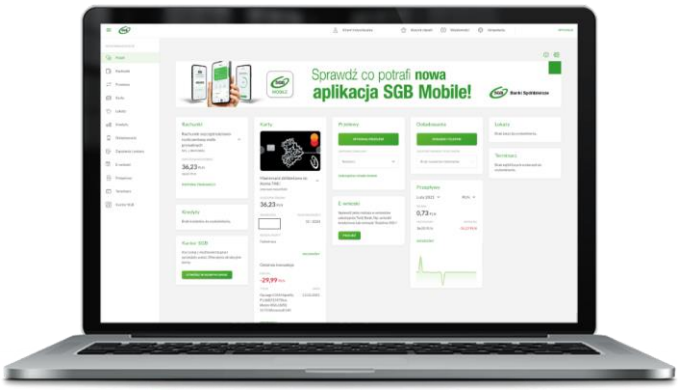


Mobilny Token SGB
Przewodnik dla Użytkownika

Mobilny Token SGB – Funkcjonalność dla SGB24 oraz SGB24 Biznes

SGB Banki Spółdzielcze

Wersja na dzień 11.04.2021 r.

SPIS TREŚCI

Zasady bezpiecznego korzystania z Usługi Bankowości Internetowej SGB24 oraz SGB24 BIZNES

Po pierwsze bezpieczeństwo!
Przy projektowaniu i budowie Usługi Bankowości Internetowej SGB24 wykorzystaliśmy najnowsze rozwiązania, które zapewniają nie tylko wygodę i oszczędności, ale i bezpieczeństwo.

System bezpieczeństwa tworzymy wspólnie z Państwem. Poniżej wskazujemy elementy systemu **zapewnione** przez Bank, a w dalszej części przedstawiamy katalog zasad bezpieczeństwa.

Podstawowe zasady bezpieczeństwa

- Aplikację Token SGB pobieraj i instaluj wyłącznie z Google Play (Android) oraz App Store (iOS)
- Sprawdzaj adres strony www, na której się logujesz oraz jej certyfikat (symbol zamkniętej kłódki. Adres rozpoczyna się od https:// w adresie strony widnieje wyłącznie domena sgb24.pl. po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla sgb24.pl przez firmę DigiCert
- Uważnie czytaj treść w wiadomości SMS / aplikacji Token SGB Przed potwierdzeniem transakcji sprawdzaj treść operacji jej kwotę oraz poprawność numeru rachunku odbiorcy.
- Nigdy nie loguj się do bankowości internetowej z linku, który przyszedł do Ciebie mailem lub SMS-em, ani poprzez link z wyszukiwarki. Wpisuj adres strony logowania ręcznie lub korzystaj z przycisku logowania na oficjalnej stronie banku.
- Nie otwieraj załączników z niepewnych źródeł i nie klikaj w podejrzane linki.
- Ustaw bezpieczne limity operacji dla przelewów, płatności kartami i wypłat gotówki.
- Zmień przypisany automatycznie obrazek bezpieczeństwa na wybrany przez siebie. **Przy każdym logowaniu, przed wpisaniem hasła sprawdzaj czy wyświetla się Twój obrazek oraz czy wyświetlana pod nim data i godzina są aktualne.**
- Korzystaj z legalnego oprogramowania, regularnie aktualizuj urządzenia i oprogramowanie na komputerze i telefonie (system, aplikacje, przeglądarkę, antywirusy).
- Twórz skomplikowane hasła oraz regularnie je zmieniaj.
- Nie używaj tego samego hasła do różnych serwisów oraz nie zapisuj haseł na kartkach ani w plikach na komputerze.
- Nie podawaj / nie wysyłaj swoich loginów i haseł innym osobom.
- Natychmiast zmień swoje hasło lub identyfikator, jeśli zaistnieje podejrzenie, że ktoś mógł je poznać.
- Nie loguj się przez publiczne, niezabezpieczone wi-fi oraz nie loguj się do Bankowości Internetowej na urządzeniach publicznie dostępnych np. w kafejkach, hotelach.
- Nie podłączaj zewnętrznych nośników danych do swojego urządzenia, jeśli nie masz pewności co do ich bezpieczeństwa.

Regularnie zapoznawaj się z komunikatami bezpieczeństwa, które Bank zamieszcza na stronie logowania https://www.sgb.pl/komunikaty-o-bezpieczenstwie/

Szyfrowa transmisja danych

Stosujemy szyfrowanie danych zabezpieczone protokołami *Transport Layer Security (TLS)* wykorzystującymi klucze o długości 256 bitów**. Szyfrowanie to** zapewnia poufność i integralność informacji oraz 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://**

Automatyczne wylogowanie

Dodatkowym zabezpieczeniem jest automatyczne wylogowanie Użytkownika z usługi, w sytuacji stwierdzenia braku jego aktywności w systemie przez określony czas. Po automatycznym wylogowaniu wystarczy ponowne zalogowanie, aby Klient mógł korzystać z usługi.

Blokada

W przypadku trzech błędnych prób zalogowania się do Usługi Bankowości Internetowej SGB24/SGB24 BIZNES następuje automatyczna blokada dostępu do systemu danego Użytkownika. W celu odblokowania systemu należy skontaktować się z Doradcą Call Center pod numerem infolinii 800 888 888 lub 61 647 28 46 (dla połączeń z zagranicy i telefonów komórkowych).

