

Witamy w świecie Bankowości Elektronicznej Spółdzielczej Grupy Bankowej



Przewodnik dla Użytkownika

Klienci indywidualni oraz firmowi



Call Center

800 888 888 dla połączeń krajowych, połączenie bezpłatne
+ 48 61 647 28 46 dla połączeń komórkowych oraz z zagranicy
(opłata za połączenie zgodna z taryfą danego operatora), dostępne w dni
robocze w godzinach 8:00 – 22:00

SPIS TREŚCI

| | |
|--|-----------|
| ZASADY BEZPIECZNEGO KORZYSTANIA Z USŁUGI BANKOWOŚCI ELEKTRONICZNEJ KDBS24..... | 3 |
| USŁUGA BANKOWOŚCI ELEKTRONICZNEJ KDBS24 | 5 |
| WYMAGANIA SPRZĘTOWE DLA APLIKACJI MOBILNEJ | 6 |
| KLIENCI INDYWIDUALNI..... | 6 |
| REJESTRACJA URZĄDZENIA AUTORYZUJĄCEGO PODCZAS PIERWSZEGO LOGOWANIA DO BANKOWOŚCI ELEKTRONICZNEJ | 6 |
| ZMIANA HASŁA TYMCZASOWEGO PODCZAS PIERWSZEGO LOGOWANIA DO BANKOWOŚCI ELEKTRONICZNEJ..... | 10 |
| LOGOWANIE DO SYSTEMU BANKOWOŚCI ELEKTRONICZNEJ ZA POMOCĄ APLIKACJI MOBILNEJ TOKEN SGB | 11 |
| WYBÓR SYSTEMU BANKOWOŚCI INTERNETOWEJ..... | 15 |
| ZMIANA SYSTEMU BANKOWOŚCI INTERNETOWEJ W APLIKACJI TOKEN SGB | 17 |
| LISTA DYSPOZYCJI DO AUTORYZACJI W APLIKACJI MOBILNEJ TOKEN SGB | 18 |
| KLIENCI KORPORACYJNI..... | 19 |
| REJESTRACJA URZĄDZENIA AUTORYZACYJNEGO PODCZAS LOGOWANIA DO USŁUGI BANKOWOŚCI ELEKTRONICZNEJ (KORPORACYJNE) | 19 |
| ZMIANA HASŁA TYMCZASOWEGO PODCZAS LOGOWANIA DO USŁUGI BANKOWOŚCI ELEKTRONICZNEJ (KORPORACYJNE) | 22 |
| LOGOWANIE DO USŁUGI BANKOWOŚCI ELEKTRONICZNEJ SGB (KORPORACYJNE) ZA POMOCĄ APLIKACJI MOBILNEJ TOKEN SGB | 23 |
| URZĄDZENIA AUTORYZUJĄCE | 26 |

Zasady bezpiecznego korzystania z Usługi Bankowości Elektronicznej KDBS24

Po pierwsze bezpieczeństwo!

Przy projektowaniu i budowie Usługi Bankowości Elektronicznej KDBS24 wykorzystaliśmy najnowsze rozwiązania, które zapewniają nie tylko wygodę i oszczędności, ale i bezpieczeństwo.

System bezpieczeństwa tworzymy wspólnie z Państwem. Poniżej wskazujemy elementy tego systemu zapewniane przez Bank, w dalszej części rozdziału przedstawiamy katalog zasad bezpieczeństwa – zalecenia do stosowania przez Użytkowników usługi.

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 na koncie. W takim przypadku wystarczy ponowne zalogowanie.

Blokada konta

W przypadku kilku błędnych prób zalogowania się do Usługi Bankowości Elektronicznej KDBS24 następuje automatyczna blokada konta danego Użytkownika, która chroni konto przed dostępem osób nieupoważnionych. W celu odblokowania konta 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).

Zastrzeżenie środków dostępu

W przypadku zagubienia lub kradzieży tokena, hasła stałego, a także utraty telefonu komórkowego należy niezwłocznie zgłosić ich zastrzeżenie 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 Elektronicznej KDBS24

- Do obsługi pełnej funkcjonalności aplikacji **zalecane jest** korzystanie z jednej z wymienionych przeglądarek (w wersjach minimalnych bądź wyższych):
 - Platformy stacjonarne (desktop/laptop)
 - Chrome 50.x
 - IE 11.x
 - Firefox 46.0
 - Platformy mobilne (tablet)
 - Chrome 50.x

