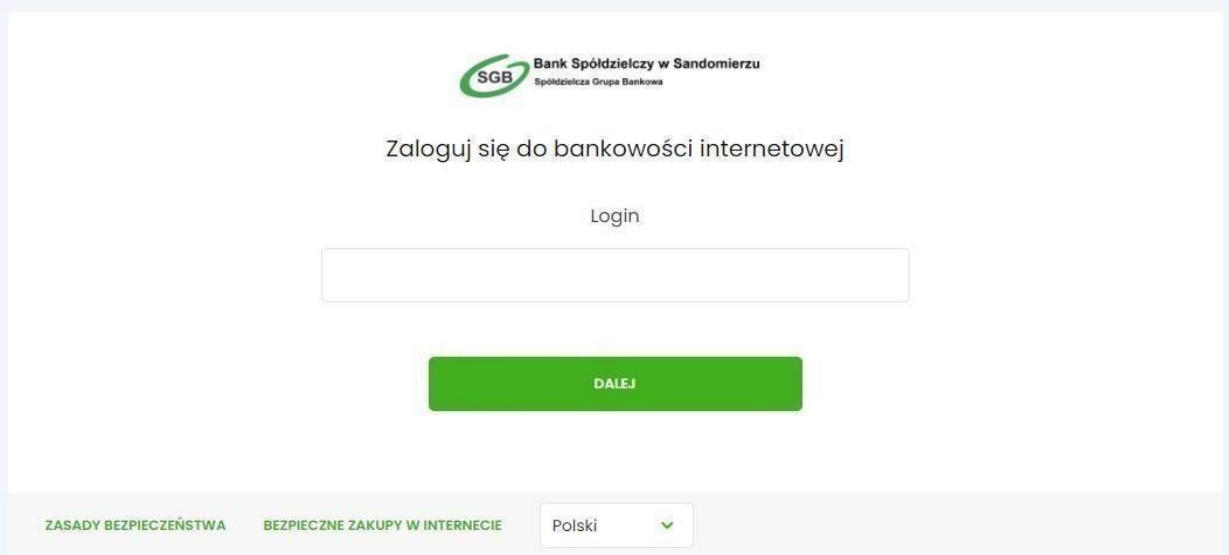
1. Pierwsze logowanie do bankowości internetowej przy pomocy hasła maskowanego + kodu SMS

Logowanie do bankowości internetowej odbywa się w następujących krokach:

W przeglądarce w pasku adresu wpisujemy https://sandomierz.cui.pl/ jak na ekranie poniżej i zatwierdzamy. W przypadku stworzonej zakładki z adresem do poprzedniej wersji bankowości również może z niej skorzystać ponieważ automatycznie zostanie przekierowany do nowej strony.



Po uruchomieniu strony wyświetlane jest okno logowania w którym należy wpisać identyfikator klienta otrzymany w banku. Wielkość liter nie ma znaczenia ponieważ system automatycznie zmienia je na duże.



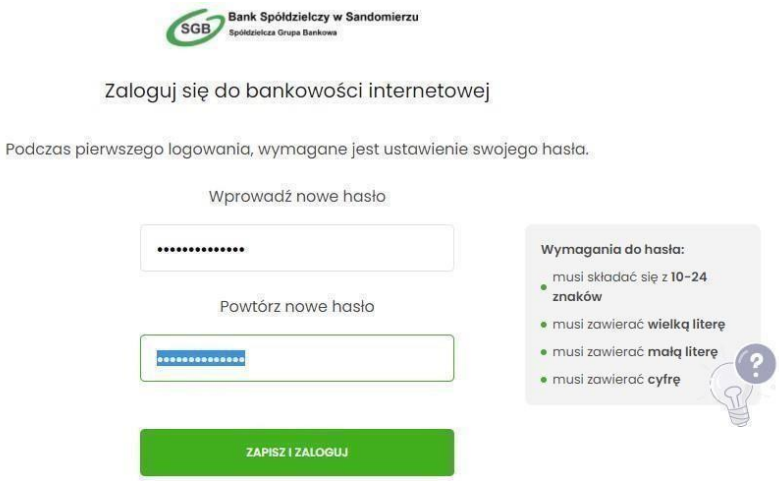
Po wpisaniu Identyfikatora i wciśnięciu przycisku „dalej” dostaniemy SMS’em tymczasowy kod dostępu i zostaniemy przekierowani do okna w którym ten kod należy wpisać.