Limity transakcji

Przed aktywacją Usługi Bankowości Internetowej SGB24 oraz w trakcie korzystania z niej można określić jednorazowe lub dzienne limity wykonywanych operacji, czyli maksymalną kwotę pojedynczego przelewu oraz maksymalną łączną kwotę wszystkich realizowanych przelewów w ciągu dnia.

Zastrzeżenie środków dostępu

W przypadku zagubienia lub kradzieży urządzenia mobilnego należy niezwłocznie je zastrzec w placówce bankowej lub telefonicznie pod numerem Call Center 800 888 888 lub 61 647 28 46 (dla połączeń z zagranicy i telefonów komórkowych).
Należy również pamiętać, by w przypadku zmiany numeru telefonu, na które przesyłane są hasła jednorazowe SMS, zgłosić ten fakt do Banku.

Logowanie do Usługi Bankowości Internetowej SGB24/SGB24 BIZNES

- Do obsługi pełnej funkcjonalności aplikacji **zalecane jest** korzystanie z jednej z wymienionych przeglądarek (w wersjach aktualnych bądź o jedną niższą):
  - Platformy stacjonarne (desktop/laptop)
    - Chrome
    - Firefox
    - Edge
    - Safari (MacOS)
  - Platformy mobilne (tablet oraz mobile)
    - Chrome
    - Safari (iOS)
- Systematycznie należy czyścić cache przeglądarki:
  - Tymczasowe pliki internetowe
  - Pliki Cookie
- Podczas wprowadzania Identyfikatora **nie należy zezwalać** na zapamiętywanie haseł przez przeglądarkę.

- Nigdy nie należy używać wyszukiwarek do znalezienia strony logowania do Bankowości Internetowej. Należy samodzielnie wprowadzać jej adres lub logować się bezpośrednio ze strony Usługi Bankowości Internetowej SGB24
- 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://,** w którym widnieje wyłącznie domena sgb24.pl, natomiast na stronie internetowej musi być widoczny symbol zamkniętej kłódki
- By sprawdzić, czy strona jest autentyczna należy kliknąć na kłódkę, aby zobaczyć, czy certyfikat cyfrowy został wystawiony dla sgb24.pl przez firmę DigiCert z aktualną datą ważności
- **Jeśli symbol kłódki jest niewidoczny lub certyfikat jest nieprawidłowo wystawiony, należy przerwać logowanie i niezwłocznie skontaktować się z Doradcą Call Center pod numerem infolinii 800 888 888 lub 61 647 28 46 (dla połączeń z zagranicy i telefonów komórkowych)**
- Jeśli przy logowaniu pojawi się **nietypowy** komunikat lub prośba o podanie danych osobowych, haseł lub ich aktualizację, należy przerwać logowanie i skontaktować się niezwłocznie z Doradcą Call Center pod numerem infolinii 800 888 888 lub 61 647 28 46 (dla połączeń z zagranicy i telefonów komórkowych)
- Należy pamiętać, iż Bank nigdy nie wysyła do swoich Klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację
- Jeśli zauważą Państwo jakąkolwiek nieprawidłowość podczas logowania lub wystąpią problemy techniczne związane z obsługą aplikacji, należy skontaktować się niezwłocznie z Doradcą Call Center pod numerem infolinii 800 888 888 lub 61 647 28 46 (dla połączeń z zagranicy i telefonów komórkowych)

Korzystanie z Usługi Bankowości Internetowej SGB24

- Po zalogowaniu się do Usługi Bankowości Internetowej SGB24/SGB24 BIZNES nie należy zostawiać komputera bez opieki
- Korzystając z Usługi Bankowości Internetowej SGB24 powinno się używać tylko jednego okna przeglądarki internetowej, natomiast kończyć pracę należy poprzez użycie polecenia Wyloguj
- Należy, co jakiś czas zmieniać hasła stałe i chronić je przed osobami trzecimi - proponujemy zmianę hasła co miesiąc
- Podczas korzystania z Usługi Bankowości Internetowej SGB24/SGB24 BIZNES nie należy używać klawiszy nawigacyjnych przeglądarki internetowej (np. Wstecz, Dalej, Odśwież), system posiada własne klawisze, które umożliwiają sprawne poruszanie się w ramach Usług Bankowości Internetowej SGB24/SGB24 BIZNES
- Jeżeli połączenie z serwisem transakcyjnym zostanie zerwane, należy ponownie zalogować się i sprawdzić, czy system zapamiętał ostatnie zlecenie
- Należy aktualizować system operacyjny i aplikacje istotne dla jego funkcjonowania, np. przeglądarki internetowe – zalecamy korzystanie z najnowszych dostępnych wersji
- 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 Usługi Bankowości Internetowej SGB24 w miejscach ogólnie dostępnych, np. w kawiarenkach internetowych lub poprzez publiczne (niezabezpieczone) sieci bezprzewodowe

Usługa Bankowości Internetowej SGB24 oraz SGB24 BIZNES

Bankowość Internetowa SGB24 to usługa, która umożliwia łatwy i szybki dostęp do konta poprzez sieć Internet. Dzięki niej w bezpieczny i wygodny sposób można zarządzać swoimi pieniędzmi na koncie, przez stały – 24 h na dobę – dostęp do wszystkich informacji o rachunkach, realizowanych operacjach oraz przez samodzielne wykonywanie, dyspozycji np. przelewów, zleceń stałych, zakładania lokat.

