

Instrukcja pierwszego logowania użytkownika do usługi CUI dla klientów z autoryzacją tokenów RSA.

Uruchomić przeglądarkę internetową – wpisać adres strony **https://cbp.cui.pl** lub na stronie **http://www.bsklodzko.pl** wybrać odnośnik(link) na górze ekranu Logowanie – Klient indywidualny.

Po uruchomieniu aplikacji zostaje wyświetlone okno autoryzacji.

The screenshot shows a light blue header with the word "LOGOWANIE" on the left and "PL" with a dropdown arrow on the right. Below the header is a form with a label "Numer Identyfikacyjny" and a text input field containing the placeholder "Wpisz numer". Below the input field is a blue button labeled "DALEJ". Underneath the button is a lock icon followed by the text "Pamiętaj o podstawowych zasadach bezpieczeństwa." Below this is a paragraph: "Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:" followed by three bullet points: "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", and "o certyfikat jest wystawiony dla Asseco Poland S.A. przez firmę DigiCert Inc". Below the bullet points is another paragraph: "Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników." At the bottom of the form area is a link: "Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa".

W polu „Numer identyfikacyjny” wpisujemy nazwę użytkownika nadaną przez Bank. W przypadku identyfikatora nie ma znaczenia wielkość wprowadzanych znaków. Po wciśnięciu przycisku „Dalej” zostaniemy przeniesieni na ekran wpisania kodu dostępu.

The screenshot shows a light blue header with a back arrow on the left and the word "LOGOWANIE" on the right. Below the header is a form with a label "Kod dostępu" and a text input field containing the placeholder "Wpisz hasło użytkownika i wskazanie tokena". Below the input field is a blue button labeled "ZALOGUJ". Underneath the button is a lock icon followed by the text "Pamiętaj o podstawowych zasadach bezpieczeństwa." Below this is a paragraph: "Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:" followed by three bullet points: "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", and "o certyfikat jest wystawiony dla Asseco Poland S.A. przez firmę DigiCert Inc". Below the bullet points is another paragraph: "Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników." At the bottom of the form area is a link: "Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa".


W polu „Kod dostępu”:
Podczas pierwszego logowania lub po resecie tokena wpisujemy aktualne wskazanie tokena.



W poniższym przykładzie kluczem będzie ciąg cyfr 159759.

Następnie system zażąda od użytkownika zdefiniowania nowego Hasła, które należy wpisać w polu "Nowy kod dostępu" oraz powtórzyć w polu „Powtórz nowy kod dostępu”. Po czym należy kliknąć przycisk „Zapisz i zaloguj”

←
Nowe hasło dostępu

 Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator użytkownika

Nowe hasło dostępu

Powtórz nowe hasło

Wpisz nowe hasło dostępu

Wpisz ponownie nowe hasło dostępu

ZAPISZ I ZALOGUJ

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

- musi składać się z 4-8 znaków

Uwaga! Hasło musi zawierać od 4 do 8 dowolnych znaków i nie może zaczyna się od cyfry „0”.

Następnie system prosi o podanie „wskazanie z tokena”.

←
Synchronizacja tokena

Wskazanie tokena

Wpisz kolejne wskazanie tokena

ZAPISZ I ZALOGUJ

Podajemy 6 cyfr z tokena pod warunkiem, że cyfry uległy zmianie.

Każde następne logowanie i autoryzacja przelewów odbywa się w taki sam sposób, tj. w polu kod dostępu wpisujemy zdefiniowane podczas pierwszego logowania hasło oraz aktualne wskazanie tokena.