- WebKit Mobile (Android 4.4.x)
- Safari (iOS 9.x)
- Platformy mobilne (mobile)
 - Chrome 50.x
 - IEMobile 11.x (Windows Phone)
 - Safari (iOS 9.x)
- Systematycznie należy czyścić cache przeglądarki:
 - Tymczasowe pliki internetowe
 - Pliki Cookie
- Podczas wprowadzania Identyfikatora **nie powinno się 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 Usługi Bankowości Elektronicznej KDBS24
- 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 należy kliknąć na kłódkę, aby zobaczyć, czy certyfikat cyfrowy został wydany na bank oraz czy jest wystawiony 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 prośb 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 Elektronicznej KDBS24

- Po zalogowaniu się do Usługi Bankowości Elektronicznej KDBS24 nie należy zostawiać komputera bez nadzoru
- Korzystając z Usługi Bankowości Elektronicznej KDBS24 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 Elektronicznej KDBS24 nie należy używać klawisze nawigacyjnych przeglądarki internetowej (np. Wstecz, Dalej, Odśwież), system posiada własne klawisze, które umożliwiają sprawne poruszanie się w ramach Usług Bankowości Elektronicznej KDBS24
- 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 internetowej
- 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 Elektronicznej KDBS24 w miejscach ogólnie dostępnych, np. w kawiarenkach internetowych

Usługa Bankowości Elektronicznej KDBS24

Bankowość Elektroniczna KDBS24 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 Elektronicznej KDBS24 ma możliwość korzystania z wybranych przez siebie, bezpiecznych środków dostępu (zgodnie z aktualną ofertą Banku) w postaci:

Identyfikator ID

Służy do identyfikacji przy logowaniu do konta internetowego. Jest to niepowtarzalny, nadawany przez Bank identyfikator, 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 dostępna 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

Autoryzacja

- Aplikacja Token SGB

Uwaga! W przypadku utraty telefonu 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 Elektronicznej KDBS24, jak i do autoryzacji zleceń 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 INDYWIDUALNI

Rejestracja urządzenia autoryzującego podczas pierwszego logowania do Bankowości Elektronicznej

Użytkownik ma możliwość zalogowania się do systemu Bankowości Elektronicznej za pomocą aplikacji mobilnej Token SGB. Wygenerowane hasło tymczasowe zostaje wysłane za pomocą sms na wskazany numer telefonu. Hasło wymagane jest przy logowaniu, ważne jest przez 24h od momentu otrzymania. Użytkownik powinien je zmienić przed upływem okresu ważności, podczas logowania.

Proces pierwszego logowania za pomocą aplikacji Token SGB do Bankowości Elektronicznej w przypadku, gdy użytkownik nie posiada aktywnego sparowanego urządzenia autoryzującego:

1. Użytkownik wprowadza identyfikator ID i hasło tymczasowe, które otrzymał na sms.
2. Użytkownik wpisuje dowolną nazwę urządzenia i wybiera przycisk [DALEJ]

URZĄDZENIE AUTORYZUJĄCE

Nazwa urządzenia

DALEJ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

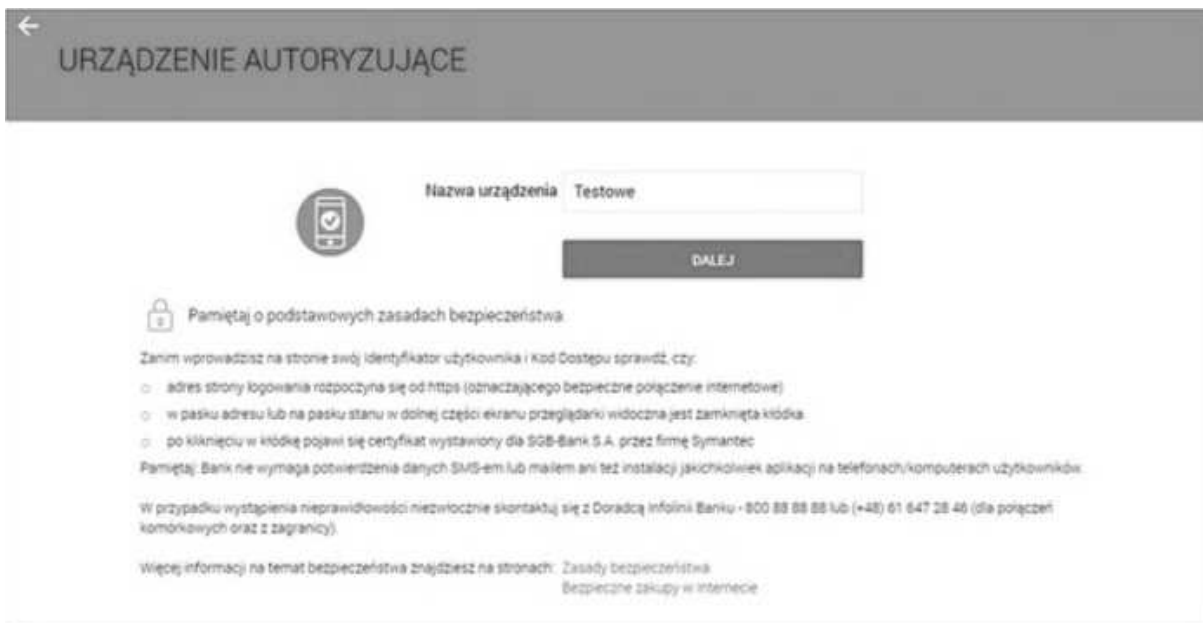
Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- o adres strony logowania rozpoczyna się od https (oznacza bezpieczne połączenie internetowe)
- o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla SGB-Bank S.A. przez firmę Symantec