Użytkownik Usługi Bankowości Internetowej SGB24 ma możliwość korzystania z wybranych przez siebie, bezpiecznych środków dostępu (zgodnie z aktualną ofertą Banku) w postaci:

Identyfikator ID

Służy do identyfikacji Użytkownika przy logowaniu do systemu. Jest to niepowtarzalny, nadawany przez Bank ciąg znaków, który otrzymuje każdy Użytkownik usługi. Składa się z cyfr i/lub liter, należy go chronić i nie udostępniać osobom trzecim.

Aplikacja Mobilna Token SGB

Aplikacja służy do logowania i autoryzacji dyspozycji złożonych za pośrednictwem Bankowości Internetowej. Instalowana jest na urządzeniach mobilnych typu smartfon lub tablet i jest udostępniona do pobrania ze sklepu - Google Play (Android) oraz App Store (iOS), w zależności od systemu operacyjnego urządzenia mobilnego.
W celu zmiany sposobu logowania należy skontaktować się z Oddziałem Banku lub CallCenter.

Logowanie

- Identyfikator ID + aplikacja Token SGB (wraz z PINem do aplikacji Token SGB)

Przy pierwszym logowaniu SMS przesłany jest w momencie gdy użytkownik wpisze swój login i naciśnie przycisk ***Dalej***.

Autoryzacja

- Aplikacja Token SGB

Uwaga! W przypadku utraty urządzenia mobilnego należy niezwłocznie zastrzec dostęp do usługi zgłaszając ten fakt w Oddziale Banku lub dzwoniąc pod numer Call Center 800 888 888 lub 61 647 28 46 (dla połączeń z zagranicy i telefonów komórkowych). Należy pamiętać również, by w przypadku zmiany numeru telefonu zgłosić ten fakt do Banku.
Środki dostępu służą zarówno do logowania do Usługi Bankowości Internetowej SGB24, jak i do autoryzacji zlecanych w systemie dyspozycji.

Wymagania Sprzętowe dla aplikacji mobilnej

Aplikacja Token SGB działa na wybranych platformach mobilnych:

- Android wersje od 6.x i wyższe
- iOS wersje od 9.x i wyższe
- Brak wsparcia dla Windows Phone

KLIENCI SGB24 oraz SGB24 BIZNES

Zmiana hasła tymczasowego/Rejestracja urządzenia mobilnego (autoryzującego) podczas pierwszego logowania do Bankowości Internetowej

Użytkownik ma możliwość zalogowania się do systemu Bankowości Internetowej za pomocą aplikacji mobilnej Token SGB. Wygenerowane hasło tymczasowe zostaje wysłane za pomocą SMS na wskazany przez Użytkownika numer telefonu. Hasło wymagane jest przy logowaniu.Użytkownik powinien je zmienić przed upływem okresu ważności, podczas logowania.

Proces pierwszego logowania za pomocą aplikacji Token SGB do Bankowości Internetowej w przypadku, gdy Użytkownik nie posiada aktywnego sparowanego urządzenia mobilnego :

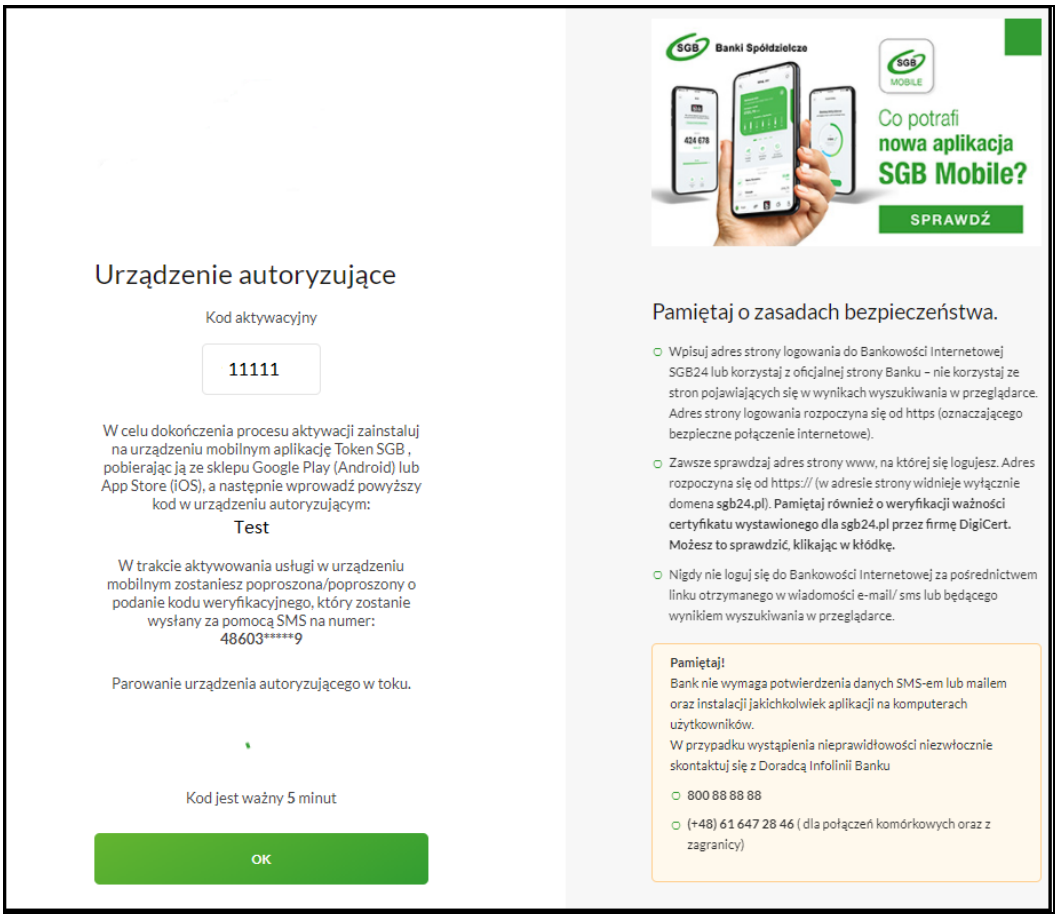
1. Użytkownik wprowadza identyfikator ID i hasło tymczasowe, które otrzymał poprzez SMS.
2. Po poprawnym wprowadzeniu hasła tymczasowego Użytkownik jest proszony o jego zmianę zgodnie z polityką bezpieczeństwa widoczną na stronie logowania. Wymagane jest podanie nowego hasła i powtórzenie nowego hasła,

