



BANK SPÓŁDZIELCZY W SŁAWNIE

Spółdzielcza Grupa Bankowa

Zmiany w logowaniu do bankowości internetowej i autoryzacji operacji od dnia 14 września 2019 r.

Silne uwierzytelnienie Klienta

Silne uwierzytelnienie Klienta, to inaczej uwierzytelnienie dwuskładnikowe, które ma podnieść stopień weryfikacji tożsamości Klienta.

Bank udostępnia 3 rodzaje autoryzacji:

- Autoryzacja – hasła SMS wraz z dodatkowym kodem uwierzytelnienia
- lub
- Autoryzacja nPodpis
- Autoryzacja e-Token – wydawanym po 14.09.2019

To Klient wybiera, z której metody chce korzystać.

Silne uwierzytelnienie jest wymagane przy logowaniu do systemu bankowości internetowej

- Autoryzacja – hasła SMS

W przypadku gdy silne uwierzytelnienie Klienta wymagane jest przy logowaniu do bankowości internetowej wówczas każdorazowo takie logowanie jest dwuetapowe: wpisujemy login i hasło, w drugim etapie wpisujemy dodatkowe hasło z SMS. Okna logowania do systemu wyglądają:

Bank Spółdzielczy
w Naszej Miejscowości

Logowanie

Identyfikator: 61488201

Hasło:

Zaloguj

2019-06-06 14:03


**Bank Spółdzielczy
w Naszej Miejscowości**

Logowanie

Identyfikator: 61488201

Hasło SMS:

Zatwierdź



■ Dodatkowy kod uwierzytelnienia

W przypadku gdy do autoryzacji SMS wymagany jest dodatkowy kod uwierzytelnienia wówczas każdorazowo logowanie i każda operacja, która wymaga podania hasła SMS, poprzedzana jest kodem uwierzytelnienia.

Kod uwierzytelnienia należy ustawić zgodnie z komunikatami wyświetlanymi przez system IB.

W trakcie logowania do serwisu Internet Banking, po wpisaniu identyfikatora i hasła, wyświetli się komunikat do podania hasła SMS:


**Bank Spółdzielczy
w Naszej Miejscowości**

Logowanie

Identyfikator: 61488201


Hasło:

Zaloguj



Bank Spółdzielczy w Naszej Miejscowości

Logowanie



2019-05-17 12:17

Identyfikator: 61488201

Hasło SMS:

Zatwierdź

Po wpisaniu hasła i poprawnym zalogowaniu się do Internet Bankingu system wyświetli okno *Ustawień - Kod uwierzytelnienia do haseł SMS*. Kod powinien zawierać 4 cyfry, posłuży do logowania do systemu i autoryzacji transakcji - gdy operacja będzie wymagała podania hasła SMS, należy poprzedzić je kodem uwierzytelnienia. Ustawienia zatwierdzamy przyciskiem **Zatwierdź**. Podajemy otrzymane hasło SMS autoryzujące tą operację i wybieramy **Podpisz**

Kod uwierzytelnienia do haseł SMS

Wprowadź i zapamiętaj swój 4-cyfrowy kod uwierzytelnienia, który będziesz podawać wraz z hasłem SMS. Każdorazowo, gdy operacja będzie wymagała podania hasła SMS, poprzedź je kodem uwierzytelnienia.

Wprowadź 4-cyfrowy kod:

Powtórz 4-cyfrowy kod:

Anuluj **Zatwierdź**

Kod uwierzytelnienia do haseł SMS

Wprowadź i zapamiętaj swój 4-cyfrowy kod uwierzytelnienia, który będziesz podawać wraz z hasłem SMS. Każdorazowo, gdy operacja będzie wymagała podania hasła SMS, poprzedź je kodem uwierzytelnienia.

Wprowadź 4-cyfrowy kod:

Powtórz 4-cyfrowy kod:

Hasło SMS:

Anuluj **Podpisz**

W momencie gdy kod uwierzytelnienia zostanie zdefiniowany, w oknie logowania do systemu po wpisaniu identyfikatora i hasła zostanie wyświetlone okno do wprowadzenia kodu uwierzytelnienia oraz hasła SMS:



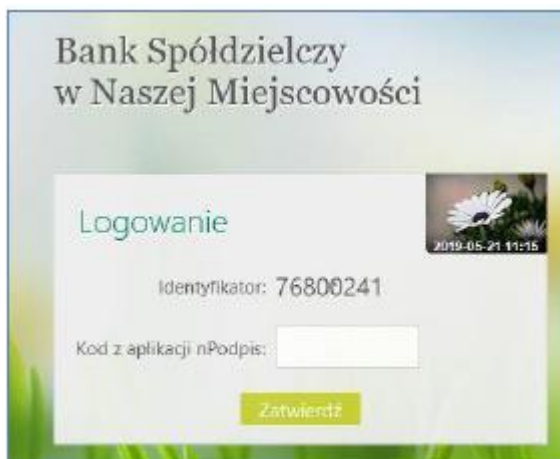
Wprowadzenie kodu uwierzytelnienia do haseł SMS będzie wymagane w oknie autoryzacji operacji.

Kod uwierzytelniania można zmienić w opcji Ustawienia – Bezpieczeństwo

■ Autoryzacja nPodpis

Korzystając z aplikacji nPodpis do obsługi certyfikatu, podczas logowania do systemu Internet Banking, w aplikacji wyświetli się kod uwierzytelnienia logowania, a w oknie logowania w serwisie IB po wpisaniu własnego identyfikatora i hasła pojawi się okno do wprowadzenia „Kodu z aplikacji nPodpis”

:



WAŻNE!

Wylogowanie

Po zakończonej pracy należy pamiętać o wylogowaniu się z systemu. Służy do tego przycisk:

Wyloguj znajdujący się w prawym górnym rogu, po użyciu którego wyświetlana jest informacja: „Nastąpiło bezpieczne wylogowanie z serwisu”.

Przycisk **OK** umożliwia natychmiastowe przejście do strony głównej serwisu i pozwala na ponowne zalogowanie.

Automatyczne wylogowanie nastąpi, jeżeli:

- użytkownik przerwie pracę na dłuższy czas (nie wykona żadnej akcji w systemie);
- w przypadku zamknięcia okna przeglądarki, opuszczenia systemu przez wybór innego adresu w przeglądarce,
- gdy użytkownik ponownie zaloguje się do systemu w innym oknie przeglądarki lub z innego komputera,
- przy próbie odświeżenia strony przez klienta.

W celu zwiększenia bezpieczeństwa zablokowano dostęp do historii przeglądanych stron. Bezpośrednio po wylogowaniu nie można zastosować przycisku strzałki „Wstecz”.

Wznowienie pracy z systemem po wylogowaniu wymaga ponownego zalogowania.