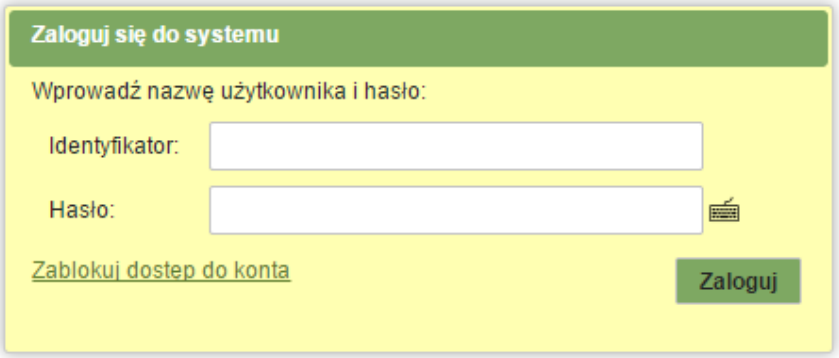
Pierwsze logowanie do systemu I-Bank

Rekomendacje Komisji Nadzoru Finansowego oraz Europejskiego Forum ds. Bezpieczeństwa Płatności Detalicznych zalecają, aby korzystanie z usług bankowych poprzez Internet poprzedzone było procedurą silnego uwierzytelnienia Klienta podczas logowania się do programu. W systemie I-Bank Klient może wybrać sposób uwierzytelnienia podczas logowania:

- **Słabe uwierzytelnienie podczas logowania –** wymaga podania tylko identyfikatora i hasła dostępu. Jest to wygodne dla Klienta, ale przy pomocy programów szpiegujących *(keylogery)* włamywacz może w łatwy sposób przechwycić parametry logowania. Jeśli słabe uwierzytelnienie jest stosowane, to bezwzględnie muszą być zastosowane dodatkowe zabezpieczenia, w szczególności:
  - program powinien być uruchamiany na dedykowanym do tego celu komputerze z ograniczonym dostępem do internetu w innych celach oraz z aktywną ochroną antywirusową,
  - jeśli na komputerze jest zainstalowany program pocztowy, to otrzymane załączniki należy otwierać z należytą ostrożnością,
  - dla konta Klienta powinna być włączona ochrona geolokalizacji, która pozwala na połączenia z Bankiem tylko z określonego adresu IP lub chociaż z określonego kraju (Polska).
  - Klient powinien być uwrażliwiony na wykrywanie sfałszowanych stron www Banku (phishing) i każdorazowo sprawdzać poprawność certyfikatu SSL strony Banku.
- **Silne uwierzytelnienie podczas logowania -** wymaga podania identyfikatora i hasła oraz – w zależności od wybranej metody - dodatkowo kodu SMS, który został przesłany na telefon komórkowy Klienta lub kodu PIN do klucza cyfrowego, który Klient podłączył na czas logowania do portu USB komputera.

1. Słabe uwierzytelnienie przy logowaniu

W celu uruchomienia systemu I-Bank w polu adresowym przeglądarki należy wpisać adres WWW strony Banku. Następnie na stronie Banku należy wybrać link do systemu I-Bank. Zostanie wówczas wyświetlony formularz logowania *(Rys. 1).*