Uwaga: Przy pierwszym logowaniu SMS zostaje dostarczony w momencie gdy użytkownik wpisze swój login i naciśnie przycisk ***Dalej***.

Po wprowadzeniu hasła Użytkownik wybiera przycisk ***Dalej***.

3. Użytkownik wpisuje dowolną nazwę urządzenia i wybiera przycisk ***Dalej***.

4. W kolejnym kroku system Bankowości Internetowej generuje oraz prezentuje kod aktywacyjny urządzenia mobilnego oraz komunikat jakie dane są wymagane do wprowadzenia przez Użytkownika w aplikacji mobilnej Token SGB w celu potwierdzenia parowania:



5. Użykownik uruchamia aplikację Token SGB i prezentowany kod aktywacyjny wprowadza w aplikacji mobilnej Token SGB:

6. Po wprowadzeniu kodu aktywacyjnego Użytkownik potwierdza go kodem weryfikacyjnym przesłanym SMS-em:

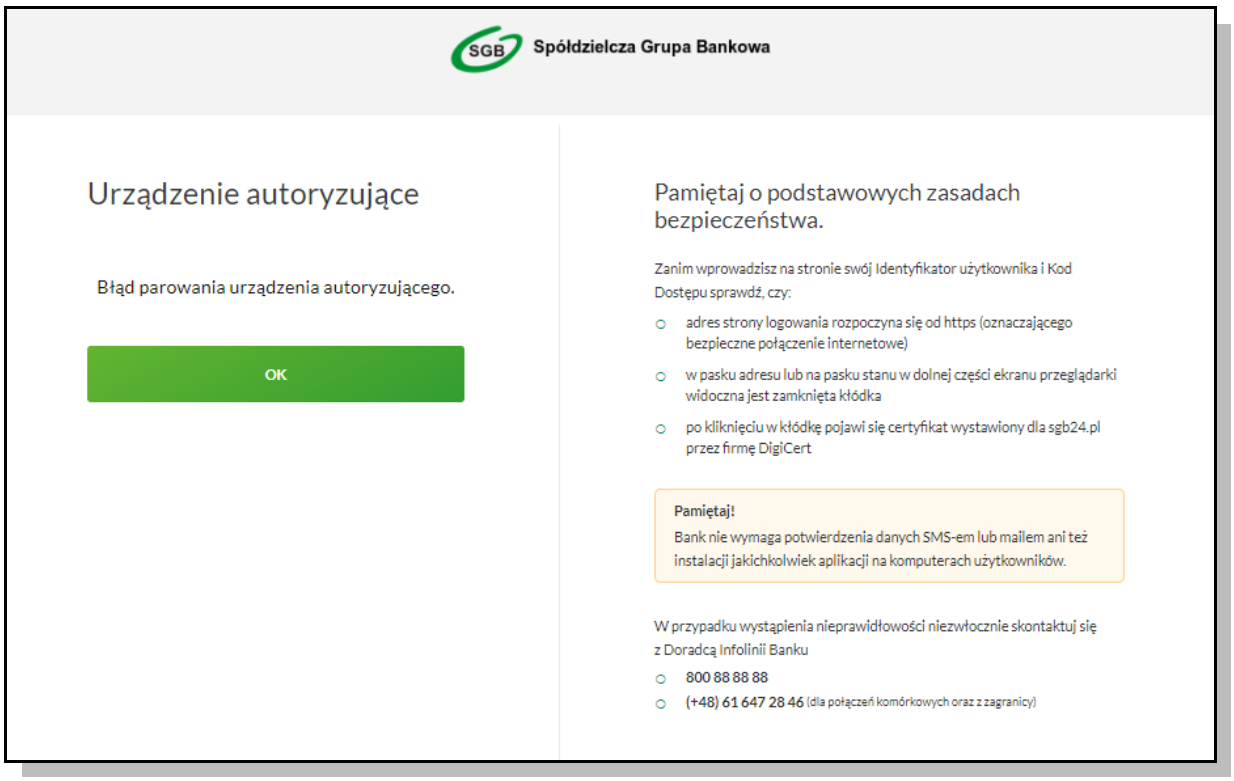
7. Użytkownik nadaje PIN do logowania w aplikacji mobilnej Token SGB:

8. Po poprawnym sparowaniu urządzenia Użytkownikowi wyświetlony jest komunikat potwierdzający dodanie urządzenia:

- w aplikacji mobilnej Token SGB:

