Przewodnik dla klienta

Instrukcja użytkowania bankowości internetowej (I-Bank)

1. Wstęp

Pragniemy zaoferować Państwu jedną z unikalnych, a zarazem bardzo bezpiecznych usług dostępu do rachunku Bankowego przez Internet.
Użytkownik Systemu I-Bank będzie mógł przeprowadzać przez Internet takie operacje jak:
sprawdzenie stanu rachunków, drukowanie wyciągów, realizacja przelewów (ELIXIR, Ekspresowy Bluecash, ZUS, US,), założenie zlecenia stałego, założenie i zerwanie lokaty, a nawet doładowanie konta telefonu komórkowego.
Korzystanie z systemu jest bardzo łatwe i bezpieczne, możliwe z dowolnego miejsca na świecie, dostępne przez całą dobę i cały rok. Jedynym warunkiem korzystania z Systemu jest posiadanie komputera wyposażonego w przeglądarkę stron WWW, system JAVA w wersji 7 minimum update 9 i dostęp do Internetu.
Warto podkreślić, że w projektowaniu i budowie Systemu wykorzystano najnowszą wiedzę i technologię zabezpieczeń przed ewentualnymi próbami włamania. Z usług Bankowych za pośrednictwem Internetu mogą korzystać tylko klienci zarejestrowani w systemie I-Bank.

Rejestrację przeprowadzi uprawniony pracownik Banku.

2. Zasady bezpiecznego korzystania z Systemu Bankowości Elektronicznej

Po pierwsze bezpieczeństwo!

Przy projektowaniu i budowie Systemu wykorzystano najnowsze rozwiązania, które zapewniają nie tylko wygodę i oszczędności ale i bezpieczeństwo.
System bezpieczeństwa tworzymy wspólnie z Państwem. Poniżej wskazujemy elementy tego systemu gwarantowane przez Bank, w dalszej części rozdziału przedstawiamy katalog zasad bezpieczeństwa – zalecenia do stosowania przez Użytkowników usługi.

Szyfrowa transmisja danych

Stosujemy szyfrowane automatyczne zabezpieczenie protokołem Secure Socket Layer (SSL) wykorzystującym klucz o długości 256 bitów. Zapewnia on poufność informacji i gwarantuje, że nikt postronny nie może odczytać lub zmienić danych przesyłanych między Klientem a Bankiem. Zastosowanie tej metody zapewnia całkowitą poufność operacji finansowych. W czasie korzystania z bezpiecznego protokołu adres strony internetowej zaczyna się od https://.

Uwierzytelnienie

Uwierzytelnienie, czyli sprawdzenie tożsamości użytkownika i jego prawa dostępu do konta za pomocą elektronicznych kanałów dostępu. Oparte jest na czymś CO ZNASZ (identyfikator i hasło, PIN, kod SMS) oraz na tym CO MASZ (klucz sprzętowy, Kod SMS).

Rejestracja aktywności
Ze względów bezpieczeństwa wszelkie ślady aktywności na koncie są rejestrowane.

Automatyczne wylogowanie
Dodatkowym zabezpieczeniem jest automatyczne wylogowanie Użytkownika z usługi w sytuacji stwierdzenia braku jego aktywności na koncie. W takim przypadku wystarczy zamknąć i ponownie uruchomić przeglądarkę oraz ponownie zalogować się.

Blokada konta
W przypadku trzech błędnych prób zalogowania się do Systemu Bankowości Elektronicznej I-BANK następuje automatyczna blokada konta danego Użytkownika, która chroni konto przed dostępem osób nieupoważnionych.

W przypadku gdy konieczne jest zablokowanie dostępu do konta (np. utracono środki identyfikacji elektronicznej) użytkownik może samodzielnie zablokować dostęp do konta. W tym celu należy na stronie logowania do systemu skorzystać z opcji „zablokuj dostęp do konta" i wykonać kolejne zalecenia systemu.

W celu odblokowania konta należy skontaktować się z bankiem pod numerami telefonów Centrala Krosno Odrzańskie tel. 683835192/ Oddział Łagów Lubuski 683412016/ Oddział Torzym 683413047 (w godzinach pracy Banku). Odblokowanie konta może wiązać się z potrzebą osobistej wizyty w placówce Banku.

Zastrzeżenie środków dostępu
W przypadku zagubienia, kradzieży klucza sprzętowego, kodów dostępu, a także utraty telefonu komórkowego należy dokonać natychmiastowej blokady konta poprzez skorzystanie z opcji „zablokuj dostęp do konta" na stronie logowania do bankowości elektronicznej lub przez kilkukrotne (minimum 4) wpisanie nieprawidłowego hasła podczas logowania oraz niezwłocznie zgłosić ich zastrzeżenie w dni robocze w godzinach pracy Banku telefonicznie pod numerami Centrala Krosno Odrzańskie tel. 683835192/ Oddział Łagów Lubuski 683412016/ Oddział Torzym 683413047
Należy również pamiętać, by w przypadku zmiany numeru telefonu, na które przesyłane są Hasła jednorazowe SMS, zgłosić ten fakt do Banku.

Zasady ustanawiania haseł

Składa się z minimum 8 znaków (minimum jedna cyfra i litery małe i duże, znaki specjalne)
Nie należy stosować polskich znaków diakrytycznych (np. . ą, ć, ę, ł, ń, ś, ó, ż, ź)

Zasady ustawiania kodu PIN

Składa się z minimum 4 do maksimum 8 znaków (minimum jedna cyfra i litery małe i duże, znaki specjalne)
Nie należy stosować polskich znaków diakrytycznych (np. . ą, ć, ę, ł, ń, ś, ó, ż, ź)

Logowanie do Systemu Bankowości Elektronicznej – WWW

Do obsługi pełnej funkcjonalności aplikacji zalecane jest korzystanie z jednej z wymienionych przeglądarek (w wersjach minimalnych bądź wyższych):
• Microsoft Edge
• Mozilla Firefox
• Google Chrome

Systematycznie należy czyścić cache przeglądarki:
• Tymczasowe pliki internetowe
• Pliki Cookie

Podczas wprowadzania identyfikatora i hasła nie wolno zezwalać na zapamiętywanie haseł przez przeglądarkę

Nigdy nie należy używać wyszukiwarek do znalezienia strony logowania Banku. Należy samodzielnie wprowadzać jej adres lub logować się bezpośrednio ze strony Systemu Bankowości Elektronicznej IBANK www.bskrosno.pl

Nigdy nie należy logować się przez adres lub link przysłany w wiadomości przez inną osobę nawet jeśli adres strony jest prawidłowy może prowadzić do fałszywych witryn

Przed zalogowaniem się na konto należy sprawdzić, czy połączenie z Bankiem jest szyfrowane. Adres strony musi zaczynać się od https://, natomiast na stronie internetowej musi być widoczny symbol zamkniętej kłódki.
By sprawdzić, czy strona jest autentyczna można kliknąć na kłódkę, aby zobaczyć, czy certyfikat cyfrowy został wydany na Bank oraz czy jest wystawiony z aktualną datą wystawienia

Jeśli symbol kłódki jest niewidoczny lub certyfikat jest nieprawidłowo wystawiony należy przerwać logowanie i niezwłocznie skontaktować się z Bankiem

Jeśli przy logowaniu pojawi się nietypowy komunikat lub prośba o podanie danych osobowych lub haseł lub ich aktualizację należy przerwać logowanie i skontaktować się niezwłocznie z Bankiem

Podczas logowania wpisuje się identyfikator i hasło (w przypadku autoryzacji kluczem sprzętowym dodatkowo klucz PIN). Należy pamiętać, iż Bank podczas logowania i użytkowania systemu nigdy nie prosi Klienta o udzielanie informacji na temat danych osobowych, haseł, PIN-ów, numerów lub modeli telefonów. Jeżeli podczas logowania nastąpi prośba o podanie którychkolwiek z tych danych, należy taką stronę niezwłocznie opuścić i powiadomić Bank.