UWAGA!

Kod jest ważny przez określony czas, jest on tymczasowy i jednorazowy.

Po wpisaniu kodu dostępu i zatwierdzeniu przyciskiem „zaloguj” zostaniemy przekierowani do kolejnego etapu autoryzacji gdzie należy wpisać dodatkowy kod wysłany SMS’em na numer telefonu.

Po wciśnięciu przycisku zaloguj zobaczymy ekran służący do tworzenia hasła.



Podczas tworzenia hasła należy pamiętać o wymogach jego złożoności:

- Hasło musi składać się z **10 - 24 znaków**.

- Musi zawierać **wielka literę**.

- Musi zawierać **małą literę**.

- Musi zawierać **cyfrę**.

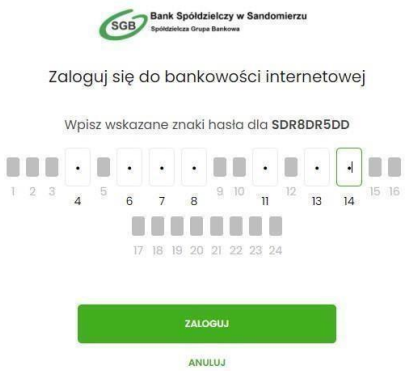
Jeśli hasła się zgadzają wciskamy „zapisz i zaloguj”. Po poprawnym wpisaniu haseł użytkownik zostanie zalogowany do bankowości internetowej.

2. Kolejne logowanie do bankowości internetowej przy pomocy hasła maskowanego + kodu

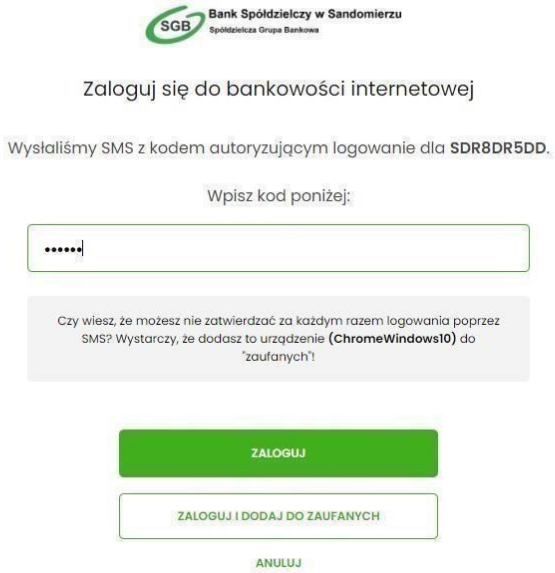
Podczas kolejnego logowania do bankowości internetowej, użytkownik musi wprowadzić:

- identyfikator użytkownika (LOGIN) i nacisnąć przycisk [DALEJ]

- hasło maskowane i potwierdzić przyciskiem [ZALOGUJ]



- otrzymany kod SMS potwierdzający logowanie i nacisnąć przycisk [ZALOGUJ] lub [ZALOGUJ I DODAJ DO ZAUFANYCH]. Dodanie urządzenia do zaufanych nie będzie wymuszało potwierdzania logowania dodatkowym kodem SMS na wybranym urządzeniu.