- w systemie Bankowości Internetowej - zostaje zalogowany do systemu:

W przypadku, gdy proces parowania urządzenia nie powiedzie się, np. w wyniku upływu czasu, na zakończenie procesu dodawania urządzenia w systemie Bankowości Internetowej wyświetlony zostanie komunikat:



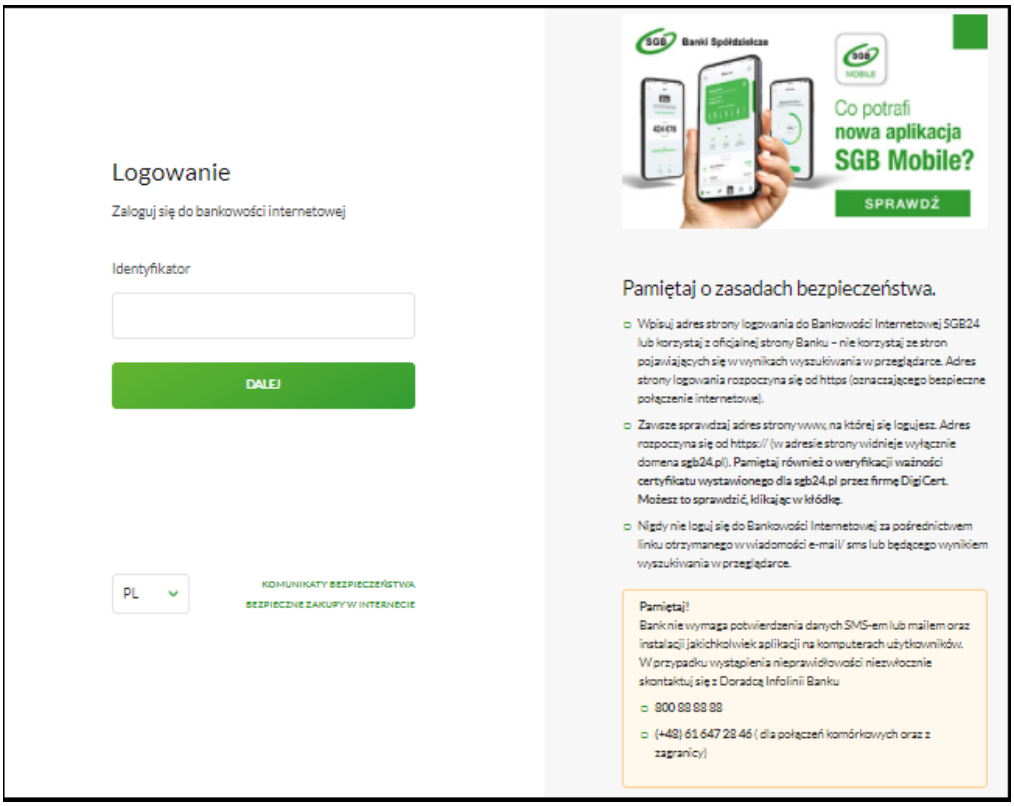
Logowanie do systemu Bankowości Internetowej za pomocą aplikacji mobilnej Token SGB

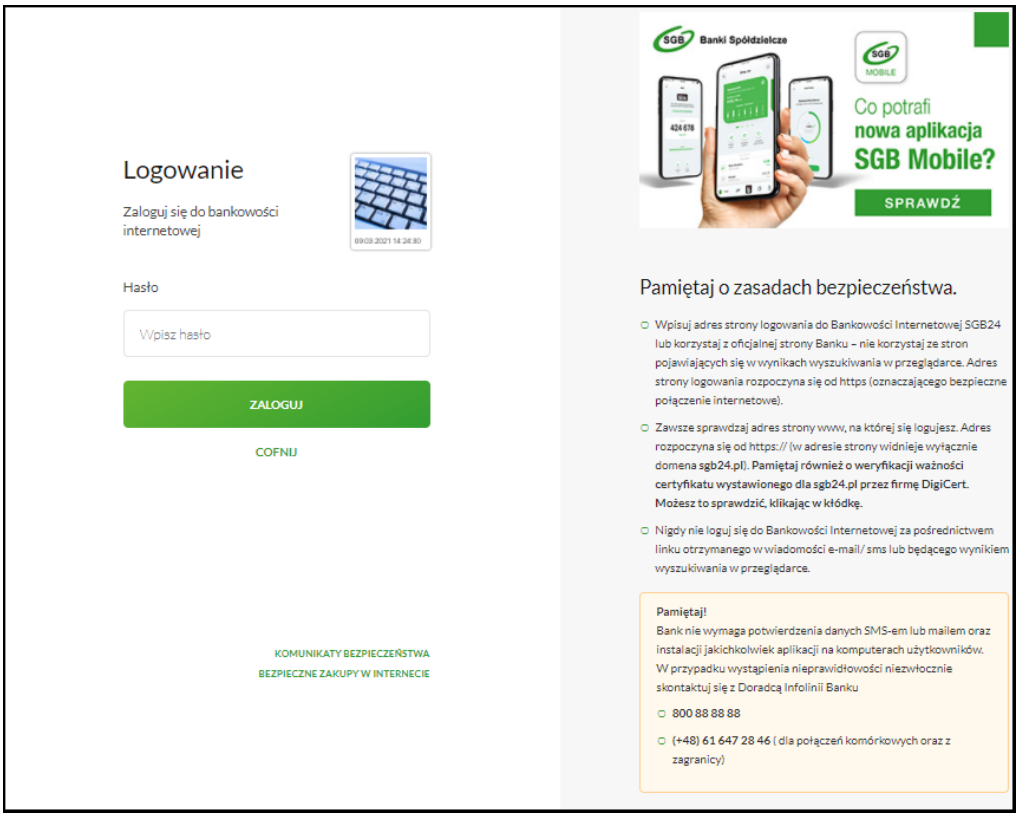
Użytkownik ma możliwość zalogowania się do systemu Bankowości Internetowej za pomocą aplikacji mobilnej Token SGB, jeżeli posiada **sparowane** aktywne urządzenie oraz ustanowione przez siebie hasło.

