

KLIENCI WYKORZYSTUJĄCY PO RAZ PIERWSZY APLIKACJĘ MOBILNĄ MTOKEN

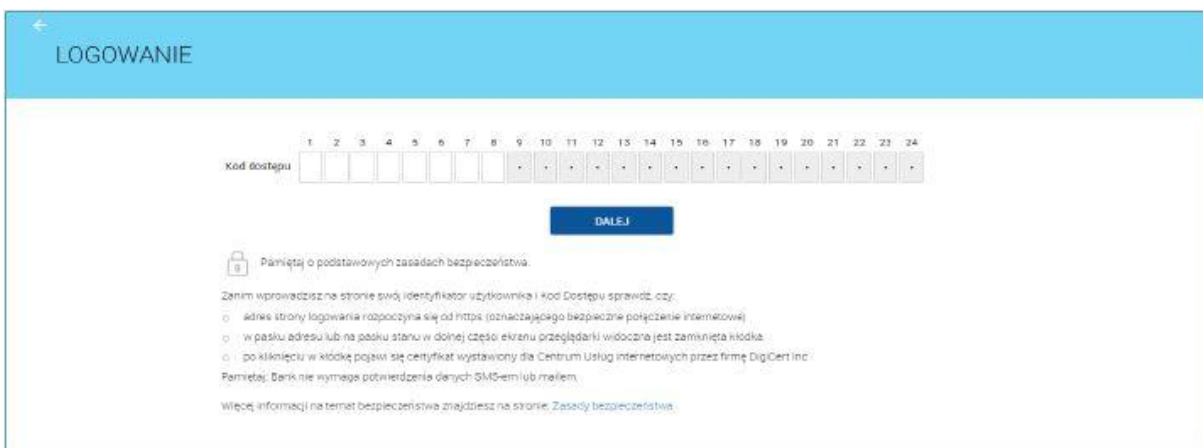
1. Zainstalować na smartfonie aplikację mobilną mToken Asseco MAA ze Sklepu Play.
2. Uruchomić stronę internetową Banku: www.bsnowe.com.pl.
3. Wybrać Bankowość Elektroniczną / Klienci detaliczni CBP.
4. Wpisać dziewięciodziesiętny nr ID otrzymany z Banku rozpoczynający się od NO.....



The screenshot shows the login page with a blue header containing the word "LOGOWANIE" and a language selector set to "PL". Below the header is a white form area. At the top of the form is a text input field labeled "Numer identyfikacyjny" (Identification number) with a placeholder "(nrpocz: numer)". Below the field is a blue button labeled "DALEJ". Underneath the button is a security notice: "Pamiętaj o podstawowych zasadach bezpieczeństwa." followed by a list of instructions: "Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdź, czy: - adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe) - w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka".

zrzut 1

5. Wpisać ośmioznakowe hasło otrzymane wiadomością SMS, które jest ważne przez 24 godziny.



The screenshot shows the login page with a blue header containing the word "LOGOWANIE" and a language selector set to "PL". Below the header is a white form area. At the top of the form is a password input field labeled "Kod dostępu" (Access code) with a placeholder "1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24". Below the field is a blue button labeled "DALEJ". Underneath the button is a security notice: "Pamiętaj o podstawowych zasadach bezpieczeństwa." followed by a list of instructions: "Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdź, czy: - adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe) - w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka - po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigCert Inc". At the bottom, there is a note: "Pamiętaj, Bank nie wymaga potwierdzenia danych SMS-em lub mail'em. Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa."

zrzut 2

6. Następnie pojawi się okno z informacją:
Do autoryzacji urządzenia wymagana jest aplikacja mToken Asseco MAA, kliknąć – POSIADAM APLIKACJĘ.
7. Wyświetli się sześciocyfrowy Kod aktywacyjny, który należy wpisać do aplikacji mobilnej mToken Asseco MAA.
8. Do aplikacji mobilnej wpisać kod SMS, który został wysłany po wpisaniu powyższego kodu aktywacyjnego.
9. Wpisać swój własny kod od 5 do 8 cyfr, który będzie służył do logowania do aplikacji mobilnej mToken oraz do podpisywania przelewów i autoryzacji innych zleceń.
10. Ponownie zalogować się do bankowości internetowej, podając nr ID - *zrzut 1*.
11. Wpisać ośmioznakowe hasło wcześniej otrzymane wiadomością SMS - *zrzut 2*.
12. Wpisać swoje własne indywidualne hasło, które będzie służyło do logowania do aplikacji, składające się od 10 do 24 znaków oraz spełniające podane wymagania.