Pamiętaj! Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników.

W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z Doradcą Infolinii Banku - 800 88 88 88 lub (+48) 61 647 28 46 (dla połączeń komórkowych oraz z zagranicy).

Więcej informacji na temat bezpieczeństwa znajdziesz na stronach: [Zasady bezpieczeństwa](#)
[Bezpieczne zakupy w Internecie](#)



3. W kolejnym kroku system Bankowości Elektronicznej generuje oraz prezentuje kod aktywacyjny urządzenia autoryzującego oraz komunikat jakie dane są wymagane do wprowadzenia przez użytkownika w aplikacji mobilnej Token SGB w celu potwierdzenia parowania:



4. Użytkownik uruchamia aplikację Token SGB i prezentowany kod aktywacyjny wprowadza w aplikacji mobilnej Token SGB:

REJESTRACJA URZĄDZENIA ✕



Przepisz kod aktywacyjny wyświetlony w bankowości internetowej

Wprowadź kod aktywacyjny

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| | 0 | ✕ |

➤ DALEJ

5. Po wprowadzeniu kodu aktywacyjnego użytkownik potwierdza go kodem weryfikacyjnym przesłanym SMS-em:

← REJESTRACJA URZĄDZENIA ✕



W celu identyfikacji konieczne jest **podanie kodu weryfikacyjnego**, który zostanie przesłany za pomocą SMS

Wprowadź kod weryfikacyjny

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| | 0 | ✕ |


➤ DALEJ

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

← REJESTRACJA URZĄDZENIA ✕



Wprowadź PIN, który będzie służył do logowania do aplikacji


Wprowadź PIN 

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| | 0 |  |

➤ DALEJ

6. Po poprawnym sparowaniu urządzenia użytkownikowi wyświetlony jest komunikat potwierdzający dodanie urządzenia:

- w aplikacji mobilnej Token SGB:

 **Banki Spółdzielcze**

REJESTRACJA URZĄDZENIA ✕

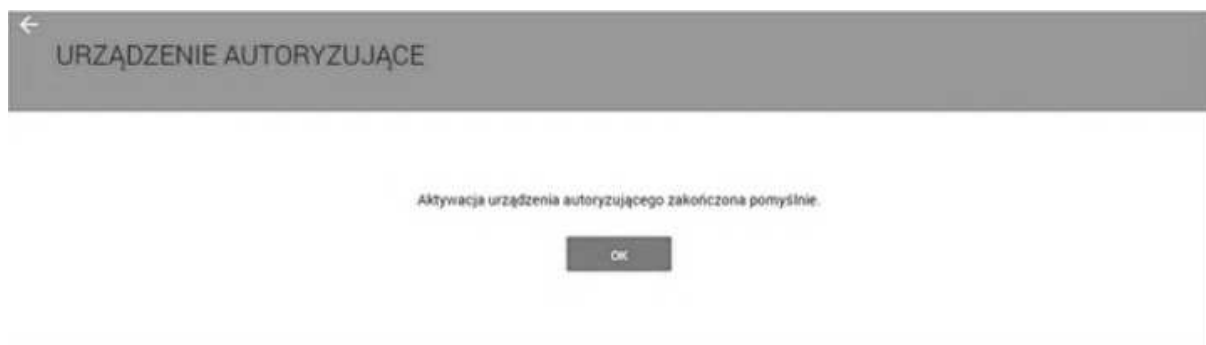


Aktywacja zakończona pomyślnie

Twoje urządzenie zostało zarejestrowane. Od teraz możesz używać aplikacji mobilnej do autoryzacji transakcji

