



**Instrukcja Użytkownika**  
**>Autoryzacja SMS<**  
**w Systemie Bankowości Internetowej**  
**BS online**

## Spis Treści

|                                |   |
|--------------------------------|---|
| 1. Definicje.....              | 3 |
| 2. Wstęp .....                 | 3 |
| 3. Logowanie do Systemu .....  | 3 |
| a. Pierwsze logowanie .....    | 3 |
| b. Kolejne logowania .....     | 5 |
| 4. Zmiana hasła .....          | 6 |
| 5. Autoryzacja transakcji..... | 6 |
| 6. Nieprawidłowy Kod SMS.....  | 8 |
| 7. Zablokowanie dostępu.....   | 9 |

## 1. Definicje

**Numer Identyfikacyjny** (Identyfikator użytkownika) – unikalny ciąg znaków przypisany do użytkownika. Służy do identyfikacji osoby logującej się do Systemu.

**Kod SMS** – ciąg cyfr otrzymanych za pomocą wiadomości SMS, służący do autoryzacji dyspozycji wewnątrz Systemu. Kod ma charakter jednorazowy.

**Hasło aktywacyjne** – ciąg znaków otrzymany z Banku przez użytkownika, służący do pierwszego logowania do Systemu.

**Hasło użytkownika** – własny ciąg znaków służący do autentykacji podczas logowania, ustalony przez użytkownika podczas pierwszego logowania.

**Hasło maskowane** – logowanie przy pomocy hasła maskowanego oznacza, że należy wprowadzić podczas logowania, losowo wybrane pozycje z **Hasła użytkownika** w polu **Kod dostępu**.

## 2. Wstęp

System Bankowości Internetowej Banku Spółdzielczego w Żurawicy do logowania wykorzystuje identyfikator użytkownika oraz hasła maskowane. Hasła maskowane są dodatkowym zabezpieczeniem stosowanym przez Bank podczas logowania do Systemu SBI.

Autoryzacja dyspozycji przez użytkownika, odbywa się poprzez Kod SMS, otrzymywany za pomocą wiadomości SMS na numer telefonu komórkowego podanego przez użytkownika przy składaniu wniosku o dostęp do Systemu SBI.

### UWAGA!!!

**Aktualnie otrzymany Kod SMS można wykorzystać tylko raz. Każda autoryzacja wymaga innego – kolejnego Kodu SMS.**

## 3. Logowanie do Systemu

Dostęp do bankowości internetowej znajduje się na stronie Banku Spółdzielczego w Żurawicy [www.bszurawica.pl](http://www.bszurawica.pl), po najechaniu kursorem myszki na przycisk **Logowanie** i wybraniu z rozwijanego menu **Klient indywidualny**.

Aplikacja bankowości internetowej znajduje się również pod bezpośrednim adresem: <https://cbp.cui.pl>.

W celu zalogowania się do Systemu należy podać otrzymany w Banku Identyfikator użytkownika oraz Hasło maskowane.

Proces logowania odbywa się dwustopniowo.

### a. Pierwsze logowanie

Podczas pierwszego logowania w pole „**Numer Identyfikacyjny**” należy wpisać ciąg znaków (identyfikator użytkownika) otrzymany od pracownika Banku w trakcie udostępniania usługi oraz nacisnąć przycisk [Dalej] (Rys. 1).

W przypadku Numeru Identyfikacyjnego nie ma znaczenia wielkość wprowadzanych znaków.



Numer Identyfikacyjny

**DALEJ**

Rys. 1

W kolejnym kroku zostanie zaprezentowana formatka umożliwiająca podanie hasła (**kod dostępu**) używanego do logowania.

W poszczególnych polach „**Kod dostępu**”, zaczynając od pierwszego pola, należy wprowadzić wszystkie znaki z **Hasła aktywacyjnego** otrzymanego od pracownika Banku w trakcie udostępniania usługi oraz nacisnąć przycisk [Zaloguj] (Rys. 2).



Kod dostępu

|   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |
|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |  |
|   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |

**ZALOGUJ**

Rys. 2

W kolejnym kroku System poprosi o ustalenia własnego **Hasła użytkownika** (Rys. 3).

**Hasło musi składać się z 10 do 24 dowolnych znaków**, np. 12345678901234567.

Należy wpisać w obu polach to samo hasło (Rys.3) oraz nacisnąć przycisk [Zapisz i Zaloguj].

**Uwaga!!!**

Proponujemy, aby ustalając swoje hasło używać kombinacji cyfr, małych i wielkich liter. Radzimy unikać używania łatwych haseł (jak np. własnego imienia), a za to stosować hasła trudne do rozszyfrowania (na przykład litery ze słów pochodzących z cytatów z książek lub z wymyślonych zdań).