zrzut 3

13. Podczas kolejnych logowań (po ustaleniu własnego hasła) najpierw należy wprowadzić nr ID a następnie wprowadzić tylko wybrane losowo przez system znaki z hasła.

zrzut 4

Na załączonym przykładzie hasło to **BsNowenadWisla12!#**, wprowadzamy wówczas : pole 1 – B, pole 2 – s, pole 3 – N, pole 4 – o, pole 5 – w, pole 14-a, pole 15-1, pole16-2.

14. Po wpisaniu hasła pojawi się poniższe okno:

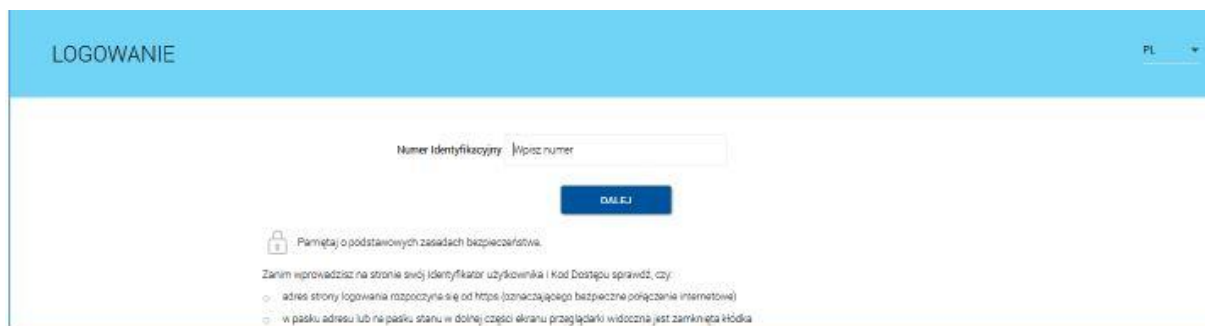
zrzut 5

15. Należy zalogować się do aplikacji mobilnej mToken Asseco MAA kodem ustalonym w pkt.9) i uwierzytelnić klikając „akceptuj” (ponownie wpisać kod).

KLIENCI WYKORZYSTUJĄCY PO RAZ PIERWSZY DO LOGOWANIA KOD SMS + PIN

LOGOWANIE

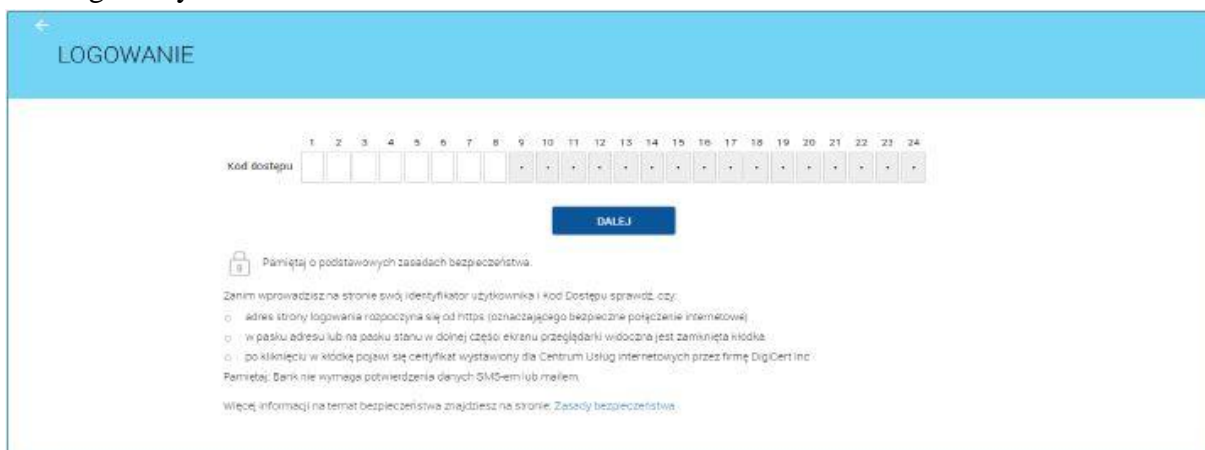
1. Uruchomić stronę internetową Banku: www.bsnowe.com.pl.
2. Wybrać Bankowość Elektroniczną / Klienci detaliczni CBP.
3. Wpisać dziewięćdziesięciocyfrowy nr ID otrzymany z Banku rozpoczynający się od NO.....