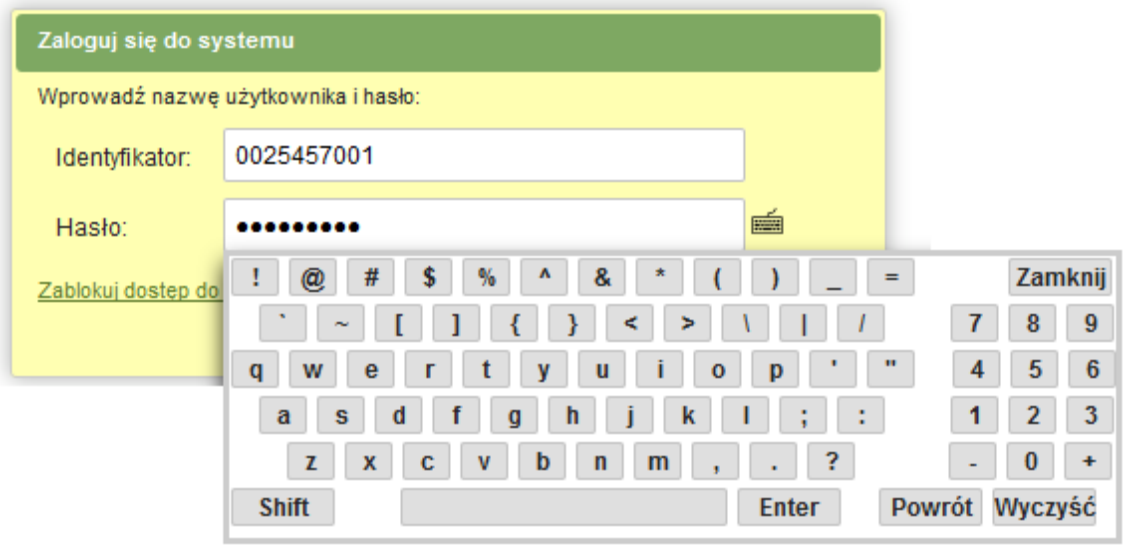


Rys. 1: Formularz logowania

Na formularzu należy wypełnić pola:

- **Identyfikator** – jest to identyfikator odczytany z karty rejestracyjnej Klienta otrzymanej z Banku.
- **Hasło** – hasło odczytane z karty rejestracyjnej Klienta. Podczas jego wpisywania zamiast liter będą wyświetlały się kropki. Jest to zabezpieczenie przed podejrzeniem hasła przez osoby postronne.

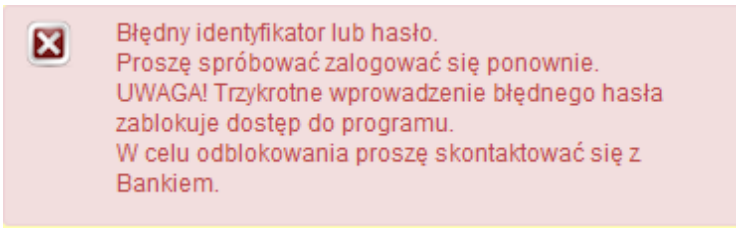
Przycisk ⌨ służy do wyświetlenia klawiatury ekranowej *(Rys. 2)*, za pomocą której zaleca się wpisać **Hasło**. Jest to zabezpieczenie przed programami typu *keylogger*, które rejestrują klawisze naciskane na klawiaturze komputera i mogą umożliwić nieuprawnione przechwycenie hasła.



Rys. 2: Klawiatura ekranowa

Po wypełnieniu formularza logowania należy go zatwierdzić przyciskiem Zaloguj.

W przypadku wprowadzenia błędnego identyfikatora lub hasła zostanie wyświetlony komunikat ostrzegawczy *(Rys. 3)*.



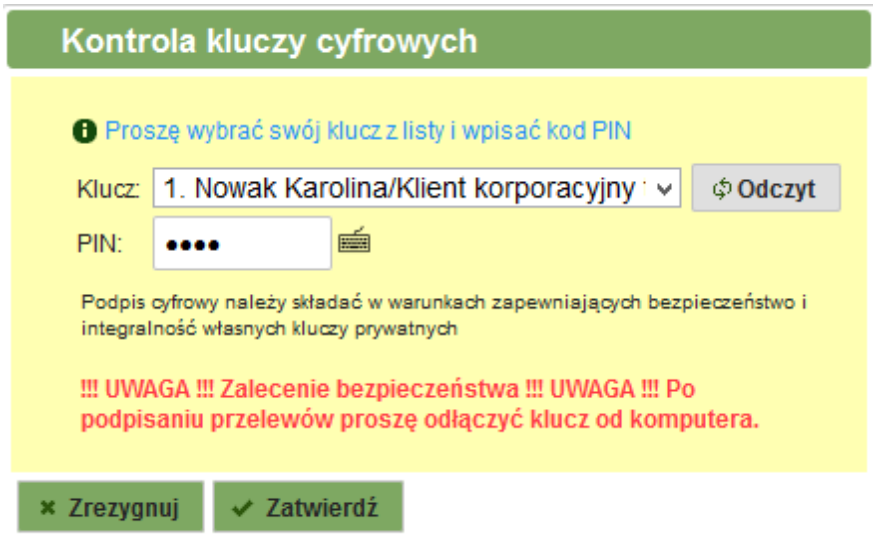
Rys. 3: Komunikat ostrzegawczy, wyświetlający się przy nieudanej próbie logowania

Uwaga!

