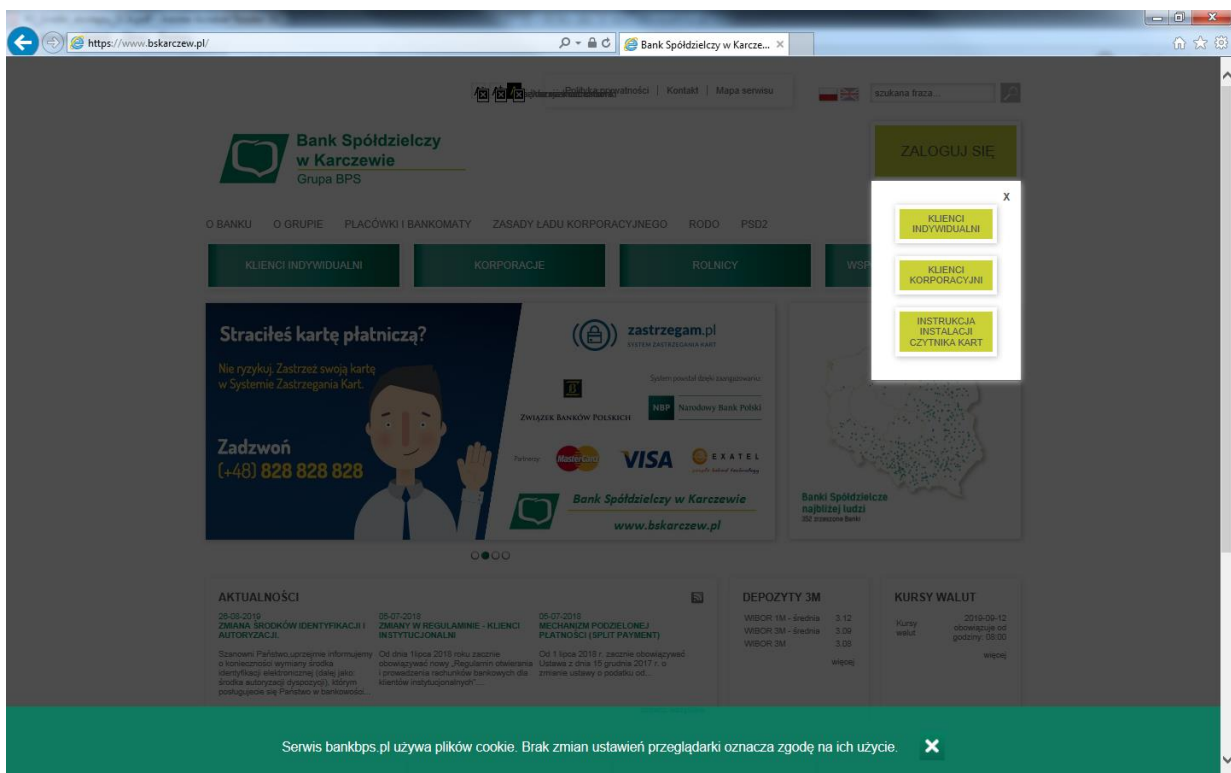


Stosowane środki dostępu do bankowości elektronicznej zostały uzupełnione o dodatkowe wymagania SCA (tzw. silne uwierzytelnianie klienta) – oznacza to uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych. Bank Spółdzielczy w Karczewie dostosował środki dostępu do systemu bankowości elektronicznej do wymogów SCA w procesie autentykacji (logowania) oraz autoryzacji (podpisu).

Opis procesu logowania kartą mikroprocesorową (dla wszystkich klientów posiadających kartę mikroprocesorową wraz z czytnikiem kart):

1. Na stronie głównej Banku Spółdzielczego w Karczewie <https://www.bskarczew.pl/> należy wybrać przycisk ZALOGUJ SIĘ a następnie KLIENCI KORPORACYJNI



2. W polu wyboru „Logowanie” należy wybrać opcję „Logowanie kartą mikroprocesorową” a następnie w polu „PIN” należy wpisać kod PIN dostarczony wraz z kartą mikroprocesorową przez Bank

UWAGA!

Podczas logowania przy użyciu karty mikroprocesorowej klient nie podaje identyfikatora, jednakże jest on ważnym składnikiem procesu autentykacji i może być wymagany przez pracowników Banku podczas zgłaszania wniosków dotyczących zmian konfiguracyjnych klienta lub obsługi w zakresie bankowości elektronicznej



Jeżeli zauważysz nietypowy wygląd strony do logowania, poinformuj bank o takiej sytuacji.

Zawsze weryfikuj czy numer rachunku (NRB) podpisywanego i przekazywanego do realizacji przelewu jest prawidłowy!

Bank nie prosi o podanie PIN-u do karty podczas logowania.

Autoryzacja

Proszę wprowadzić PIN
oraz nacisnąć przycisk "Zatwierdź".

