

**Instrukcja Użytkownika
Token SID 700
w Systemie Bankowości Internetowej
BS online**

Spis Treści

1. Definicje	3
2. Wstęp	3
3. Logowanie do Systemu	3
<i>a. Pierwsze logowanie</i>	4
<i>b. Kolejne logowania</i>	6
4. Zmiana hasła	6
5. Autoryzacja transakcji	7
6. Zablokowanie dostępu	9

1. Definicje

Token – urządzenie generujące ciąg cyfr.

Identyfikator użytkownika – unikalny ciąg znaków przypisany do użytkownika. Służy do identyfikacji osoby logującej się do Systemu.

Kod dostępu – unikalny ciąg znaków służący do autentykacji podczas logowania oraz autoryzacji transakcji wewnątrz Systemu.

Wskazanie tokena – aktualnie wyświetlany ciąg cyfr

Hasło – własny ciąg znaków ustalony przez użytkownika podczas pierwszego logowania.

2. Wstęp

System Bankowości Internetowej Banku Spółdzielczego w Łąncucie zarówno do logowania, jak i autoryzacji transakcji wykorzystuje token RSA SecurID 700 (Rys. 1). Urządzenie to nie wymaga żadnych czynności od użytkownika. Ciąg sześciu cyfr generowany jest automatycznie co 60 sekund.



Rys. 1

Token sygnalizuje czas pozostały do wyświetlenia kolejnego ciągu. Symbolizowane jest to sześcioma poziomymi kreskami po lewej stronie wyświetlacza (Rys. 2).



Rys. 2

UWAGA!!!

Aktualnie wyświetlany ciąg cyfr można wykorzystać tylko raz. Każda autoryzacja wymaga innego – kolejnego ciągu cyfr.

3. Logowanie do Systemu

Dostęp do bankowości internetowej znajduje się na stronie Banku Spółdzielczego w Łąncucie www.bslancut.pl, po najechaniu kursorem myszki na przycisk **Logowanie** i wybraniu z rozwijanego menu **Klient indywidualny**.

KLIENCI INDYWIDUALNI

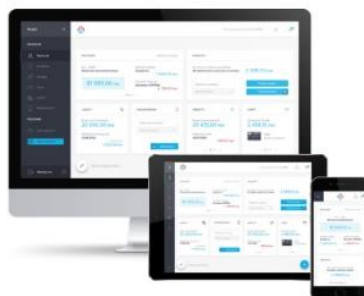
FIRMY I INSTYTUCJE

ROLNICY

KALKULATOR
KREDYTOWY

LOGOWANIE do bankowości internetowej

Nowy system BS online



Zaloguj się

więcej

Dotychczasowy system bankowości internetowej
dostępny do 31.05.2018r.

Zaloguj się

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

W celu zalogowania się do Systemu należy podać otrzymany w Banku Identyfikator użytkownika oraz Kod dostępu.

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.

LOGOWANIE PL ▾

Numer Identyfikacyjny

DALEJ

Rys. 3

W pole „**Kod dostępu**” należy wpisać **wyłącznie aktualne wskazanie tokena** (Rys. 4) oraz nacisnąć przycisk [Zaloguj]” (Rys. 5).

W poniższym przykładzie wskazaniem tokena będzie ciąg cyfr: 959759



Rys. 4



Kod dostępu

ZALOGUJ

Rys. 5

W kolejnym kroku System poprosi o ustalenia własnego hasła (hasło dostępu) (Rys. 6).


Hasło musi składać się z 4 do 8 dowolnych znaków, np. 123456.

Należy wpisać w obu polach to samo hasło (Rys.6) 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). Przykład dobrego hasła: **wmi4Mzjs** pochodzące ze zdania „W moje imieniny 4 marca zawsze jest słonecznie”.



 Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator
użytkownika

LA

Nowe hasło dostępu

Powtórz nowe hasło

ZAPISZ I ZALOGUJ

Definiując swoje nowe hasło dostępu pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

- o musi składać się z 4-8 znaków

Rys. 6

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. 3).

W przypadku Numeru Identyfikacyjnego nie ma znaczenia wielkość wprowadzanych znaków.

W pole „**Kod dostępu**” należy wpisać **hasło wraz z aktualnym wskazaniem tokena** oraz nacisnąć przycisk [Zaloguj] (Rys. 5).

Przykład: Wskazanie tokena (Rys. 7): 959759

Zdefiniowane podczas pierwszego logowania hasło: 123456.

W pole „**Kod dostępu**” należy wpisać: 123456959759



Rys. 7

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":



Do wylogowania pozostało 00:34



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 obecny Kod dostępu (**obecne hasło wraz ze aktualnym wskazaniem tokena**), a następnie dwukrotnie nowe hasło (Rys. 9).

Hasło musi mieć od 4 do 8 znaków.

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

Przykład:

Wskazanie tokena (Rys.8): 959759

Zdefiniowane podczas pierwszego logowania hasło: 123456

W pole „**Obecny kod dostępu**” należy wpisać: 123456959759



Rys. 8

W pole „**Nowe hasło dostępu**” wpisujemy np.: 1111
Pole „**Powtórz nowe hasło**” wpisujemy ponownie: 1111
Po naciśnięciu przycisku [Zatwierdź] hasło zostanie zmienione na 1111.

← Zmiana hasła dostępu ×

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 4-8 znaków

Obecny kod dostępu:

Nowe hasło dostępu:

Powtórz nowe hasło:

ZATWIERDŹ

Rys.9

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

Uwaga!!!