Proces logowania za pomocą aplikacji mobilnej Token SGB do systemu Bankowości Internetowej jest następujący:

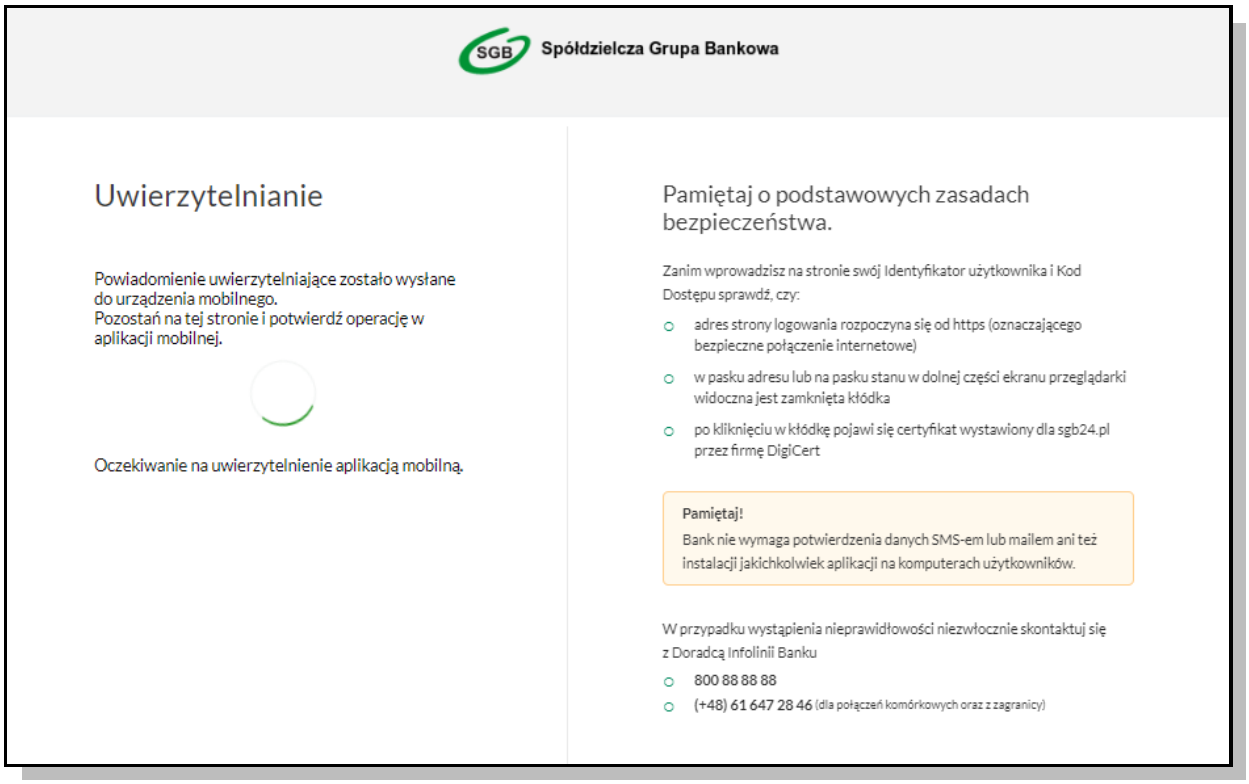
1. W polu Identyfikator Użytkownik wprowadza identyfikator ID nadany przez Bank i wybiera opcję ***Dalej***, a następnie w polu ***HASŁO*** wprowadza hasło do logowania i wybiera przycisk ***ZALOGUJ***.

Uwaga: Przy pierwszym logowaniu SMS zostaje dostarczony w momencie gdy użytkownik wpisze swój login i naciśnie przycisk ***Dalej***.





2. System w kolejnym kroku prezentuje ekran informujący o wysłaniu dyspozycji logowania (powiadomienia uwierzytelniającego) na aplikację Token SGB.