W przypadku wprowadzenia poprawnych danych, użytkownik zostanie zalogowany do bankowości, 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. Logowanie do systemu za pomocą tokena mobilnego (aplikacji BSGo)

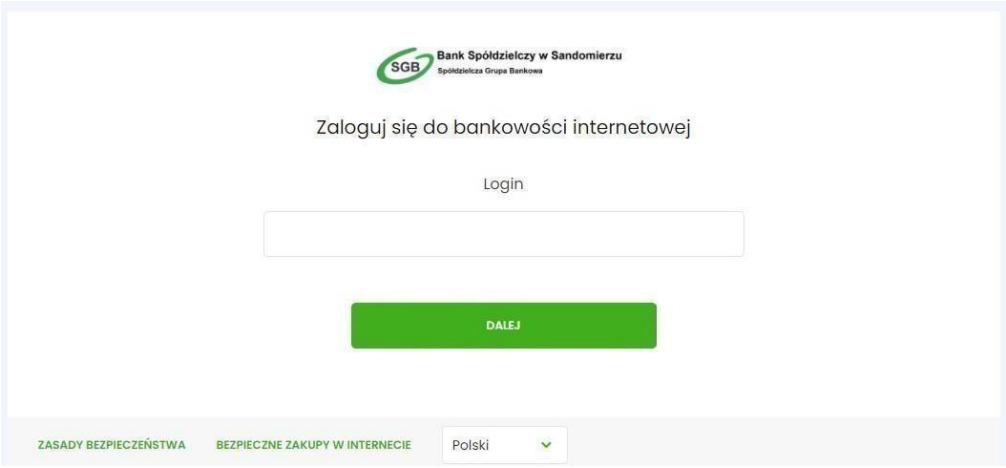
Użytkownik ma możliwość zalogowania się do bankowości elektronicznej za pomocą aplikacji BSGo pobranej ze sklepu - Google Play (Android), App Store (iOS) i zainstalowanej na urządzeniu mobilnym.

3.1. Pierwsze logowanie wraz z rejestracją urządzenia

1. Proces pierwszego logowania za pomocą aplikacji BSGo do bankowości internetowej w przypadku gdy użytkownik nie posiada aktywnego sparowanego urządzenia autoryzującego przebiega w następujący sposób:

- przechodzimy na stronę bankowości internetowej https://sandomierz.cui.pl/

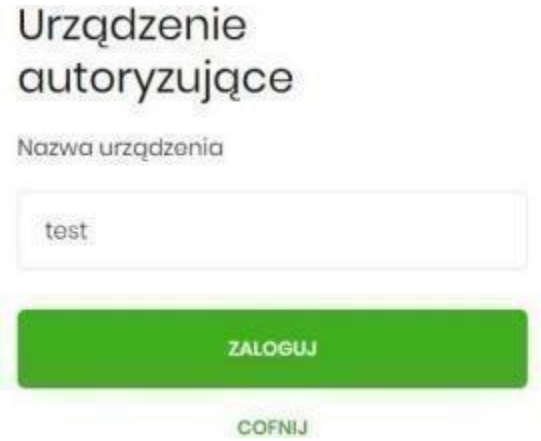
- użytkownik wprowadza numer identyfikacyjny i zatwierdza przyciskiem „DALEJ”



Wpisuje otrzymane za pomocą SMS hasło tymczasowe(kod dostępu) i zatwierdza przyciskiem „zaloguj”.

Następnie użytkownik ustawia nowe hasło, zgodnie z polityką bezpieczeństwa widoczną na stronie oraz potwierdza zmianę hasła klikając „ZAPISZ I ZALOGUJ’’

Użytkownik wpisuje nazwę urządzenia autoryzacyjnego czyli nazwę telefonu lub innego urządzenia na którym można zainstalować aplikację mToken Asseco MAA .



Po wpisaniu nazwy urządzenia autoryzacyjnego i wciśnięciu „zaloguj” zostanie wyświetlony na ekranie komputera kod aktywacyjny.

W tym momencie przechodzimy do aplikacji w telefonie BSGo. Jeśli jeszcze jej nie pobraliśmy to wchodzimy do aplikacji „Sklep Play”(dla systemów Android) lub „App Store” (dla systemów iOS) tam wyszukujemy aplikacje i klikamy „instaluj”.
W widoku po lewej stronie wybieramy „Posiadam kod aktywacyjny” po czym zostajemy przekierowani do ekranu po stronie prawej. Tam wpisujemy kod aktywacyjny z przeglądarki i zatwierdzamy przyciskiem „dalej”.

