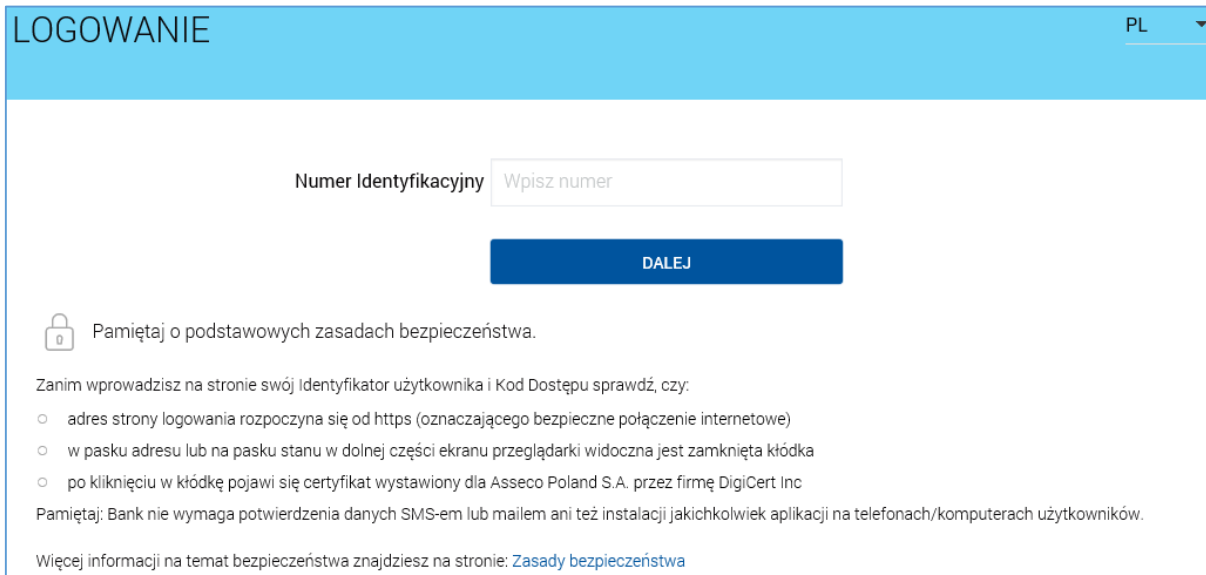


Pierwsze logowanie za pomocą tokena.


1. Uruchom przeglądarkę internetową i przejdź do witryny **www.gbsmosina.pl**.
2. Po wczytaniu witryny Gospodarczego Banku Spółdzielczego w Mosinie kliknij (po prawej stronie) w link **„Bank dla klienta indywidualnego”**.
3. W nowo otwartym oknie przeglądarki w polu **„Numer Identyfikacyjny”** podaj ciąg 6 znaków (identyfikator użytkownika) otrzymany z banku na kolorowym kartoniku i kliknij przycisk **„DALEJ”**.



LOGOWANIE PL

Numer Identyfikacyjny

DALEJ

 Pamiętaj o podstawowych zasadach bezpieczeństwa.