Rys. 3

### b. Kolejne logowania

Podczas kolejnych logowań w pole „**Numer Identyfikacyjny**” należy wpisać ciąg znaków (identyfikator użytkownika) otrzymany od pracownika Banku w trakcie udostępniania usługi oraz nacisnąć przycisk [Dalej] (Rys. 1).

W przypadku Numeru Identyfikacyjnego nie ma znaczenia wielkość wprowadzanych znaków.

W pole „**Kod dostępu**” należy wpisać **Hasło maskowane**, czyli losowo wybrane wymagane pozycje z **Hasła użytkownika** oraz nacisnąć przycisk [Zaloguj] (Rys. 4).

Wymagane pola w polu „**Kod dostępu**” są aktywne, tzn. można w dane pole wprowadzić znak z hasła. Pola nieaktywne są „wyszarzone” i „wykropkowane”.

#### Uwaga!!!

**Liczba aktywnych pól do wpisania hasła może być krótsza od długości całego hasła.**

Przy wpisywaniu **Hasła maskowanego** po wpisaniu znaku następuje automatyczne przejście do kolejnego pola.

W przypadku poprawnego wprowadzenia odpowiednich znaków hasła i potwierdzeniu danych użytkownik zostanie zalogowany do Systemu.

Maska hasła zmienia się po każdym udanym logowaniu do Systemu SBI.

Przykład:

Zdefiniowane podczas pierwszego logowania Hasło użytkownika: [12345678901234567](#).

Na ekranie poniżej (Rys. 4) w pole „**Kod dostępu**” należy wprowadzić drugi, szósty, siódmy, dziewiąty, dziesiąty i dwunasty znak hasła tj.: **267902**

Rys. 4

System automatycznie kończy sesję pracy użytkownika po upływie 10 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 "Do wylogowania pozostało".

#### 4. Zmiana hasła

Ustalone podczas pierwszego logowania hasło można zmienić w dowolnym momencie. Warunkiem jest zalogowanie się do Systemu i wybranie pozycji **Ustawienia** z menu aplikacji a następnie **Zmiana hasła dostępu**.

W celu zmiany hasła należy podać Hasło maskowane (obecne hasło wprowadzone zgodnie z maską), a następnie dwukrotnie nowe hasło (Rys. 5).

**Hasło musi mieć od 10 do 24 znaków.**

System kontroluje długość hasła oraz zgodność wartości wpisanych w polu „Nowe hasło dostępu” oraz „Powtórz nowe hasło”.

Przykład:

Zdefiniowane podczas pierwszego logowania Hasło użytkownika: 12345678901234567.

Na ekranie poniżej (Rys. 5) w pole „**Obecny kod dostępu**” należy wprowadzić pierwszy, czwarty, szósty, siódmy, dziesiąty i dwunasty znak hasła tj.: 146702

W pole „**Nowe hasło dostępu**” wpisujemy np.: 9876543210987

Pole „**Powtórz nowe hasło**” wpisujemy ponownie: 9876543210987

Po naciśnięciu przycisku [Zatwierdź] hasło zostanie zmienione na 9876543210987

← Zmiana hasła dostępu X

Prosimy pamiętać, że hasło dostępu jest numerem poufnym. W związku z tym nie powinien być ujawniany osobom trzecim.  
Definiując swoje hasło dostępu pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:  
Hasło Dostępu:

- musi składać się z 10-24 znaków
- nie powinno zaczynać się od cyfry zero

Obecny kod dostępu

|    |    |    |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |   |
|----|----|----|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|---|
| 1  | 2  | 3  | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |   |
|    | .  | .  |   | . |   |   | . | . |    | .  |    | .  | .  | .  | .  | .  | .  | .  | .  | .  | . |
| 22 | 23 | 24 |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |   |
| .  | .  | .  |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |   |

Nowe hasło dostępu Wpisz nowe hasło dostępu

Powtórz nowe hasło Powtórz nowe hasło dostępu

ZATWIERDŹ

Rys.5

Po zatwierdzeniu (przycisk [Zatwierdź]), nowe hasło należy stosować od najbliższego logowania w Systemie.