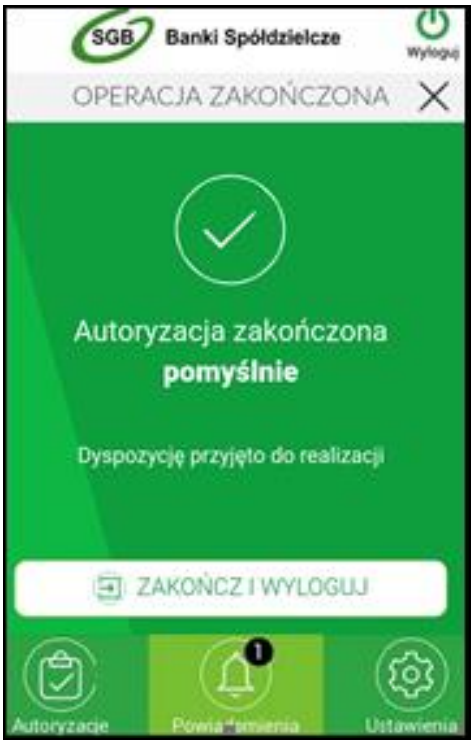


3. System wysyła do aplikacji Token SGB powiadomienie o nowej dyspozycji logowania.

4. Aplikacja wyświetla na urządzeniu mobilnym powiadomienia z informacją o oczekującej na zaakceptowanie dyspozycji.
5. Użytkownik wybiera baner powiadomienia, które uruchamia aplikację Token SGB lub bezpośrednio uruchamia aplikację z systemu operacyjnego urządzenia mobilnego.
6. Użytkownik loguje się do aplikacji Token SGB poprzez wprowadzenie PIN-u.
7. Aplikacja Token SGB prezentuje dane dyspozycji logowania.

8. Użytkownik weryfikuje wyświetlone dane oraz potwierdza realizację dyspozycji logowania wybierając opcję ***AKCEPTUJ***.

9. Aplikacja Token SGB24 wysyła podpisaną dyspozycję do systemu.
10. Użytkownik zostaje zalogowany do systemu Bankowości Internetowej.
11. Aplikacja mobilna Token SGB24 prezentuje potwierdzenie autoryzacji logowania.



W przypadku, gdy Użytkownik nie autoryzował dyspozycji w określonym czasie po wskazaniu dyspozycji w aplikacji Token SGB zostanie zaprezentowany komunikat informujący o braku akceptacji.

W przypadku odrzucenia autoryzacji w aplikacji mobilnej Token SGB, prezentowany jest komunikat:

W przypadku, gdy logowanie do Bankowości Internetowej nie powiodło się z powodu:

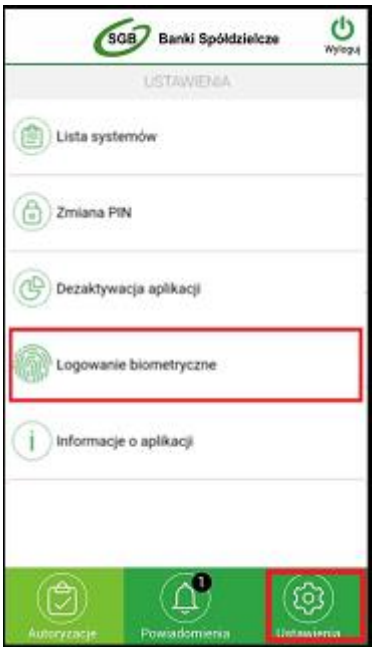
- braku autoryzacji dyspozycji w określonym czasie,
- odrzucenia autoryzacji w aplikacji mobilnej Token SGB,

w systemie Bankowości Internetowej jest wyświetlany komunikat:

Powiadomienie autoryzacyjne zostało wysłane do urządzenia mobilnego.
Pozostań na tej stronie i potwierdź operację w aplikacji mobilnej.
Autoryzacja została odrzucona

Logowanie biometryczne do systemu Bankowości Internetowej

Użytkownik ma możliwość włączenia i wyłączenia logowania biometrycznego. W tym celu należy przejść do ustawień, a następnie nacisnąć **Logowanie biometryczne**



Przy włączonej opcji prezentuje się następujący ekran:

1. Logowanie odciskiem palca

2. Logowanie za pomocą FaceID (dla użytkowników iOS)

W celu włączenia logowania biometrycznego należy zatwierdzić operację przyciskiem ***WŁĄCZ LOGOWANIE***

UWAGA: W systemie android należy dodatkowo potwierdzić operację przykładając odcisk palca do czytnika.

Po włączeniu logowania biometrycznego prezentowane są następujące informacje dla:
Logowania odciskiem palca:

Logowania za pomocą FaceID

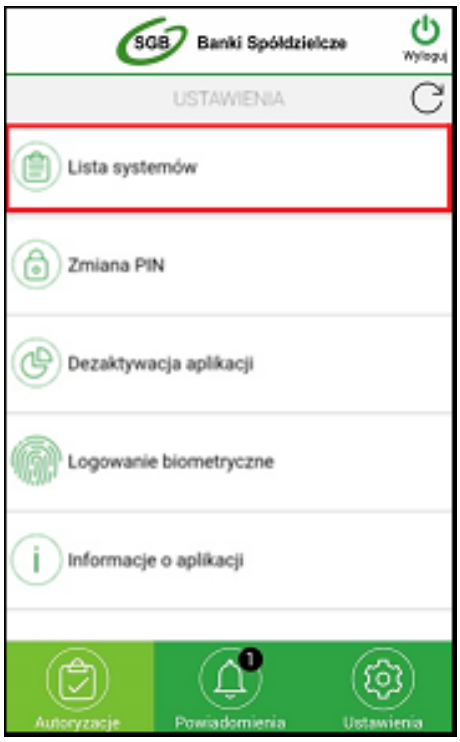
Wybór systemu Bankowości Internetowej

W przypadku, gdy Klient posiada **sparowaną** aplikację z więcej niż jednym systemem bankowości internetowej (np. w BS Miasto1 oraz w BS Miasto2), wówczas na ekranie logowania aplikacji Token SGB Użytkownik ma możliwość wyboru systemu Bankowości Internetowej, w ramach którego działać będzie aplikacja. Kod PIN służący do logowania do aplikacji Token SGB może być taki sam w ramach różnych systemów bankowości internetowej.