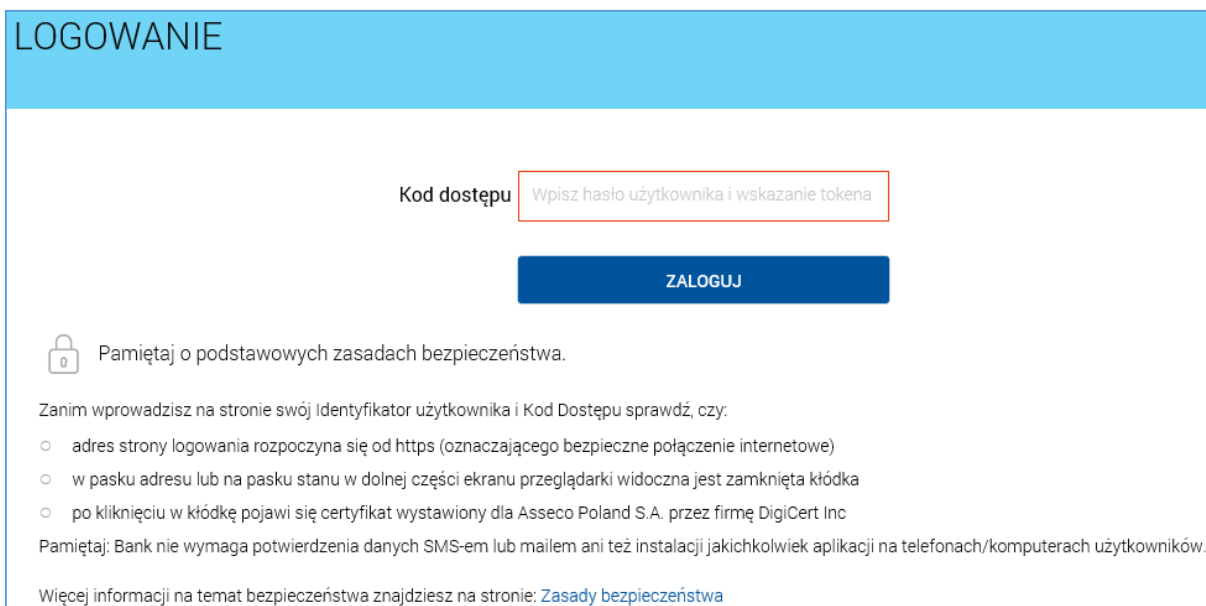
Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Asseco Poland S.A. przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)


4. W kolejnym etapie w polu **„Kod dostępu”** wpisz 6 cyfrowy kod wyświetlany na tokenie, a następnie kliknij **„ZALOGUJ”**. Należy tutaj pamiętać, że wyświetlany 6 cyfrowy kod na tokenie jest ważny tylko przez **60 sekund** po czym wygenerowany zostaje nowy 6 cyfrowy kod dostępu.



LOGOWANIE

Kod dostępu

ZALOGUJ

 Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:


- o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Asseco Poland S.A. przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

5. Po prawidłowym podaniu ciągu 6 cyfr z tokena, system zażąda od nas nadania własnego hasła. Własne hasło musi mieć długość od 4 do 8 znaków. Hasła zawierające więcej niż 8 znaków zostaną obcięte do pierwszych 8 znaków. We własnym hasle nie należy używać polskich znaków.

NADAWANIE NOWEGO KODU DOSTĘPU

 Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator użytkownika

Nowy kod dostępu

Powtórz nowy kod dostępu

ZAPISZ I ZALOGUJ

Definiując swój nowy kod dostępu pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

- musi składać się z 4-8 znaków

W polu „**Identyfikator użytkownika**” podaj ciąg 6 znaków otrzymany z banku na kolorowym kartoniku. W polu „**Nowy kod dostępu**” i „**Powtórz nowy kod dostępu**” wpisz własne hasło. Następnie kliknij „**ZAPISZ I ZALOGUJ**”.

6. Jeśli w powyższym kroku wszystkie dane zostaną podane poprawnie, pojawi się nowe okno z synchronizacją tokena. W polu „**Wskazanie tokena**” wpisz 6 cyfrowy kod wyświetlany na tokenie, a następnie kliknij „**ZAPISZ I ZALOGUJ**”. W tym miejscu należy podać 6 cyfrowy kod wyświetlany na tokenie, ale różny od tego, który został podany w kroku 4.