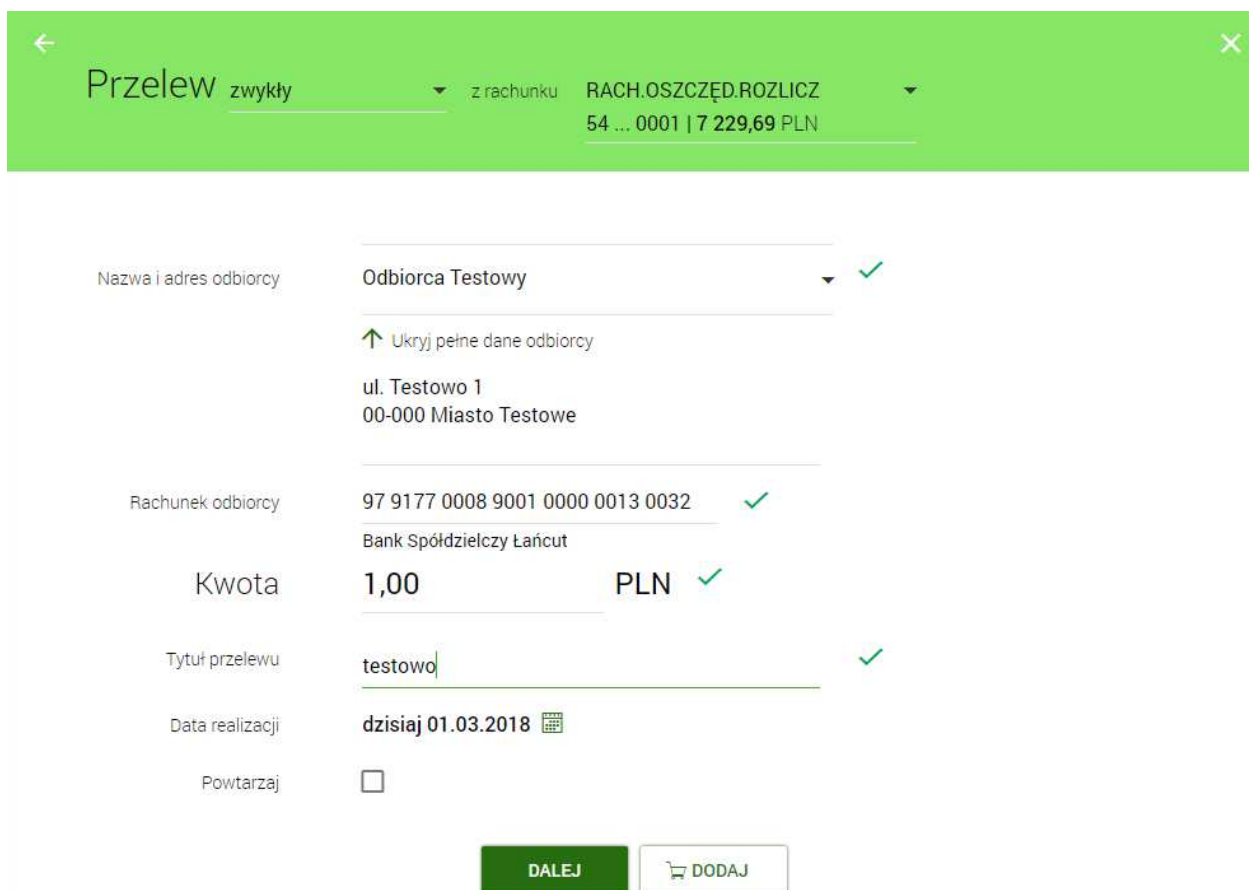
#### 5. Autoryzacja transakcji

Każda operacja mająca wpływ na zmianę stanu środków na rachunku wymaga autoryzacji **Kodem SMS** otrzymywanym za pomocą wiadomości SMS na numer telefonu komórkowego podanego przez użytkownika przy składaniu wniosku o dostęp do Systemu SBI.

Przykład:

Proces autoryzacji operacji Kodem SMS jest następujący:

- rysunek nr 6 przedstawia ekran formatki zlecenia przelewu,
- przejście do ekranu potwierdzenia danych poprzez wybór przycisku [Dalej] na formatce zlecenia, skutkuje wysłaniem do użytkownika (na numer telefonu komórkowego podanego przez użytkownika w momencie składania wniosku i zapisanego w Systemie), wygenerowanego na podstawie danych zlecenia/dyspozycji Kodu SMS; (opcja [Dodaj] przekazuje zlecenie do koszyka),
- na ekranie potwierdzenia operacji (Rys. 7) prezentowany jest opis pola „Podaj kod autoryzacyjny” do wprowadzenia Kodu SMS zawierający nr operacji autoryzowanej w danym dniu np: „*Operacja nr 1 z dnia 01.03.2018*”,
- zlecenie będzie poprawnie zautoryzowane po wprowadzeniu właściwego Kodu SMS dla danej operacji oraz po wyborze przycisku [Akceptuj]”.