Jeśli zauważą Państwo jakąkolwiek nieprawidłowość pod czas logowania lub wystąpią problemy techniczne związane z obsługą aplikacji należy skontaktować się niezwłocznie z Bankiem pod numerem Centrala Krosno Odrzańskie tel. 683835192/ Oddział Łagów Lubuski 683412016/ Oddział Torzym 683413047

Korzystanie Systemu Bankowości Elektronicznej - WWW

- Po zalogowaniu się do Systemu nie należy zostawiać komputera bez opieki
- Korzystając z Systemu powinno się używać tylko jednego okna przeglądarki internetowej, natomiast kończyć pracę należy poprzez użycie polecenia Koniec Pracy
- Należy co jakiś czas zmieniać hasła stałe i chronić je przed osobami trzecimi, proponujemy zmianę hasła co miesiąc.
- Podczas korzystania z Systemu nie należy używać klawiszy nawigacyjnych przeglądarki internetowej (np. Wstecz, Dalej, Odśwież), system posiada własne klawisze, które umożliwiają sprawne poruszanie się w ramach strony .
- Jeżeli połączenie z serwisem transakcyjnym zostanie zerwane, należy ponownie zalogować się i sprawdzić, czy system zapamiętał ostatnie zlecenie
- Należy stosować legalne i często aktualizowane oprogramowanie antywirusowe
- Należy używać aplikacji typu firewall i systemu wykrywania intruzów - blokujących niepożądane połączenia komputera z Internetem.
- Nie należy korzystać z Systemu Bankowości Elektronicznej I-Bank w miejscach ogólnie dostępnych np. kawiarenkach internetowych, publiczne hot spoty.

Korzystanie z Systemu Bankowości Elektronicznej – Informacja SMS

- Nigdy nie należy wysyłać wiadomości SMS zawierających kody dostępu (Identyfikator ID, hasło, PIN) na żadne numery telefonów. Bank nie prosi o takie informacje.

3. System Bankowości Elektronicznej IBANK – WWW

W celu poprawnego działania Systemu Bankowości Elektronicznej I-BANK sprzęt komputerowy Posiadacza powinien spełniać następujące wymagania:
1) jeden z systemów: Linux, macOS, Windows 10 lub kolejne nowsze wersje,
2) dostęp do sieci Internet,
3) przeglądarkę internetowa,
4) złącze USB w przypadku korzystania z autoryzacji kluczem sprzętowym lub telefon komórkowy z numerem operatora krajowego w przypadku autoryzacji kodem SMS.

Po podpisaniu Umowy Bankowości Elektronicznej Klient otrzymuje z Banku:
I.
W przypadku autoryzacji z wykorzystaniem klucza sprzętowego:

1) klucz sprzętowy USB, zawierający certyfikat (elektroniczny podpis Klienta). Certyfikat zawarty na kluczu sprzętowym jest rejestrowany na okres dwóch lat. Po tym okresie należy zgłosić się do Banku w celu ponownego utworzenia certyfikatu. Za odnowienie certyfikatu pobierana jest opłata zgodna z obowiązującą Taryfą opłat i prowizji.

2) kartę rejestracyjną, która zawiera:
   a) modulo - numer Bankowy jednoznacznie identyfikujący klienta
   b) identyfikator - unikalny numer dysponenta rachunku
   c) hasło - hasło jednorazowe umożliwiające pierwsze zalogowanie się do systemu I-Bank. Klient może być zobowiązany do zmiany hasła.
   d) PIN - kod PIN do autoryzacji przelewów i logowania

II.
W przypadku autoryzacji z wykorzystaniem kodu SMS:

1) kartę rejestracyjną, która zawiera:
   a) modulo - numer Bankowy jednoznacznie identyfikujący klienta
   b) identyfikator - unikalny numer dysponenta rachunku
   c) hasło - hasło jednorazowe umożliwiające pierwsze zalogowanie się do systemu I-Bank. Klient może być zobowiązany do zmiany hasła.
2) Dodatkowo, w Systemie zostanie zarejestrowany certyfikat z numer telefonu komórkowego klienta, na który będą przesyłane kody SMS. Po wystawieniu zlecenia System wyliczy z jego treści kod SMS i prześle go na wskazany numer telefonu. Klient zobowiązany jest przepisać odczytany kod na formularz zlecenia. Certyfikat z numerem telefonu klienta jest rejestrowany na okres trzech lat. Po tym okresie należy zgłosić w Banku potrzebę ponownej rejestracji certyfikatu z numeru telefonu (osobiście, telefonicznie). Oprócz tego na leży zgłosić do Banku każdy przypadek zmiany numeru telefonu. Za odnowienie certyfikatu pobierana jest opłata zgodna z obowiązującą Taryfą opłat i prowizji.

System I-Bank w wersji z kodami SMS obsługuje zarówno klientów indywidualnych jak i instytucjonalnych jak również JST.

Różnice w systemach operacyjnych i konfiguracji komputerów mogą być przyczyną tego, że wygląd okien, komunikatów oraz kolejność ich wyświetlania przez Państwa komputer - mogą różnić się od podanych w instrukcji. Instrukcja ma charakter poglądowy i jej zadaniem jest zobrazowanie standardowego przebiegu aktywacji systemu I-Bank oraz rozwiązanie podstawowych trudności lub wątpliwości