Trzykrotne wprowadzenie błędnego hasła zablokuje dostęp do programu. Dostęp do programu może być odblokowany jedynie przez uprawnionego pracownika Banku.

2. Silne uwierzytelnienie przy logowaniu – klucz cyfrowy

Jeśli na koncie Klienta zostanie ustawiony wymóg silnego uwierzytelniania podczas logowania, to po uruchomieniu programu i wpisaniu identyfikatora i hasła pojawi się okno kontroli klucza cyfrowego (Rys. 4).



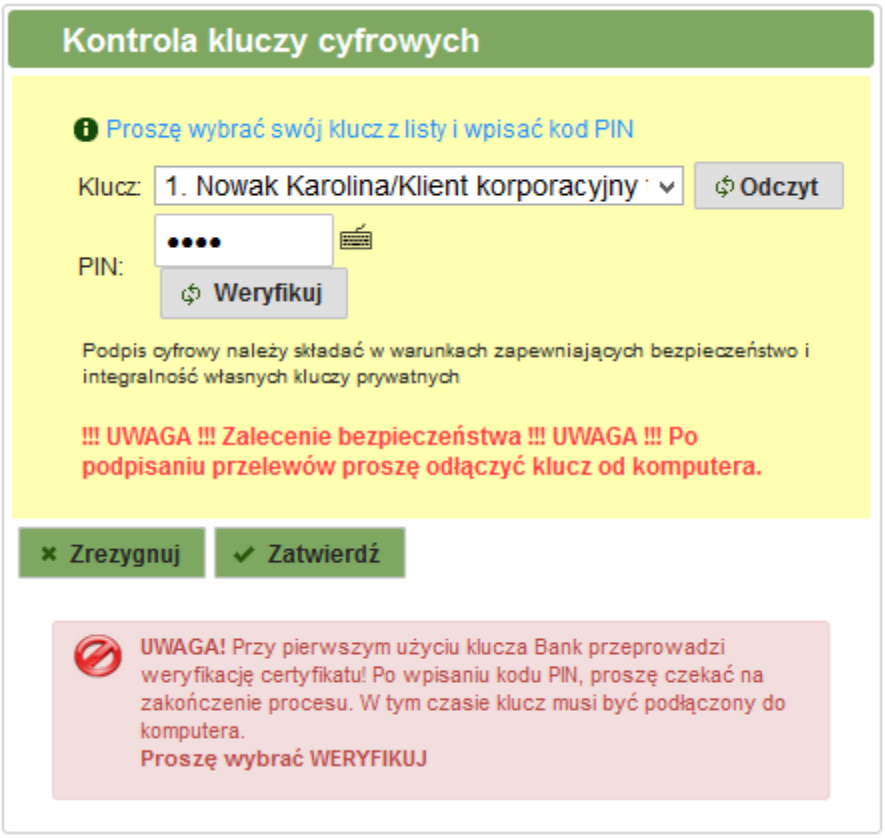
Rys. 4: Okno kontroli kluczy cyfrowych

Z listy dostępnych kluczy należy wybrać swój klucz, wprowadzić kod **PIN** (znajdujący się na karcie rejestracyjnej otrzymanej w Banku) oraz kliknąć przycisk Zatwierdź. Jeśli posiadany klucz nie będzie znajdował się na liście, należy odłączyć wszystkie pamięci typu Pendrive z portów USB, upewnić się czy nasz klucz jest włożony poprawnie i wcisnąć przycisk Odczyt.