W kolejnym kroku na formularzu **Weryfikacja SMS** w celu identyfikacji należy wprowadzić dodatkową informację zgodnie z instrukcją wyświetlaną na ekranie. Informacją dodatkową jest kod weryfikacyjny

wysłany za pomocą wiadomości SMS. Po wprowadzeniu (za pomocą klawiatury na urządzeniu) danych w polu **Weryfikacja SMS** należy w celu zatwierdzenia wybrać ponownie przycisk [DALEJ].

Kolejnym krokiem jest nadanie numeru PIN do aplikacji. W tym celu klikamy przycisk „Nadaj PIN”.

PIN jest stały, należy go zapamiętać ponieważ będzie służył do logowania w aplikacji, zatwierdzania przelewów oraz zatwierdzania logowań w bankowości inetrnetowej. Pin musi składać się z 5 do 8 cyfr. Podczas jego nadawania wpisujemy go dwa razy.

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 w tym samy czasie zostaje zalogowany do bankowości internetowej w systemie Asseco EBP oraz może zalogować się do aplikacji BSGo wybierając „ZALOGUJ SIĘ” i wpisując PIN.

4. Logowanie po rejestracji urządzenia

Logowanie po zarejestrowaniu urządzenia przebiega bardzo podobnie do pierwszego logowania.

Przechodzimy na stronę https://sandomierz.cui.pl/ -Wpisujemy numer identyfikacyjny, klikamy „dalej”

-Wpisujemy hasło i zatwierdzamy przyciskiem „zaloguj”.

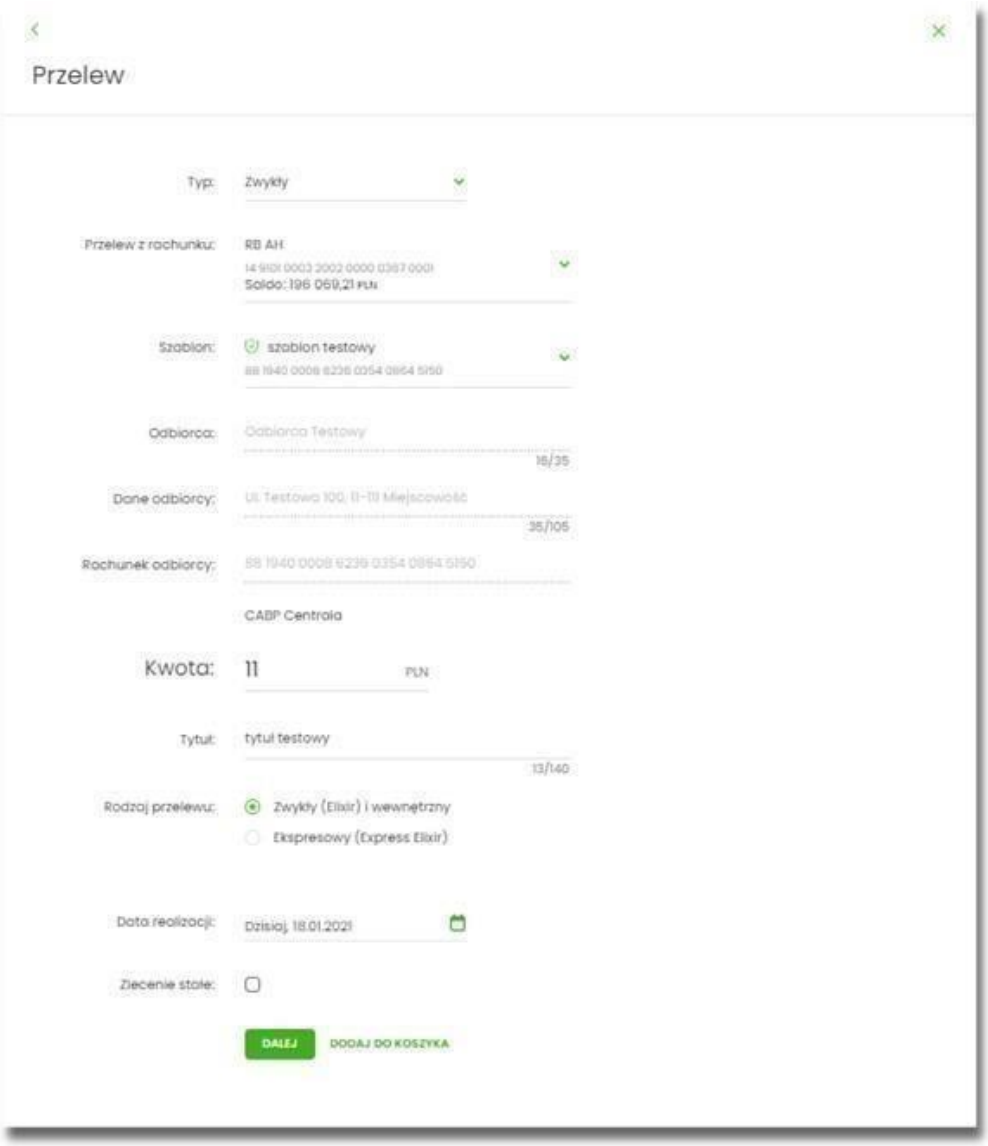
Gdy zobaczymy taki ekran jak niżej przechodzimy do aplikacji w telefonie.