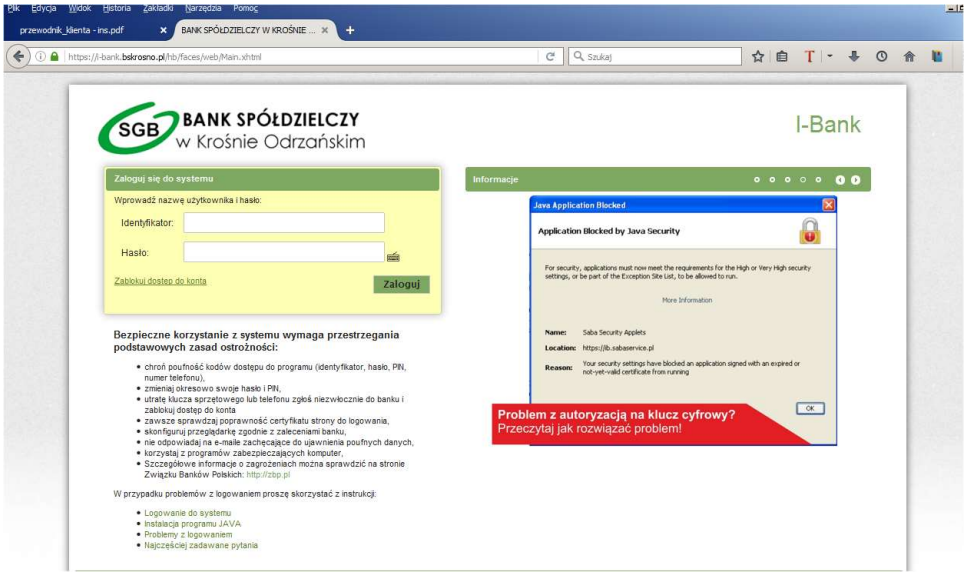
3.1 Instalacja programu wtyczki Saba Seciurity Plugin w systemie operacyjnym dla użytkowników przeglądarek Microsoft Edge, Mozilla Firefox lub Google Chrom

Jeżeli Klient korzysta z autoryzacji kodem SMS instalacja wtyczek Saba Seciurity Plugin nie jest wymagana

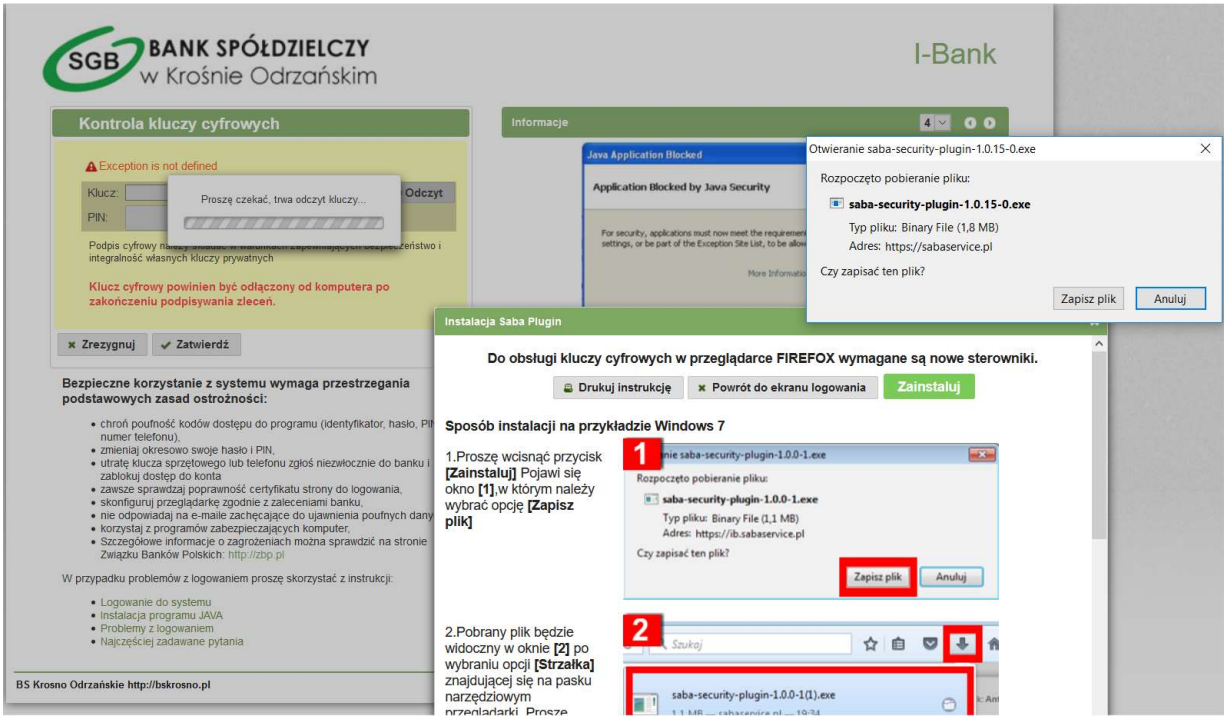
Przy autoryzacji kluczem sprzętowym USB prawidłowe działanie oprogramowania I-Bank wymaga, by na komputerze klienta Banku było zainstalowane oprogramowanie Saba Seciurity Plugin.

3.2 Pierwsze uruchomienie aplikacji

3.2.1 klienci korzystający z autoryzacji kluczem USB i PIN

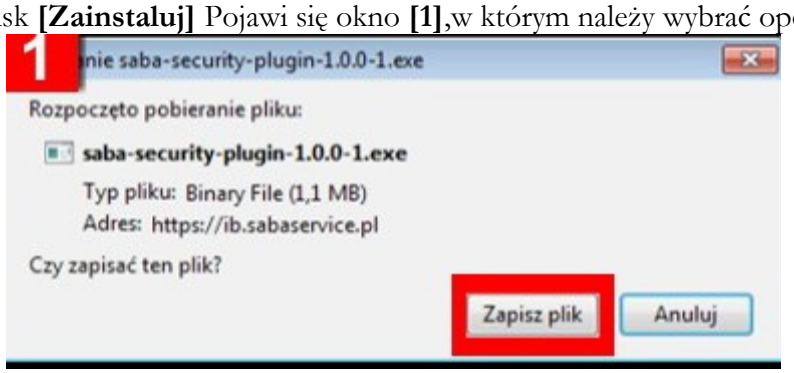


Przy pierwszym logowaniu po wpisaniu identyfikatora i hasła w przeglądarkach należy zainstalować dodatkowe sterowniki obsługi kluczy cyfrowych (patrz rysunek poniżej)

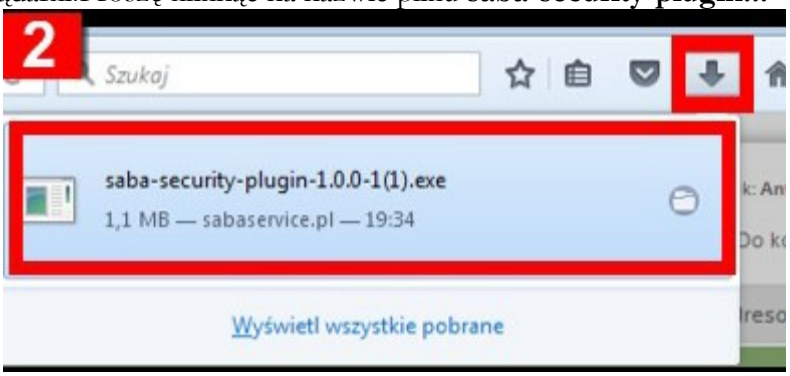


Instalację sterowników należy przeprowadzić zgodnie z wyświetlającą się informacją.