Zmiana hasła nie ma związku ze wskazaniami tokena i nie zwalnia użytkownika z konieczności stosowania wskazania tokena podczas logowania/autoryzacji dyspozycji w Systemie SBI.

5. Autoryzacja transakcji

Każda operacja mająca wpływ na zmianę stanu środków na rachunku wymaga autoryzacji **Kodem dostępu** (Klucz do podpisu).

Przykład:

Proces autoryzacji operacji jest następujący:

- rysunek nr 10 przedstawia ekran formatki zlecenia przelewu,

- przejście do ekranu potwierdzenia danych wykonujemy poprzez wybór przycisku [Dalej]; (opcja [Dodaj] przekazuje zlecenie do koszyka),
- na ekranie potwierdzenia operacji (Rys. 12) prezentowany jest opis pola „**Klucz do podpisu**” do wprowadzenia hasła wraz z aktualnym wskazaniem tokena np.:
Rysunek 12 przedstawia ekran potwierdzenia dyspozycji przelewu.
Formularz zawiera dane dotyczące odbiorcy, kwoty zlecenia oraz pole „**Klucz do podpisu**”.
Wskazanie tokena (Rys. 11): 959759
Zdefiniowane hasło: 123456
W pole „**Klucz do podpisu**” należy wpisać: 123456959759
- zlecenie będzie zautoryzowane po wprowadzeniu poprawnego Klucza do podpisu oraz po wyborze przycisku [Akceptuj]”.

← Przelew zwykły z rachunku RACH.OSZCZĘD.ROZLICZ 54 ... 0001 | 5 862,57 PLN

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

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

Kwota: 1,00 PLN ✓

Tytuł przelewu: testowo ✓

Data realizacji: dzisiaj 19.03.2018 📅

Powtarzaj:

DALEJ DODAJ

Rys. 10



Rys. 11

←
×

Przelew

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

Odbiorca	Odbiorca Testowy ul. Testowa 1 00-000 Miasto Testowe
Rachunek odbiorcy	97 9177 0008 9001 0000 0013 0032 Bank Spółdzielczy Łańcut
Kwota	1,00 PLN
Tytułem	testowo
Data realizacji	dzisiaj 19.03.2018
	↓ Pokaż dodatkowe informacje
Klucz do podpisu	Hasło i kod z tokena

AKCEPTUJ

Rys. 12

6. Zablokowanie dostępu

W przypadku podania błędnych danych (w pole „**Kod dostępu**”), System wyświetli stosowny komunikat „[Niepoprawne dane do autoryzacji](#)” (Rys. 16), a użytkownik nie zostanie zalogowany.

←

LOGOWANIE

Kod dostępu

▲ Niepoprawne dane do autoryzacji

ZALOGUJ

Rys. 16

Wielokrotne niepoprawne logowanie spowoduje zablokowanie dostępu do Systemu Bankowości Internetowej.

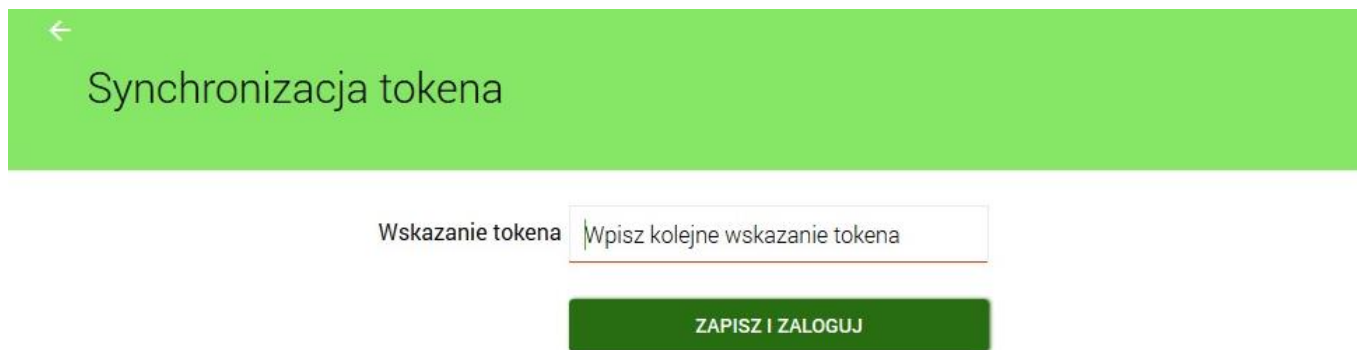
W przypadku zablokowania dostępu należy skontaktować się z Bankiem:

- osobiście – w placówce Banku, która wydała dostęp do Systemu SBI,
- telefonicznie – pod numerem telefonu 17 225 83 00.

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 odblokowane przez pracownika Banku urządzenie autoryzacji tj. Token oraz zresetowane Hasło. Po odblokowaniu dostępu użytkownik postępuje zgodnie z pkt. 3a niniejszej Instrukcji, a potwierdzając nadanie nowego hasła wprowadza, celem synchronizacji tokena, kolejne wskazanie tokena i zatwierdza przyciskiem [Zapisz i Zaloguj] (Rys. 17).



Rys. 17

Na stronie internetowej Banku: www.bslancut.pl dostępne są szczegółowe informacje na temat systemu oraz pełne instrukcje użytkownika.