Tam klikamy w powiadomienie na pasku powiadomień lub uruchamiamy aplikacje BSGo System poprosi nas o wprowadzenie PIN’u który nadaliśmy podczas parowania/rejestracji urządzenia.

Po zalogowaniu się do aplikacji zobaczymy ekran z możliwością akceptacji lub odrzucenia. Wybieramy „akceptuj”. Po czym otrzymamy powiadomienie o udanej autoryzacji:

5. Zlecenie przelewu zwykłego krajowego

Złożenie zlecenia zwykłego (krajowego) jest możliwe w przypadku, gdy na formatce nowego przelewu Użytkownik wybierze typu płatności **Zwykły.**

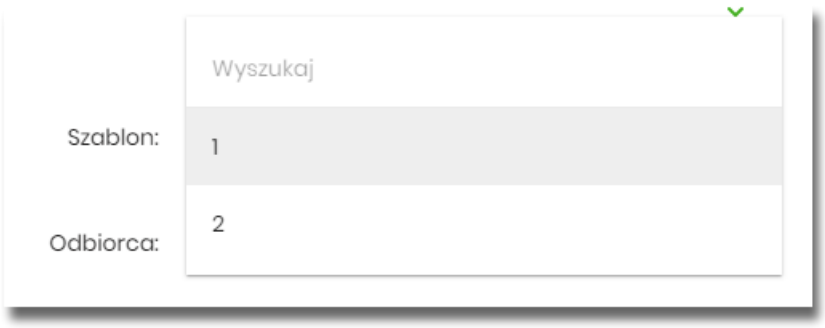

Przelew
Typ:
Zwykły
Przelew z rachunku:
RB AH
Saldo: 196 069,21 PLN
Szablon:
szablon testowy
Odbiorca:
Odbiorca Testowy
16/35
Dane odbiorcy:
35/105
Rachunek odbiorcy:
CABP Centrala
Kwota:
11
PLN
Tytuł:
tytuł testowy
13/140
Rodzaj przelewu:
Zwykły (Elixir) i wewnętrzny
Ekspresowy (Express Elixir)
Data realizacji:
Dzisiaj, 18.01.2021
Zlecenie stałe:
DALEJ
DODAJ DO KOSZYKA

Następnie Użytkownik wypełnia poniższe dane:

Typ - pole zawiera wybraną wcześniej wartość Zwykły. Kliknięcie w pole prezentuje lista typów przelewów i daje możliwość zmiany typu składanego przelewu; pole wymagalne,

Przelew z rachunku - pole z listą rachunków do obciążenia, lista rachunków ograniczona jest tylko do rachunków prowadzonych w walucie PLN i takich, do których Użytkownik ma dostęp; w polu podstawiany jest domyślny rachunek do obciążenia; pole wymagalne,