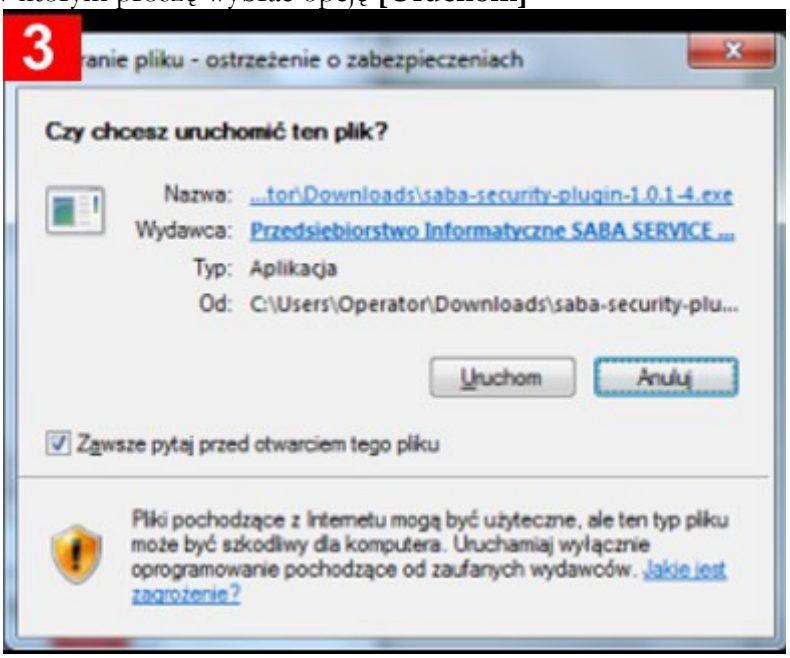
1. Proszę wcisnąć przycisk **[Zainstaluj]** Pojawi się okno **[1]**,w którym należy wybrać opcję **[Zapisz plik]**



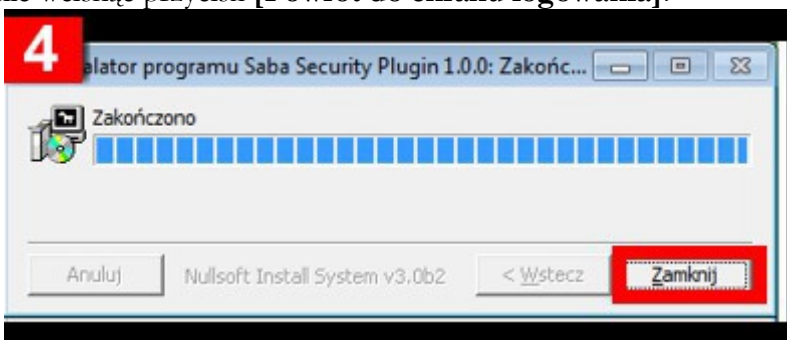
2. Pobrany plik będzie widoczny w oknie **[2]** po wybraniu opcji **[Strzałka]** znajdującej się na pasku narzędziowym przeglądarki.Proszę kliknąć na nazwie pliku **saba-security-plugin...**



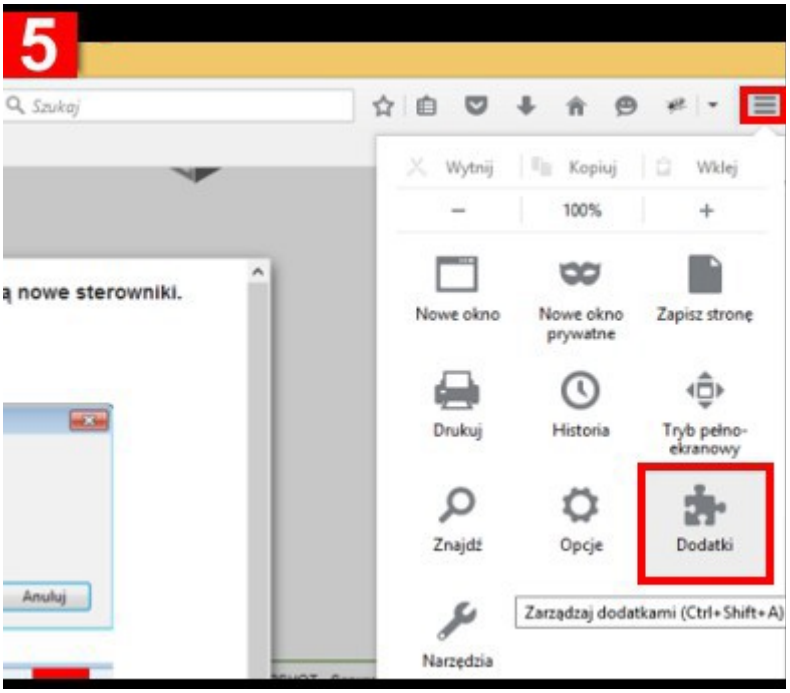
3. Pojawi się okno **[3]**, w którym proszę wybrać opcję **[Uruchom]**



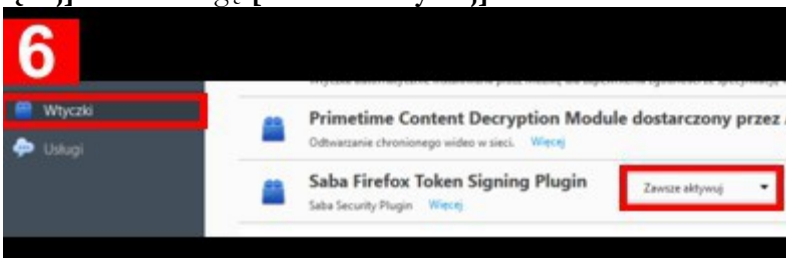
4. Postęp instalacji pliku widoczny jest w oknie **[4]**. Po zakończeniu instalacji proszę wybrać opcję **[Zamknij]**, a następnie wcisnąć przycisk **[Powrót do ekranu logowania]**.



5. Jeśli po instalacji sterowników wyświetli się ta instrukcja to proszę otworzyć Menu przeglądarki - widoczne w oknie **[5]** (kliknąć na trzy poziome kreski w prawym górnym rogu) i wybrać opcję **[Dodatki]**