SYNCHRONIZACJA TOKENA

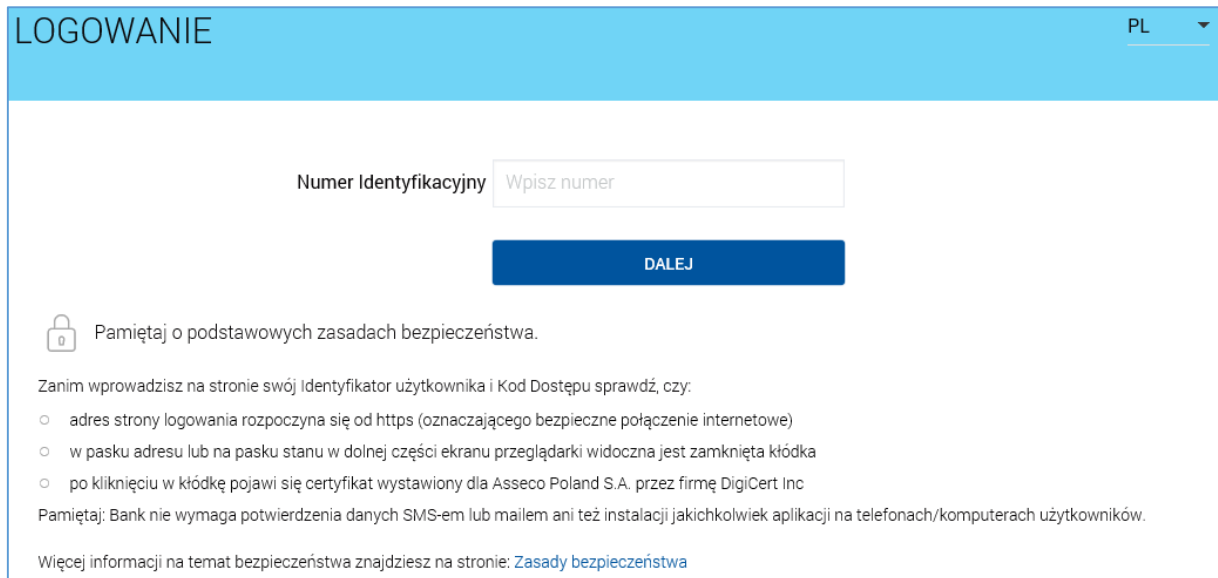
Wskazanie tokena

ZAPISZ I ZALOGUJ

Po pomyślnym zatwierdzeniu wskazania tokena, od tego momentu logowanie oraz każda operacja na koncie będzie wymagała podania kodu dostępu/autoryzującego w postaci: **własne hasło użytkownika, a zaraz za nim aktualne wskazanie z tokena.**

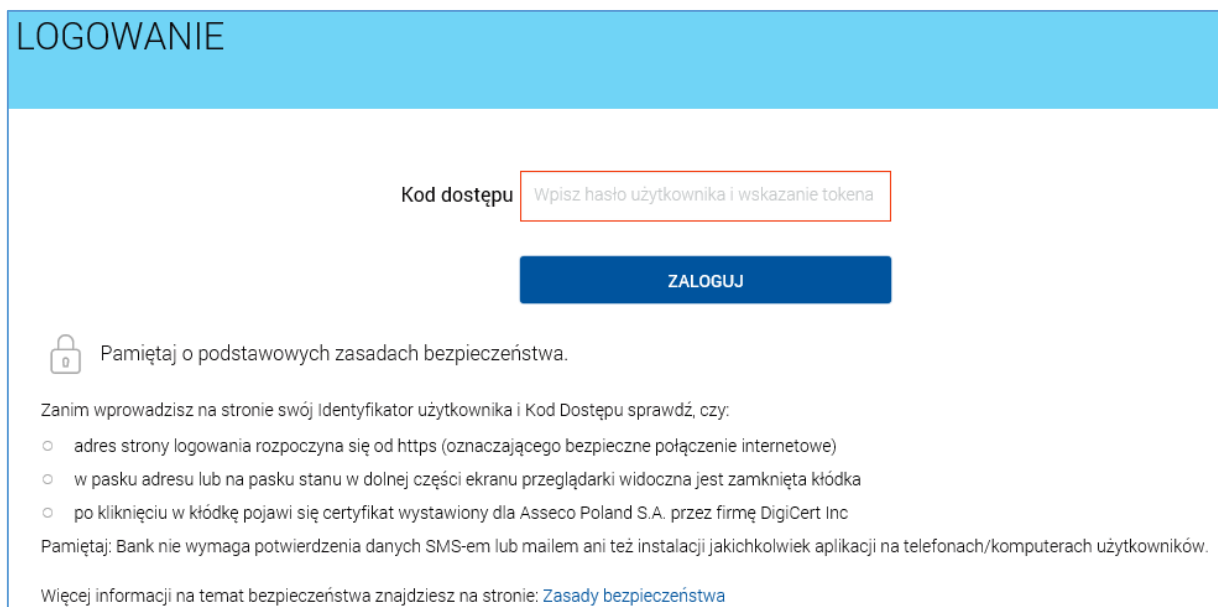
Drugie i kolejne logowanie za pomocą tokena.