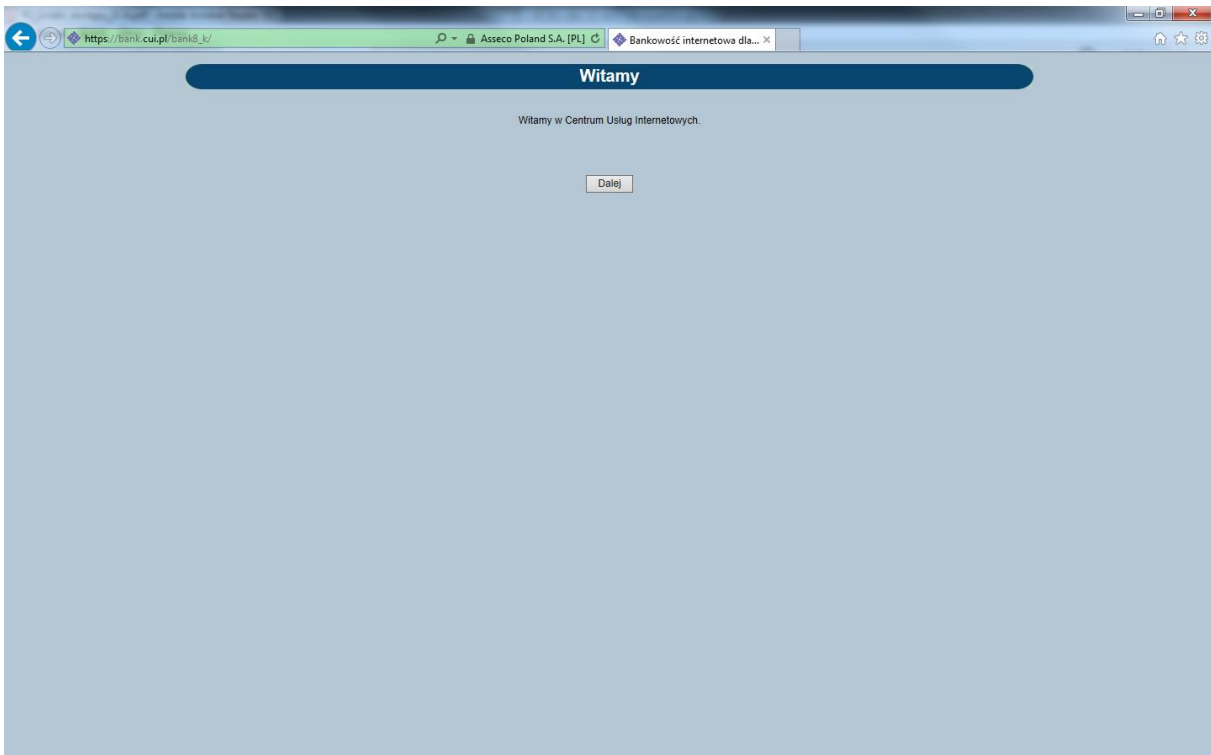
Logowanie:

PIN:

PRZYPOMINAMY O ZASADACH BEZPIECZNEGO KORZYSTANIA Z BANKOWOŚCI ELEKTRONICZNEJ

1. Zabezpiecz komputer aktualnym oprogramowaniem antywirusowym oraz zaporą (firewall)
2. Regularnie aktualizuj system operacyjny, wersję przeglądarki oraz oprogramowanie na stacji roboczej korzystającej z bankowości elektronicznej
3. Nie otwieraj strony bankowości elektronicznej poprzez link z e-maila i nie instaluj oprogramowania z nieznanego źródła. Przesłany w ten sposób mogą próbować przejąć kontrolę nad Twoim urządzeniem (komputer, tablet, smartfon)
4. Sprawdź czy w pasku przeglądarki znajduje się symbol "zatrzęsniętej kłódki", który gwarantuje szyfrowanie sesji. W zależności od przeglądarki, ikona kłódki może się pojawić w pasku adresu lub w pasku stanu w dolnej części ekranu
5. Zweryfikuj czy certyfikat strony wystawiony jest dla Asseco Poland S.A. przez firmę DigiCert Inc (kliknięcie na "zatrzęsniętą kłódkę" w pasku przeglądarki)
6. Po zakończeniu pracy w bankowości elektronicznej wyloguj się używając przeznaczonej do tego opcji w aplikacji, gwarantuje to poprawne zamknięcie sesji przez użytkownika
7. Chron dane dostępne do bankowości elektronicznej
8. Nie loguj się i nie dokonuj płatności w punktach bezpłatnego publicznego dostępu do Internetu - w tzw. hotspotach
9. Sprawdź poprawność numeru NRB przed i po podpisie przelewu
10. Zwróć szczególną uwagę na poprawność numeru NRB po wklejeniu go ze schowka systemu. Najlepiej zrezygnuj z kopiowania NRB
11. Aby zmniejszyć możliwość ataku upewnij się, że baza wirusów programu antywirusowego jest aktualna i zainstaluj dwustronny firewall na komputerze
12. Karta mikroprocesorowa używana do podpisu zleceń musi zostać usunięta z czytnika po zakończeniu procesu

3. Po naciśnięciu przycisku „Zatwierdź” aplikacja poinformuje o wyniku autentykacji



Witamy

Witamy w Centrum Usług Internetowych.