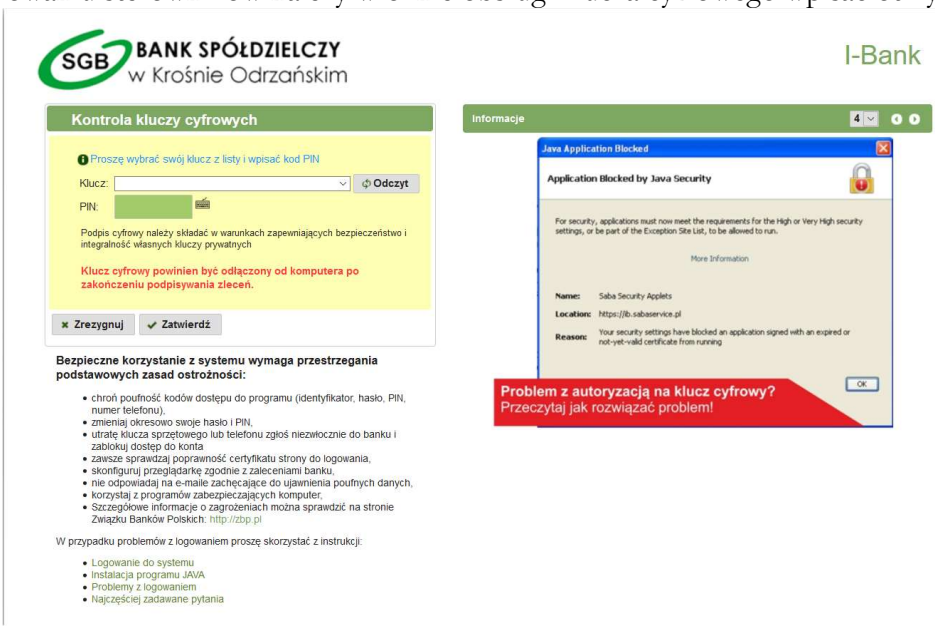


6. Następnie z lewego Menu proszę wybrać **[Wtyczki]**, odszukać na liście **[Saba Firefox Token Signing lugin...]** i w opcji **[Więcej]** ustawić flagę **[Zawsze aktywuj]**



7. Niektóre programy antywirusowe mogą blokować wtyczkę **Saba Plugin.** Należy wtedy dodać stronę banku internetowego do stron zaufanych, np. **ESET Smart Security, ESET Endpoint Antivirus** W menu głównym programu antywirusowego należy wybrać zakładkę Ustawienia, a następnie przejść do ustawień Ochrony dostępu do stron internetowych. W oknie ustawień kliknąć na sekcję Zarządzanie adresami URL i dopisać adres banku internetowego. **ESET NOD32 Antivirus** W oknie ustawień zaawansowanych należy przejść do zakładki Ochrona systemu plików w czasie rzeczywistym, następnie w sekcji Skanuj odznaczyć opcję Tworzenie pliku i zatwierdzić wybierając przycisk OK.

8. Po zainstalowaniu sterowników należy w oknie obsługi klucza cyfrowego wpisać otrzymany z banku PIN.

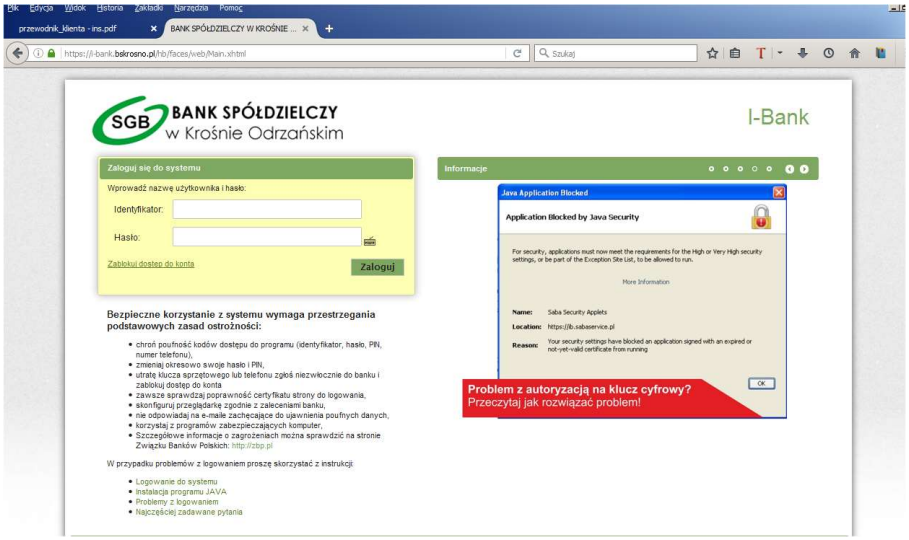


Uwaga!!! Przy pierwszym logowaniu system wymaga zmiany hasła logowania do systemu. Dodatkowo po zalogowaniu przy użyciu otrzymanego z banku PIN należy dokonać zmiany PIN w zakładce

ustawienia systemu. W celu bezpiecznego użytkowania systemu należy okresowo zmieniać hasło dostępu do systemu oraz PIN.

3.2.2 Klienci korzystający z autoryzacji kodem SMS

Po wybraniu opcji logowania do systemu I-Bank na ekranie zostanie wyświetlony formularz rejestracji.

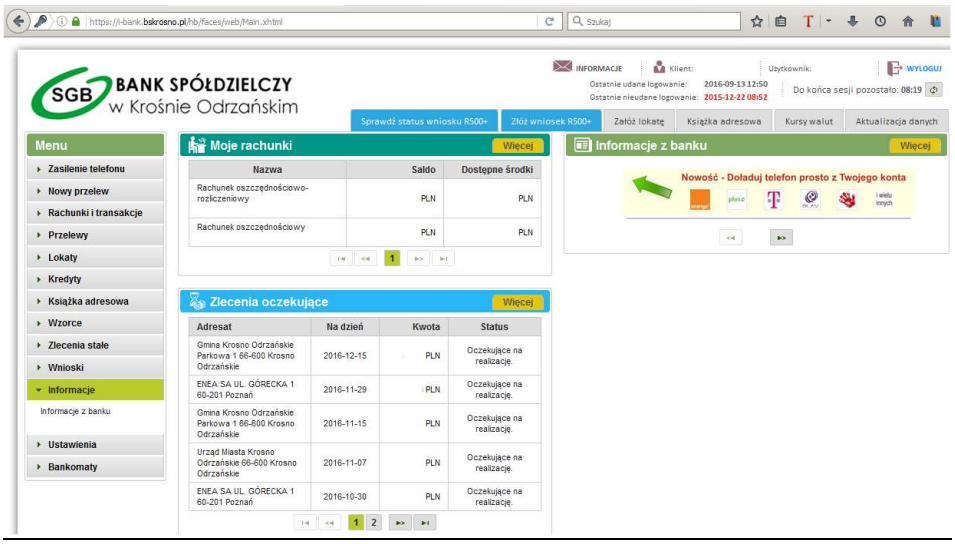


Uwaga!: W przypadku pierwszego logowania system zażąda zmiany hasła!

Należy podać nowe i potwierdzić nowe hasło składające się ze znaków opisanych w zasadach bezpieczeństwa niniejszego Przewodnika.

Uwaga! W przypadku wyboru w banku opcji silnego uwierzytelniania o logowaniu do systemu klient zostanie poinformowany komunikatem SMS.