Użytkownik po wyborze interesującego go systemu Bankowości Internetowej, a następnie przycisku ***ZALOGUJ*** będzie pracował w wybranym systemie. Użytkownik będzie widział wyłącznie powiadomienia oraz **dyspozycje do autoryzacji** we wskazanym przez siebie systemie Bankowości Internetowej.

Zmiana systemu Bankowości Internetowej w aplikacji Token SGB

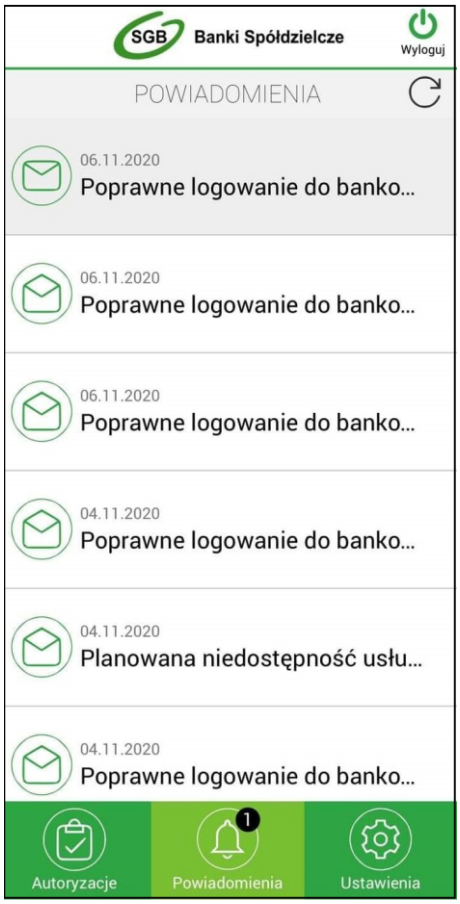
W przypadku, gdy Klient posiada **sparowaną** aplikację z więcej niż jednym systemem Bankowości Internetowej, po zalogowaniu do aplikacji oraz wyborze opcji *Ustawienia -> Lista systemów* prezentowana jest lista systemów dostępnych dla Użytkownika.



Po wskazaniu systemu zostanie zaprezentowana formatka umożliwiająca **zalogowanie się** do wybranego banku w ramach Bankowości Internetowej.

Powiadomienia

W tokenie SGB możliwe jest odbieranie powiadomień. SMS wysyłane z Banku wyświetlane są jako PUSH na urządzeniu mobilnym bez wyświetlania szczegółów powiadomienia. Użytkownik ma możliwość odczytania powiadomień:

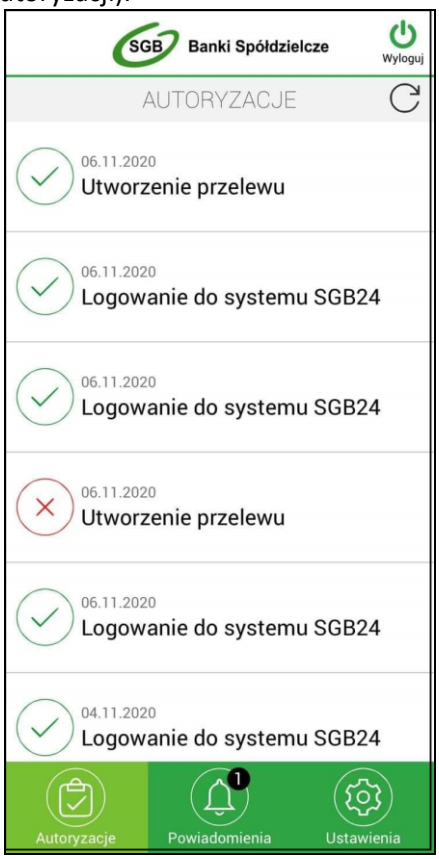


Lista dyspozycji do autoryzacji w aplikacji mobilnej Token SGB

Po wyborze opcji ***AUTORYZACJE*** prezentowana jest lista dyspozycji złożonych w systemie Bankowości Internetowej, dla których wymagana jest autoryzacja. Dyspozycje mają określony czas ważności, po upływie którego są anulowane – autoryzacja nie jest możliwa. Dyspozycje, które zostały obsłużone w aplikacji Token SGB prezentowane są w następujących statusach:

- *Podpisana* – dyspozycja zaakceptowana poprawnie (oznaczona ikonką)
- *Anulowana* – dyspozycja niezaakceptowana w określonym czasie (oznaczona ikonką)
- *Odrzucona* – dyspozycja odrzucona (oznaczona ikonką)
- *Oczekująca* – dyspozycja oczekuje na zaakceptowanie (oznaczona ikonką)

W ramach obsługi jednego systemu Bankowości Internetowej, pojawienie się kolejnej dyspozycji do autoryzacji anuluje obecnie aktywną dyspozycję do autoryzacji (w danym czasie może być dostępna wyłącznie jedna dyspozycja do autoryzacji).



Ikonka dostępna nad listą autoryzacji powoduje odświeżenie prezentowanej listy.
Wybór pozycji na widżecie **Autoryzacje** przenosi Użytkownika do podglądu szczegółów autoryzacji.