The screenshot shows the 'LOGOWANIE' (Login) page. At the top, there is a blue header with the word 'LOGOWANIE' and a language selector set to 'PL'. Below the header, there is a form with a label 'Numer identyfikacyjny / Idpocz numer' and a text input field. A blue button labeled 'DALEJ' (Next) is positioned below the input field. Underneath the button, there is a lock icon and the text 'Pamiętaj o podstawowych zasadach bezpieczeństwa.' (Remember the basic security rules). Below this, there is a small instruction: 'Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdź, czy:' (Before you enter your user ID and Access Code on the page, check if:). This is followed by three bullet points: 'o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)', 'o w pasku adresu lub w pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka', and 'o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę Digicert Inc.'. At the bottom, there is another line of text: 'Pamiętaj, Bank nie wymaga potwierdzenia danych SMS-em lub mailem.' (Remember, the Bank does not require confirmation of data via SMS or email.) and a link: 'Więcej informacji na temat bezpieczeństwa znajdziesz na stronie, Zasady bezpieczeństwa'.

zrzut 1

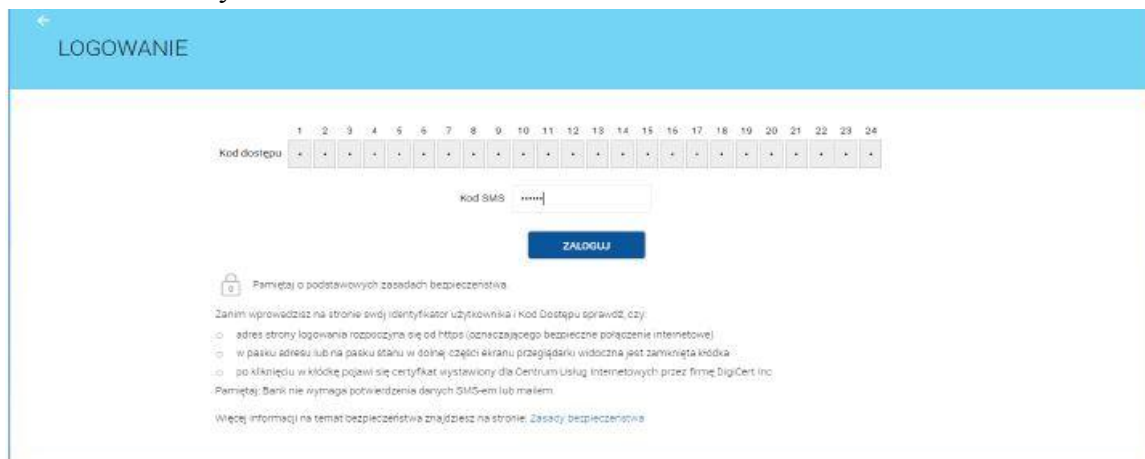
4. Wpisać ośmioznakowe hasło otrzymane wiadomością SMS, które jest ważne przez 24 godziny.