3.2 Ekran główny systemu bankowości elektronicznej

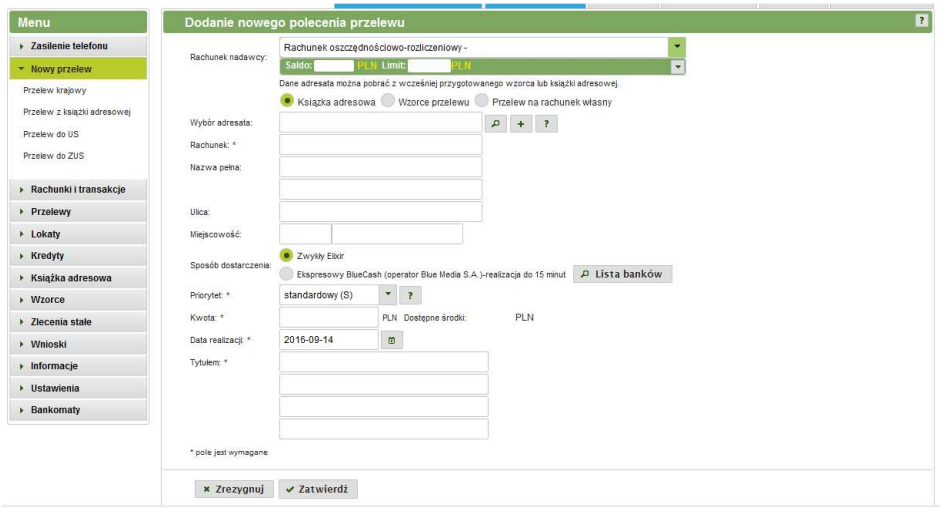


Ekran główny może składać się z bloków tematycznych tj. „MENU"; „Moje rachunki"; „Zlecenia oczekujące"; „Informacje z banku".

<u>Zasilanie telefonów komórkowych:</u>

Należy wpisać lub wybrać wcześniej wpisany do [książki adresowej] numer telefonu komórkowego, który ma zostać doładowany. Następnie zaznaczyć operatora, podać kwotę i wskazać który rachunek ma zostać obciążony wskazaną kwotą. Po zatwierdzeniu należy wpisać otrzymany [kod SMS] i zatwierdzić lub użyć [klucza USB oraz PIN].

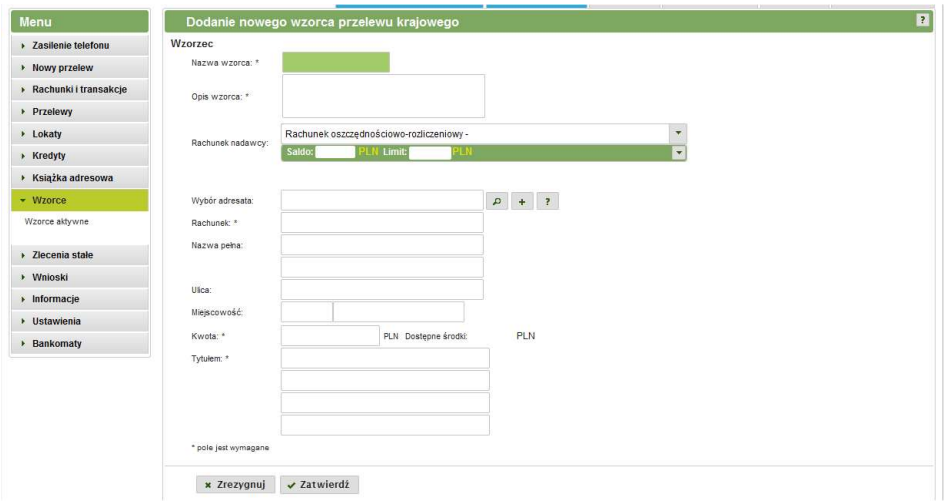
Nowy przelew



Nowy przelew Elixir lub przelew Ekspresowy Bluecash można dokonać na kilka sposobów.

1. W sytuacji gdy jest to przelew jednorazowy wybieramy rachunek z którego ma być realizowany, następnie wypełniamy pola przelewu. Zaznaczamy sposób dostarczenia (zwykły, ekspresowy). W przypadku wyboru przelewu [ekspresowego bluecash] należy zaznaczyć oświadczenie, o świadomości iż operatorem jest blue media SA.

2. Jeżeli płatność będzie powtarzać się w przyszłych okresach, można stworzyć wzorzec przelewu. Wzorzec ma postać formatki (rys. poniżej) przelewu i wymaga akceptacji otrzymanym [kodem SMS] lub użyć [klucza USB oraz kodu PIN] .

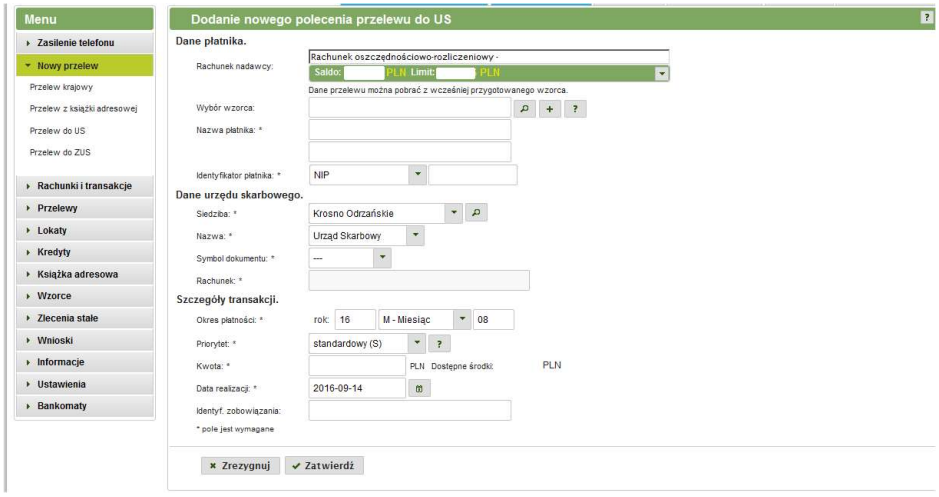


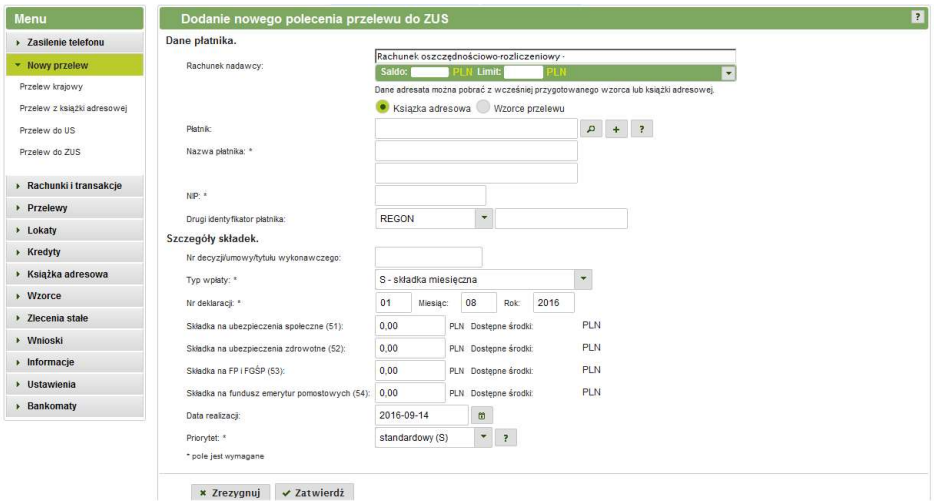
Następnie w razie potrzeby powtórzenia przelewu do wybranego kontrahenta wystarczy wybrać wypełniony wzorzec z listy, poprawić kwotę, i/lub tytuł przelewu i zatwierdzić otrzymanym [kodem SMS] lub użyć [klucza USB oraz kodu PIN]. Wzorce można edytować, każda zmiana wymaga [kodu SMS] lub użyci [klucza USB oraz kodu PIN].