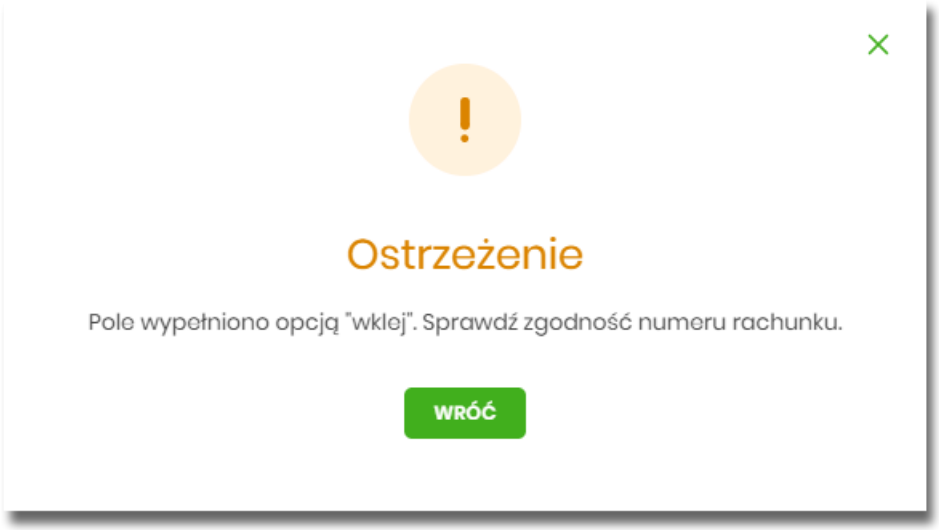
Szablon - pole z rozwijalną listą szablonów [Wybierz szablon], o ile zostały dodane lub zaimportowane,



Odbiorca - nazwa odbiorcy przelewu, wypełnione z klawiatury lub automatycznie uzupełnione w przypadku użycia szablonu - odnośnik [Wybierz szablon]; pole wymagane,

Dane odbiorcy - pełne dane odbiorcy, wypełnione z klawiatury lub automatycznie uzupełnione w przypadku użycia szablonu - odnośnik [Wybierz szablon]; pole wymagane,

Rachunek odbiorcy - numer rachunku odbiorcy; pole wymagane, wypełnione z klawiatury, wklejone lub automatycznie uzupełnione w przypadku użycia szablonu - odnośnik [Wybierz szablon]. Po wklejeniu numeru rachunku w polu prezentowany jest komunikat informujący o wklejeniu wartości w polu formularza z numerem rachunku.



Po wypełnieniu numeru rachunku pod polem prezentowana jest nazwa banku odbiorcy przelewu:

Kwota - kwota przelewu wyrażona w walucie rachunku wybranego do obciążenia; pole wymagalne.

Tytuł - tytuł przelewu, pole wymagane, pole może zawierać maksymalnie 140 znaków,

Rodzaj przelewu - możliwość wyboru następujących wartości:

◦ Zwykły (ELIXIR) i wewnętrzny

◦ Ekspresowy (Express Elixir) - znacznik dyspozycji przelewu natychmiastowego.

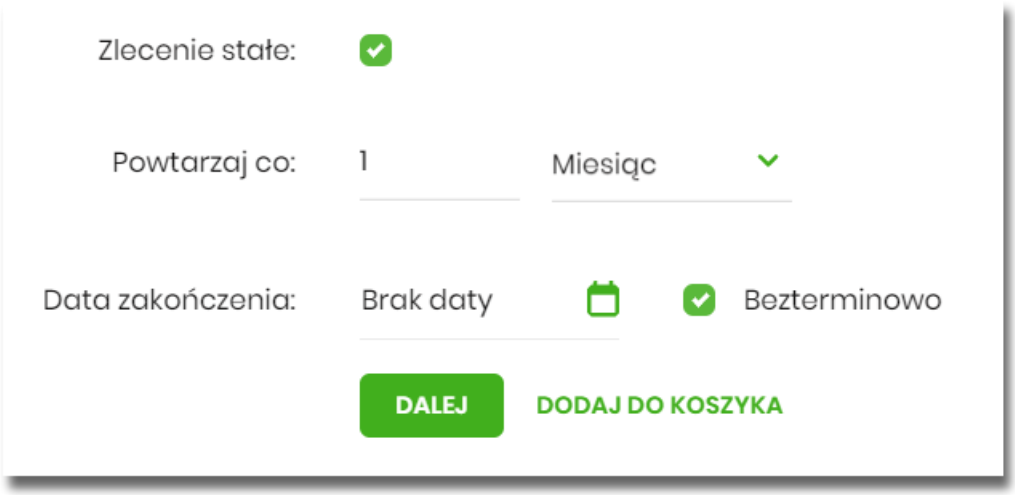
Data realizacji - data realizacji przelewu; domyślnie wstawiana jest data bieżąca poprzedzona wpisem *Dzisiaj.* W przypadku wyboru daty przyszłej (możliwość użycia ikony kalendarza) przy dacie prezentowany jest zapis: Jutro lub Za X dni.

