

PSD2 – logowanie z dniem 14.09.2019 r.

Zgodnie z unijną dyrektywą „PSD2” z dniem 14 września 2019 r. wycofujemy możliwość dostępu i autoryzacji transakcji z wykorzystaniem Tokenów RSA. Po tym terminie możliwa będzie autoryzacja transakcji przy pomocy SMS-a. Będzie to oznaczało zablokowanie dostępu do bankowości elektronicznej przy użyciu tokena RSA.

Środki dostępu w bankowości będą dostosowane do SCA (tzw.: „silne uwierzytelnienie klienta”). „Silne uwierzytelnianie klienta” oznacza 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, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających. Dostosowanie do wymogów wynikających z zapisów dyrektywy PSD2 dotyczy zarówno procesu logowania - autentykacji i autoryzacji - podpisu.

Spis treści

BANKOWOŚĆ DETALICZNA (https://bsskepe.cui.pl)	2
Proces logowania	2
Proces autoryzacji (podpisu)	3
BANKOWOŚĆ KORPORACYJNA (https://bank.cui.pl/skepe_k)	4
Proces logowania:	4
Proces autoryzacji:	4

BANKOWOŚĆ DETALICZNA (<https://bsskepe.cui.pl>)

Proces logowania

Wprowadzenie identyfikatora użytkownika:

LOGOWANIE PL

Numer identyfikacyjny

DALEJ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

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.

Wprowadzenie hasła maskowanego:

LOGOWANIE

Kod dostępu

DALEJ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

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 DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

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

Wprowadzenie kodu SMS:

LOGOWANIE

Kod dostępu

Kod SMS

ZALOGUJ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

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 DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

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

Proces autoryzacji (podpisu)

Pierwsza autoryzacja będzie poprzedzona wysłaniem poprzez SMS jednorazowego numeru PIN wraz z wymuszeniem jego zmiany:

← Przelew ZWYKŁY ×

Przelew z rachunku	Rachunki Bieżące 84 8707 0006 0000 5656 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

Wymagana zmiana 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-znaków
musi się różnić od 3 ostatnich pinów

Obecny pin autoryzacyjny	<input type="text" value="Wpisz obecny pin"/>
Nowy pin autoryzacyjny	<input type="text" value="Wpisz nowy pin"/>
Powtórz nowy pin	<input type="text" value="Powtórz nowy pin"/>

ZATWIERDŹ

Kolejne autoryzacje będą wymagały wprowadzenia zdefiniowanego wcześniej PIN-u do podpisu oraz kodu SMS:

← Przelew ZWYKŁY ×

Przelew z rachunku	Rachunki Bieżące 84 8707 0006 0000 5656 2000 0001
Odbiorca	ODBIORCA SKROCONY PEŁNY
Rachunek odbiorcy	94 1020 1505 0000 0802 0011 2714 PKOBP
Kwota	1,00 PLN
Tytułem	TYTUŁ PŁATNOŚCI
Data realizacji	dzisiaj 26.08.2019

↓ Pokaż dodatkowe informacje

Pin autoryzacyjny oraz kod SMS

<input type="text" value="Wpisz pin"/>
<input type="text" value="Wpisz kod"/>

Operacja nr 738167 z dnia 26.08.2019

AKCEPTUJ

BANKOWOŚĆ KORPORACYJNA (https://bank.cui.pl/skepe_k)

1. Proces logowania - autentykacji

Obecnie stosowane hasło stałe zostanie zastąpione kartą mikroprocesorową i numerem PIN.

2. Proces autoryzacji - podpisu

Autoryzacja za pomocą karty mikroprocesorowej + numer PIN

Proces logowania:

Wybór metody autentykacji – Logowanie karta mikroprocesorową:



Autoryzacja

Proszę wprowadzić PIN oraz nacisnąć przycisk "Zatwierdź".

Logowanie: **Logowanie kartą mikroprocesorową**

PIN:

Zatwierdź

Umieszczenie karty mikroprocesorowej w czytniku i wprowadzenie numeru PIN karty mikroprocesorowej:



Autoryzacja

Proszę wprowadzić PIN oraz nacisnąć przycisk "Zatwierdź".

Logowanie: **Logowanie kartą mikroprocesorową**

PIN: ****

Zatwierdź

Proces autoryzacji:

Umieszczenie karty mikroprocesorowej w czytniku i wprowadzenie numeru PIN karty mikroprocesorowej:



Przelew - akceptowanie

Referencje:	
Rachunek do obciążenia:	40 8818 0009 3001 0000 0123 0002 Rachunek pomocniczy
Nazwa kontrahenta:	Test Przelewów
Nr rachunku kontrahenta:	87 9484 1017 1600 0224 2590 0001
Tytułem:	Szablon
Przelew VAT:	Nie
Kwota:	10,00 PLN
Droga płatności:	Elixir
Data:	2019-07-09
Zleceniodawca:	bankowy jan

PIN Podpisz

Zamknij

Log:
2019-07-09 13:00 Nowy przelew - DSL2 2

O wszelkich zmianach będziemy Państwa informować na bieżąco.