3. Kolejnym sposobem jest stworzenie zlecenia stałego. W przypadku gdy kwota jest niezmienna a płatność ma być dokonywana z częstotliwością (tygodniową, miesięczną, kilku miesięczną, lub roczną) wypełniamy formatkę zlecenia stałego (rys. poniżej) i zatwierdzamy otrzymanym [kodem SMS] lub poprzez użycie [klucza USB oraz kodu PIN]. System będzie automatycznie realizował zlecenie w ustalonych terminach bez konieczności każdorazowej akceptacji.

Formatka nowego przelewu daje możliwość pobrania danych z wcześniej stworzonej książki adresowej lub wzorca przelewu oraz dokonani przelewu wewnętrznego pomiędzy kontami własnymi klienta.

Menu „Przelewy" umożliwia także w prostu sposób dokonywanie przelewów do Urzędów Skarbowych lub ZUS. (Patrz. rysunki poniżej)

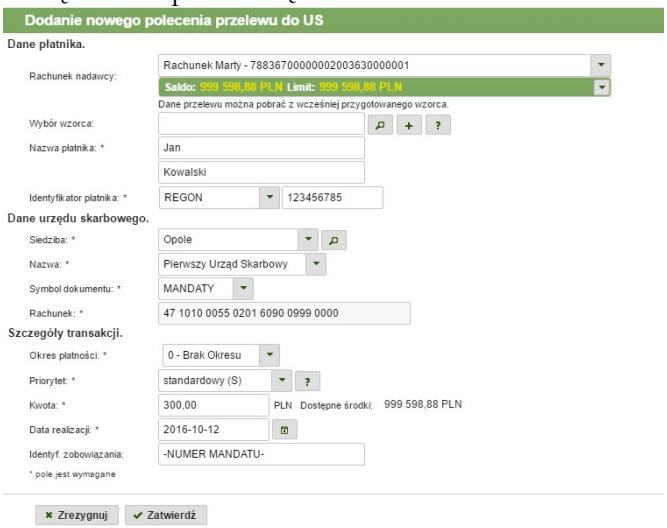




Sposób dokonywania wpłat należności z tytułu grzywien

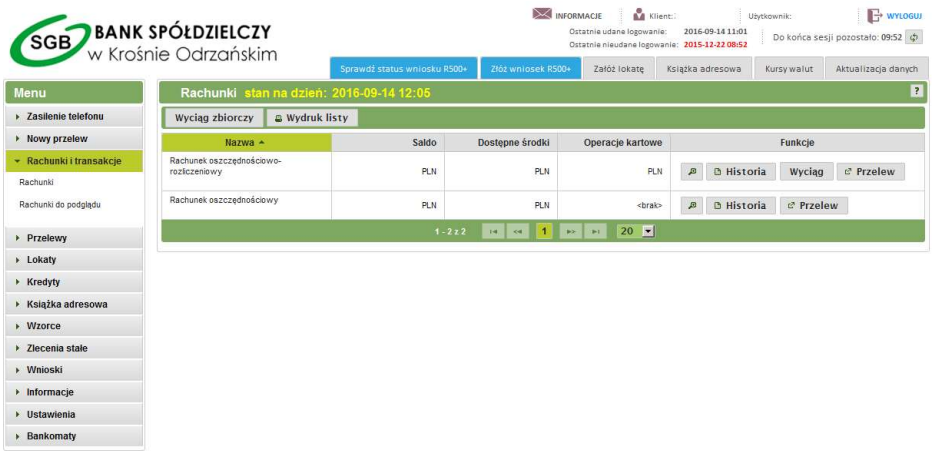
W systemie I-Bank należy wybrać opcję **Nowy Przelew -> Przelew do US**

1. W sekcji "Dane urzędu skarbowego" wypełnić pola:
   - Siedziba: Opole,
   - Nazwa: Pierwszy Urząd Skarbowy
   - Symbol dokumentu: MANDATY
2. W polu "Identyfikator zobowiązania" wpisać serię i numer mandatu



Rachunki i transakcje

W menu „Rachunki i transakcje" uzyskasz dostęp do informacji o aktualnym saldzie na rachunkach, dostępnych środkach, blokadach wynikających z operacji kartami płatniczymi. Ponadto sprawdzisz historię rachunku lub wydrukujesz wyciąg bankowy.



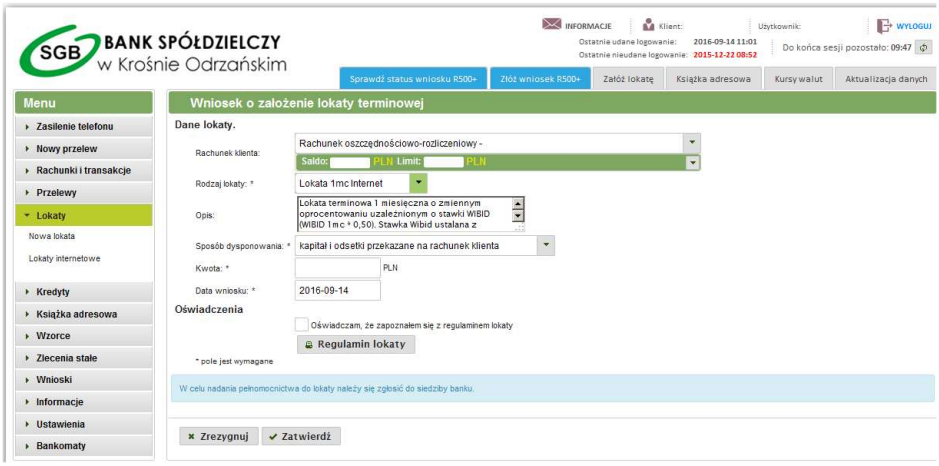
W zależności od wyboru we wniosku na usługę bankowości elektronicznej rodzaju wyciągu, otrzymujesz podgląd oraz możliwość wydruku wyciągów dziennych, miesięcznych lub za wybrany okres. Wydruki można zapisywać w formacie PDF lub zapisywać w wybranym formacie wykorzystywanym w zewnętrznych aplikacjach,

Przelewy

W tej zakładce uzyskasz informacje o aktualnie oczekujących na realizację przelewach, o przelewach zrealizowanych lub o przelewach odrzuconych przez Bank. W przypadku przelewów odrzuconych uzyskasz informacje o powodzie odrzucenia realizacji przelewu przez bank.