Zlecenie stałe - checkbox umożliwiający zdefiniowanie płatności cyklicznej; po jego zaznaczeniu pojawiają się dodatkowe pola:

◦ **Powtarzaj co** - pole do określenia częstotliwości realizacji przelewu (co: *dzień/miesiąc*). Domyślnie: *1 miesiąc*,

Data zakończenia - w polu można określić datę zakończenia płatności po wybraniu ikony kalendarza

bądź ustawić bezterminową realizację płatności zaznaczając checkbox **Bezterminowo** (checkbox domyślnie zaznaczony).



[DALEJ] – przejście do kroku 2 (sprawdzenie schematu itd.) i potwierdzenie płatności.

6. Blokowanie kanałów dostępu

W przypadku utraty 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.

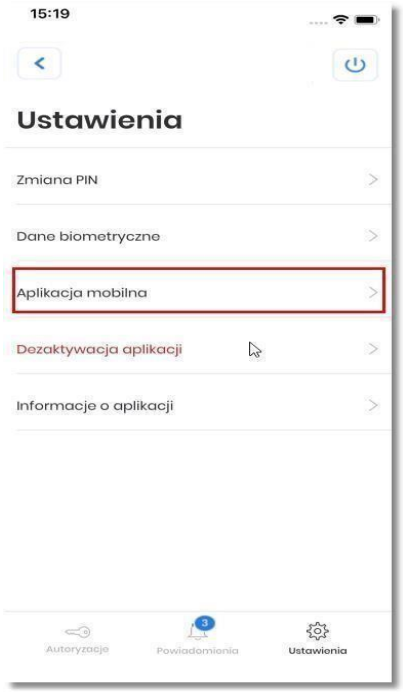
W momencie udostępnienia Klientom rozszerzonych funkcjonalności aplikacji BSGo, zostanie

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 indywidualnych”

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 indywidualnych”

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

  W przypadku aktualizacji dowodu osobistego dodatkowo konieczne jest załączenie skanu dokumentu (możliwe formaty: JPEG, JPG, PNG, GIF i PDF) w zakładce Wnioski/Inny wniosek z załącznikiem
- 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

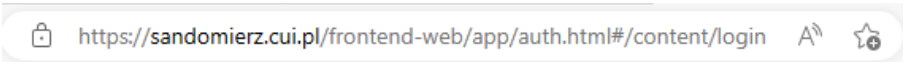
10.1 Uważaj na fałszywe wiadomości e-mail

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.

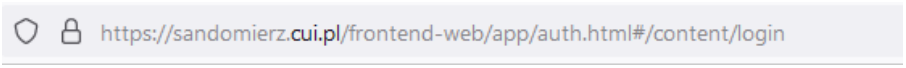
10.2 Sprawdź adres strony logowania do CUI

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 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 10-24 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.

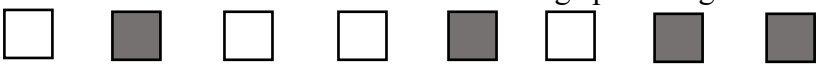
Pięciokrotne błędne wpisanie hasła powoduje blokadę dostępu do bankowości.

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.:

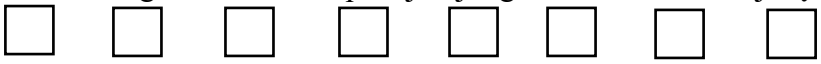
Pierwsza próba logowania:

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.