The screenshot shows the 'LOGOWANIE' (Login) page. At the top, there is a blue header with the word 'LOGOWANIE' and a language selector set to 'PL'. Below the header, there is a form with a label 'Kod dostępu' (Access Code) and a 24-digit PIN input field. A blue button labeled 'DALEJ' (Next) is positioned below the input field. Underneath the button, there is a lock icon and the text 'Pamiętaj o podstawowych zasadach bezpieczeństwa.' (Remember the basic security rules). Below this, there is a small instruction: 'Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdź, czy:' (Before you enter your user ID and Access Code on the page, check if:). This is followed by three bullet points: 'o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)', 'o w pasku adresu lub w pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka', and 'o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę Digicert Inc.'. At the bottom, there is another line of text: 'Pamiętaj, Bank nie wymaga potwierdzenia danych SMS-em lub mailem.' (Remember, the Bank does not require confirmation of data via SMS or email.) and a link: 'Więcej informacji na temat bezpieczeństwa znajdziesz na stronie, Zasady bezpieczeństwa'.

zrzut 2

5. Zatwierdzić tymczasowe hasło kodem SMS.



The screenshot shows the 'LOGOWANIE' (Login) page. At the top, there is a blue header with the word 'LOGOWANIE' and a language selector set to 'PL'. Below the header, there is a form with a label 'Kod dostępu' (Access Code) and a 24-digit PIN input field. A blue button labeled 'DALEJ' (Next) is positioned below the input field. Underneath the button, there is a lock icon and the text 'Pamiętaj o podstawowych zasadach bezpieczeństwa.' (Remember the basic security rules). Below this, there is a small instruction: 'Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdź, czy:' (Before you enter your user ID and Access Code on the page, check if:). This is followed by three bullet points: 'o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)', 'o w pasku adresu lub w pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka', and 'o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę Digicert Inc.'. At the bottom, there is another line of text: 'Pamiętaj, Bank nie wymaga potwierdzenia danych SMS-em lub mailem.' (Remember, the Bank does not require confirmation of data via SMS or email.) and a link: 'Więcej informacji na temat bezpieczeństwa znajdziesz na stronie, Zasady bezpieczeństwa'.

zrzut 3

6. Wpisać swoje własne indywidualne hasło, które będzie służyło do logowania do aplikacji, składające się od 10 do 24 znaków oraz spełniające podane wymagania.

zrzut 4

7. Zatwierdzić kodem otrzymanym wiadomością SMS.
8. Podczas kolejnych logowań (po ustaleniu własnego hasła) najpierw należy wprowadzić nr ID a następnie wprowadzić tylko wybrane losowo przez system znaki z hasła.

zrzut 5

Na załączonym przykładzie hasło to **BsNowenadWisla12!#**, wprowadzamy wówczas : pole 1 – B, pole 2 – s, pole 3 – N, pole 4 – o, pole 5 – w, pole 14-a, pole 15-1, pole16-2.

9. Zatwierdzić kodem otrzymanym wiadomością SMS.

AUTORYZACJA

1. Przy wykonywaniu przelewu po raz pierwszy, należy wpisać tymczasowy PIN autoryzacyjny otrzymany wiadomością SMS; uwaga jeśli minęły 72 godziny od jego otrzymania, prosimy o kontakt z Bankiem (tel. 52 33 28 507).
2. Wprowadzić nowy, indywidualny PIN autoryzacyjny składający się od 4 do 8 cyfr, potwierdzić wpisując ponownie.

← Przelew ZWYKŁY

Przelew z rachunku Rachunki Bieżące
84 8707 0006 0000 5666 2000 0001

Odbiorca Jan Testowy

Rachunek odbiorcy 02 1500 1894 0690 2900 3640 4254
KBSA O. w Chorzowie

Kwota 1,43 PLN

Tytułem tytuł testowy

Data realizacji dzisiaj
26.08.2019

⌵ Pokaż dodatkowe informacje

Wymagane zmianę pinu autoryzacyjnego

Prosimy pamiętać, że pin autoryzacyjny jest numerem poufnym. W związku z tym nie powinien być ujawniany osobom trzecim. Definiując swój pin autoryzacyjny pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa.
Pin Autoryzacyjny:
musi składać się z 4-8 znaków
musi się różnić od 3 ostatnich pinów

Obecny pin autoryzacyjny

Nowy pin autoryzacyjny

Powtórz nowy pin

ZATWIERDŹ

zrzut 6

3. Zatwierdzić kodem otrzymanym wiadomością SMS.
4. Kolejne autoryzacje będą wymagały wprowadzenia zdefiniowanego w pkt.2. PIN-u do podpisu oraz kodu SMS.