Lokaty

W zakładce „Lokaty" masz możliwość założenia, likwidacji lokat dostępnych wyłącznie dla użytkowników bankowości elektronicznej. Każdą operację zatwierdzamy [kodem SMS] lub [kluczem USB oraz PIN].



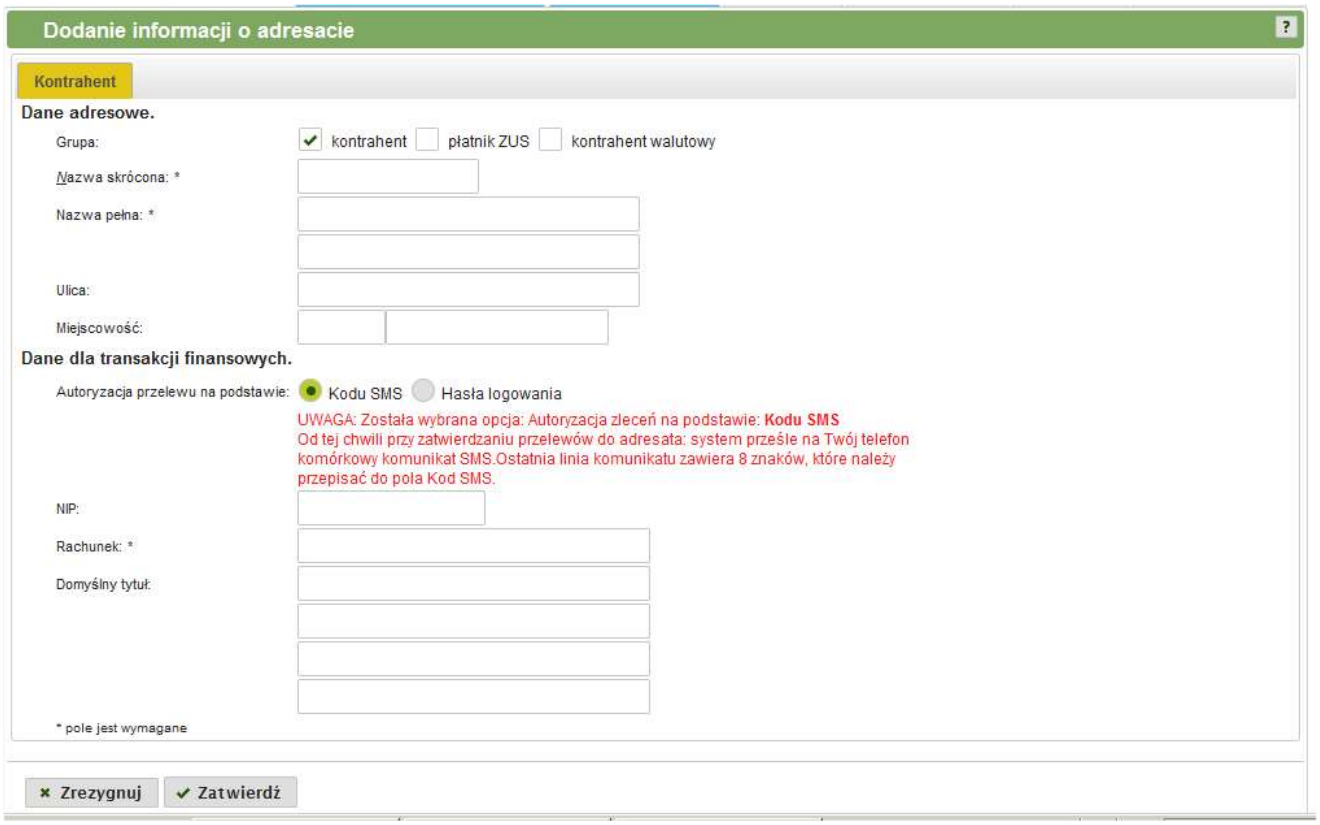
Kredyty

W zakładce „kredyty" uzyskasz informacje o aktualnie posiadanych w banku kredytach ich historii oraz harmonogramach.

Książka adresowa

W tej zakładce masz możliwość tworzenia bazy stałych kontrahentów, z której będzie można korzystać na etapie sporządzania przelewu. Formatka nowego przelewu daje możliwość pobrania danych z wcześniej stworzonej książki adresowej lub wzorca przelewu. Formatka dodania nowej pozycji do książki adresowej daje możliwość wyboru przyszłego sposobu autoryzacji na podstawie [kodu SMS] [klucza USB i PIN] lub [hasła logowania].

Uwaga!. Zaleca się wybór opcji autoryzacji na podstawie [kodu SMS] lub [klucza USB i PIN]!



Wzorce oraz Zlecenia stałe

Formatkę „wzorce" i formatkę „zlecenia stałe' oraz sposób wprowadzania nowego wzorca czy zlecenia stałego opisano w dziale dotyczącym tworzenia przelewów.

Wnioski

Formatka umożliwiająca składanie dedykowanych wniosków do banku lub innych instytucji za pośrednictwem banku (np. rządowy program 500+)

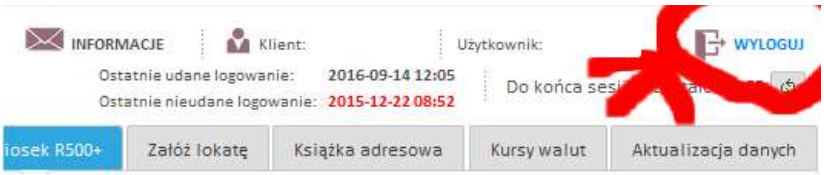
Ustawienia

W zakładce ustawienia mamy możliwość spersonalizowania informacji o rachunku, dokonania zmiany hasła do systemu, zmiany PIN, lub wprowadzenia podpowiedzi na wypadek konieczności blokowania dostępu do konta.

Bankomaty

W tej formatce zlokalizujesz najbliższy bankomat bezprowizyjny lub bankomat innego banku.

3.4 Koniec pracy



Uwaga! Po zakończeniu pracy zawsze korzystaj z opcji ->WYLOGUJ

3.5. Dodatkowe informacje

- **W celach bezpieczeństwa każde zalogowanie do systemu rozpoczyna 10 minutową sesję. Jeśli w tym czasie nie dokonasz żadnej czynności w systemie sesja wygaśnie.**
- **Każda czynność wymaga autoryzacji wykorzystywanym środkiem identyfikacji elektronicznej (kod SMS, klucz USB i PIN) z wyjątkiem książki adresowej gdzie użytkownik może wybrać szybszą metodę autoryzacji nowego przelewu sporządzonego z wykorzystaniem książki adresowej.**
- **Ze względów bezpieczeństwa wyłączona jest możliwość korzystania z systemu z innej geolokalizacji niż POLSKA, w celu uzyskania dostępu z innej geolokalizacji należy skontaktować się z bankiem.**