1. Uruchom przeglądarkę internetową i przejdź do witryny **www.gbsmosina.pl**.
2. Po wczytaniu witryny Gospodarczego Banku Spółdzielczego w Mosinie kliknij (po prawej stronie) w link „**Bank dla klienta indywidualnego**”.
3. W nowo otwartym oknie przeglądarki w polu „**Numer Identyfikacyjny**” podaj ciąg 6 znaków (identyfikator użytkownika) otrzymany z banku na kolorowym kartoniku i kliknij przycisk „**DALEJ**”.



The screenshot shows the login page with a blue header containing the word "LOGOWANIE" and a language selector "PL". The main content area has a white background. At the top, there is a label "Numer Identyfikacyjny" followed by a text input field with the placeholder "Wpisz numer". Below the input field is a blue button labeled "DALEJ". Underneath the button, there is a lock icon and the text "Pamiętaj o podstawowych zasadach bezpieczeństwa." followed by a list of instructions: "Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:" followed by three bullet points: "adres strony logowania rozpoczyna się od https (oznacza bezpieczne połączenie internetowe)", "w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka", and "po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Asseco Poland S.A. przez firmę DigiCert Inc". Below this is another reminder: "Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników." At the bottom, there is a link: "Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)".

4. W kolejnym etapie w polu „**Kod dostępu**” wpisz ustalone wcześniej własne hasło użytkownika (od 4 do 8 znaków), a zaraz za nim 6 cyfrowy kod wyświetlany na tokenie. Kliknij przycisk „**ZALOGUJ**”. Należy tutaj pamiętać, że wyświetlany 6 cyfrowy kod na tokenie jest ważny tylko przez **60 sekund** po czym wygenerowany zostaje nowy 6 cyfrowy kod dostępu.



The screenshot shows the login page with a blue header containing the word "LOGOWANIE" and a language selector "PL". The main content area has a white background. At the top, there is a label "Kod dostępu" followed by a text input field with the placeholder "Wpisz hasło użytkownika i wskazanie tokena". Below the input field is a blue button labeled "ZALOGUJ". Underneath the button, there is a lock icon and the text "Pamiętaj o podstawowych zasadach bezpieczeństwa." followed by a list of instructions: "Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:" followed by three bullet points: "adres strony logowania rozpoczyna się od https (oznacza bezpieczne połączenie internetowe)", "w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka", and "po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Asseco Poland S.A. przez firmę DigiCert Inc". Below this is another reminder: "Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników." At the bottom, there is a link: "Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)".

... UWAGA ...

Po 3 nieudanych próbach zalogowania się do konta internetowego (za pomocą tokena), dostęp zostanie automatycznie zablokowany. W takim przypadku należy skontaktować się z działem obsługi bankowości internetowej w celu odblokowania dostępu do konta internetowego (tel. **+48 61 81 97 708** lub **+48 61 81 97 728**, od **poniedziałku** do **piątku** w godz. **8:00 - 18:00**). Po odblokowaniu w/w dostępu, logowanie do konta internetowego przebiega tak samo jak przy pierwszym logowaniu za pomocą tokena.