← Przelew zwykły z rachunku RACH.OSZCZĘD.ROZLICZ 54 ... 0001 | 7 229,69 PLN ×

Nazwa i adres odbiorcy Odbiorca Testowy ✓  
↑ Ukryj pełne dane odbiorcy  
ul. Testowo 1  
00-000 Miasto Testowe

Rachunek odbiorcy 97 9177 0008 9001 0000 0013 0032 ✓  
Bank Spółdzielczy Łańcut

Kwota 1,00 PLN ✓

Tytuł przelewu testowo ✓

Data realizacji dzisiaj 01.03.2018 📅

Powtarzaj

DALEJ DODAJ

Rys. 6

←
×

## Przelew

zwykły z rachunku RACH.OSZCZĘD.ROZLICZ | 54 9177 0008 3001      0001

|   |  |
|---|--|
| Odbiorca  | Odbiorca Testowy<br>ul. Testowo 1<br>00-000 Miasto Testowe   |
| Rachunek odbiorcy   | 97 9177 0008 9001 0000 0013 0032<br>Bank Spółdzielczy Łańcut |
| <b>Kwota</b>  | <b>1,00 PLN</b>  |
| Tytułem   | testowo  |
| Data realizacji   | dzisiaj<br>01.03.2018  |
| <span style="color: #00b050;">↓</span> Pokaż dodatkowe informacje |  |
| Podaj kod autoryzacyjny   | Wpisz kod<br>Operacja nr 1 z dnia 01.03.2018                 |

AKCEPTUJ

Rys. 7

### Uwaga!!!

**Każdorazowe wejście na formatkę potwierdzenia danych zlecenia (nawet w przypadku powrotu do formularza bez faktycznej zmiany danych) powoduje wygenerowanie i wysłanie nowego Kodu SMS.**

Do każdej operacji generowany jest oddzielny Kod SMS.

Prosimy o każdorazowe weryfikowanie poprawności danych otrzymanych w treści wiadomości.

**Uwaga: Kod autoryzacji należy wpisać i zatwierdzić do 3 minut, gdyż po tym okresie wygasa jego ważność.**

W przypadku braku dostępności systemu autoryzacji generowany jest komunikat „System autoryzacji niedostępny. Prosimy spróbować później”.

## 6. Nieprawidłowy Kod SMS

Wielokrotna niepoprawna autoryzacja operacji (błędnie podany Kod lub Kod nieważny z powodu wygaśnięcia) spowoduje zablokowanie dalszej możliwości autoryzacji zleceń (zablokowanie urządzenia autoryzacji tj. numeru telefonu komórkowego użytkownika, do czasu odblokowania urządzenia autoryzacji przez pracownika Banku). W takiej sytuacji zostanie zaprezentowany komunikat „Brak aktywnego telefonu dla usługi SMS”.



## 7. Zablokowanie dostępu

W przypadku podania błędnych danych (w pole „**Kod dostępu**”), System wyświetli stosowny komunikat „**Niepoprawne dane do autoryzacji**” (Rys. 10), a użytkownik nie zostanie zalogowany.



The screenshot shows a login interface with a green header containing a back arrow and the word "LOGOWANIE". Below the header is a 24-character password field labeled "Kod dostępu". The field consists of 24 boxes, each containing a dot. The second box from the left has a vertical cursor. Below the password field, a red error message reads "▲ Niepoprawne dane do autoryzacji". At the bottom center, there is a green button labeled "ZALOGUJ".

Rys. 8

Wielokrotne niepoprawne logowanie spowoduje zablokowanie dostępu do Systemu Bankowości Internetowej.

**W przypadku zablokowania dostępu należy skontaktować się z Bankiem:**

- **osobiście** – w placówce Banku, która wydała dostęp do Systemu SBI,
- **telefonicznie** – pod numerem telefonu 16 672 37 84.

### **Uwaga!**

W przypadku kontaktu telefonicznego, warunkiem przyjęcia dyspozycji odblokowania dostępu jest potwierdzenie tożsamości posiadacza rachunku lub użytkownika i potwierdzenie jego uprawnień do korzystania z Systemu Bankowości Internetowej SBI i dysponowania rachunkiem bankowym.

**W celu odblokowania dostępu do Systemu SBI, użytkownikowi zostanie wydane nowe Hasło aktywacyjne, które jest przesyłane wiadomością SMS na numer telefonu komórkowego podanego przez użytkownika w momencie składania wniosku i zapisanego w Systemie.**

**Po otrzymaniu Hasła aktywacyjnego użytkownik postępuje zgodnie z pkt. 3a niniejszej Instrukcji.**

Na stronie internetowej Banku: [www.bszurawica.pl](http://www.bszurawica.pl) dostępne są szczegółowe informacje na temat systemu oraz pełne instrukcje użytkownika.