Przy wprowadzaniu kodu PIN zaleca się korzystanie z klawiatury ekranowej uruchamianej przyciskiem . Jest to zabezpieczenie przed programami typu *keylogger*, które rejestrują klawisze naciskane na klawiaturze komputera i mogą umożliwić nieuprawnione przechwycenie kodu PIN.

Podczas pierwszego logowania do systemu zostanie przeprowadzona także weryfikacja klucza (Rys. 5).

Po wpisaniu kodu PIN należy wybrać opcję Weryfikuj i poczekać na zakończenie procesu. Po pomyślnej weryfikacji należy zakończyć proces przyciskiem Zatwierdź.

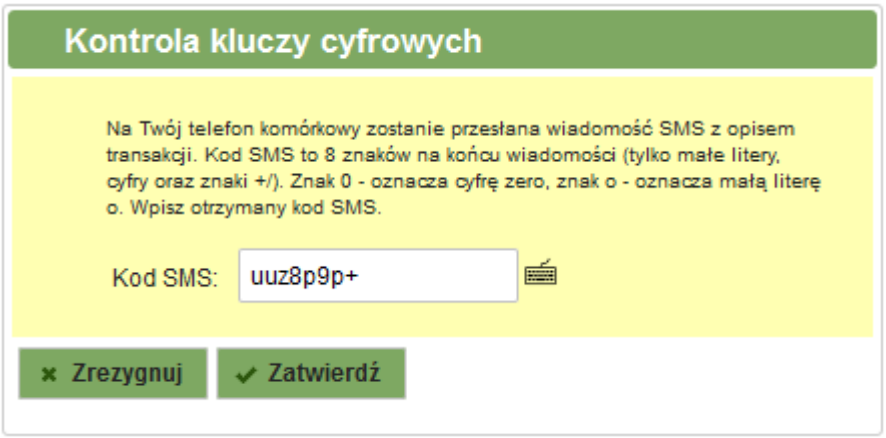


Rys. 5: Okno kontroli kluczy cyfrowych przy pierwszym logowaniu wymagające weryfikacji klucza

Uwaga! W czasie weryfikacji nie należy wyciągać klucza z portu USB, ponieważ może to spowodować jego blokadę. Zablokowany klucz należy dostarczyć do Banku w celu ponownej aktywacji.

3. Silne uwierzytelnienie przy logowaniu – kod SMS

Jeśli na koncie Klienta zostanie ustawiony wymóg silnego uwierzytelniania podczas logowania, to po uruchomieniu programu i wpisaniu identyfikatora oraz hasła pojawi się okno kontroli klucza cyfrowego (Rys. 6), w którym należy wpisać kod odczytany z wiadomości SMS przesłanej przez Bank na telefon Klienta.



Rys. 6: Okno kontroli kluczy cyfrowych

4. Zmiana hasła po pierwszym logowaniu

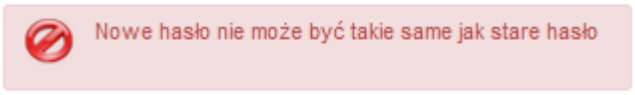
Na otrzymanej z Banku karcie rejestracji znajduje się hasło dostępu do programu. Jest to hasło startowe, które powinno być zmienione podczas pierwszego logowania. Na ekranie pojawi się formularz (Rys. 7), w którym należy wypełnić pola:

- **Nowe hasło**,
- **Powtórz nowe hasło.**

Rys. 7: Formularz zmiany hasła

Przy wpisywaniu haseł należy zwrócić uwagę na to, że program zapamiętuje wielkość wpisywanych liter. Wymagana długość hasła oraz zestaw dopuszczalnych znaków zależy od polityki

bezpieczeństwa stosowanej w Banku. Użycie znaku niedozwolonego i inne błędy są sygnalizowane komunikatem, np.:



Rys. 8: Komunikat błędu wyświetlany podczas zmiany hasła

Zatwierdzenie zmiany hasła odbywa się poprzez wciśnięcie przycisku 

.

Po wprowadzeniu i zatwierdzeniu nowego hasła nastąpi ponowne przekierowanie do okna logowania.

W przypadku problemów prosimy o kontakt z Bankiem pod numerem telefonu: +48 32 43 42 725