... BEZPIECZEŃSTWO ...

1. Zawsze sprawdzaj adres internetowy strony logowania do bankowości internetowej. W przypadku Gospodarczego Banku Spółdzielczego w Mosinie, adres internetowy strony logowania do bankowości internetowej to „<https://cbp.cui.pl>” lub „cbp.cui.pl” („Bank dla klienta indywidualnego”).
2. Zawsze sprawdzaj czy połączenie z bankowością internetową jest szyfrowane - na pasku adresu lub obok paska adresowego (w którym dla Gospodarczego Banku Spółdzielczego w Mosinie musi widnieć adres „<https://cbp.cui.pl>” lub „cbp.cui.pl”) musi być widoczny symbol „*zatrzaśniętej kłódki*”. Współczesne przeglądarki internetowe sygnalizują połączenie szyfrowane znakiem *zielonej „zatrzaśniętej kłódki*” na pasku adresu. Brak „zatrzaśniętej kłódki” lub „kłódka przekreślona” oznaczają, że mamy do czynienia z niebezpiecznym połączeniem, w którym dane nie są szyfrowane. W takim przypadku prosimy o zaprzestanie używania wyświetlonej strony internetowej i kontakt z działem obsługi bankowości internetowej banku.
3. Nigdy nie ignoruj ostrzeżeń przeglądarek internetowych o błędnych certyfikatach na stronach bankowości internetowej.
4. Nie wchodź w linki do bankowości internetowej przesyłane w mailach.
5. Uważaj na fałszywe e-maile od nieznanymi osobami i załączniki dołączane do e-maili - szczególnie dotyczące rzekomych przesyłek, ciekawych artykułów, wezwań do zapłaty, faktur do opłacenia, itp. Zawsze sprawdzaj adres, z którego została przesłana wiadomość, a w przypadku wątpliwości skontaktuj się telefonicznie z firmą, od której rzekomo pochodzi.
6. Zadbaj o regularną zmianę hasła do bankowości internetowej. Nie powinno być ono zbyt proste. Nie zapisuj danych logowania w przeglądarkach internetowych i/lub na dyskach twardych komputerów.
7. Chronić dane do logowania do bankowości internetowej - nie przekazuj ich nawet najbliższym osobom. Jeśli chcesz, aby powyższe osoby mogły korzystać z Twojego konta w bankowości internetowej, możesz ustanowić dla nich w banku stosowne pełnomocnictwo.
8. Po zakończeniu pracy w bankowości internetowej wyloguj się używając przeznaczonej do tego opcji, gwarantuje to poprawne zamknięcie sesji przez użytkownika.
9. Nie loguj się do bankowości internetowej z ogólnodostępnych komputerów i nie korzystaj z bankowości internetowej poprzez nieznaną Tobie, niezabezpieczoną sieć wifi (np. w punktach bezpłatnego publicznego dostępu do Internetu - w tzw. hot-spotach).
10. Aktualizuj na bieżąco system operacyjny komputera i przeglądarki internetowe z których korzystasz.
11. Na komputerach na których korzystasz z bankowości internetowej używaj aktualizowanego na bieżąco programu antywirusowego.
12. Czytaj dokładnie treść SMS'ów autoryzacyjnych - treść powinna dokładnie zgadzać się z transakcją, którą zlecasz w serwisie bankowości internetowej.
13. Sprawdzaj poprawność numeru NRB odbiorcy przed i po zatwierdzeniu przelewu do dyspozycji w bankowości internetowej.
14. Jeśli otrzymasz komunikat o przerwie konserwacyjnej bankowości internetowej podczas realizacji przelewu, zrezygnuj z dalszej realizacji przelewu i skontaktuj się z działem obsługi bankowości internetowej banku.