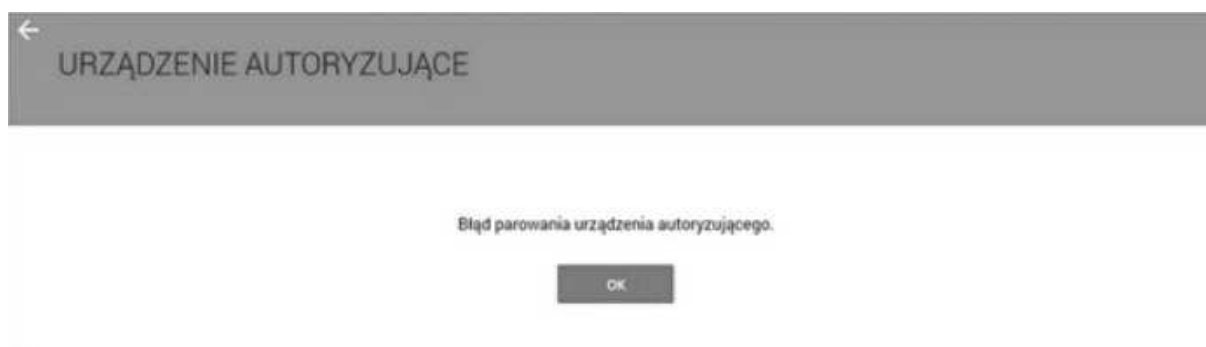
➤ LOGOWANIE

- w Bankowości Elektronicznej - jeżeli użytkownik pozostanie na stronie:



Po wybraniu przycisku [OK] wyświetlona jest formatka do logowania Bankowości Elektronicznej.

W przypadku, gdy proces sparowania urządzenia nie powiedzie się np. w wyniku upłynięcia czasu na zakończenie procesu dodawania urządzenia w systemie Bankowości Elektronicznej wyświetlony jest komunikat:



Zmiana hasła tymczasowego podczas pierwszego logowania do Bankowości Elektronicznej

Po sparowaniu urządzenia autoryzującego podczas pierwszego logowania do Bankowości Elektronicznej za pomocą aplikacji mobilnej Token SGB wymagana jest zmiana hasła tymczasowego na hasło stałe spełniające wymogi bezpieczeństwa:

1. Użytkownik wprowadza identyfikator ID oraz to samo hasło tymczasowe, które otrzymał w wiadomości sms do pierwszego logowania.
2. Po autentykacji użytkownik jest proszony o zmianę hasła tymczasowego zgodnie z polityką bezpieczeństwa widoczną na stronie logowania.

← ZMIANA HASŁA

Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator użytkownika: BR170TQP

Nowe hasło: Wpisz hasło

Powtórz nowe hasło: Wpisz ponownie nowe hasło

ZAPISZ I ZAŁOGUJ

Zadbaj o zachowanie poufności swojego hasła. Nie udostępniaj hasła innym osobom, na żadnych stronach internetowych, pocztą elektroniczną, wiadomością SMS lub w odpowiedzi na zapytania otrzymane od pracowników banku. Definiując swoje hasło pamiętaj o zachowaniu zasad bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

Zasady budowy haseł są następujące:

- musi składać się z 4-20 znaków
- musi zawierać przynajmniej jeden znak specjalny
- musi zawierać przynajmniej jedną wielką literę
- musi zawierać przynajmniej jedną małą literę
- musi zawierać przynajmniej jedną cyfrę

3. Wymagane jest podanie nowego hasła i powtórzenie nowego hasła. Po zapisaniu zmiany hasła za pomocą przycisku [ZAPISZ I ZAŁOGUJ] pojawia się ekran informujący o wysłaniu dyspozycji logowania na aplikację mobilną Token SGB.

Logowanie do systemu Bankowości Elektronicznej za pomocą aplikacji mobilnej Token SGB

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

Proces logowania za pomocą aplikacji mobilnej Token SGB do systemu Bankowości Elektronicznej 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 [ZAŁOGUJ].

Identyfikator

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 SGB-Bank S.A. przez firmę Symantec

Pamiętaj! Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników

W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z Doradcą Infolini Banku – 800 88 88 88 lub (+48) 61 647 28 48 (dla połączeń komórkowych oraz z zagranicy).

Więcej informacji na temat bezpieczeństwa znajdziesz na stronach: [Zasady bezpieczeństwa](#)
[Bezpieczne zakupy w Internecie](#)

← LOGOWANIE

Hasło

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 SGB-Bank S.A. przez firmę Symantec

Pamiętaj! Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników

W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z Doradcą Infolini Banku – 800 88 88 88 lub (+48) 61 647 28 48 (dla połączeń komórkowych oraz z zagranicy).

Więcej informacji na temat bezpieczeństwa znajdziesz na stronach: [Zasady bezpieczeństwa](#)
[Bezpieczne zakupy w Internecie](#)

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

← UWIERZYTELNIANIE

 Powiadomienie uwierzytelniające zostało wysłane do urządzenia mobilnego.
Pozostań na tej stronie i potwierdź operację w aplikacji mobilnej.

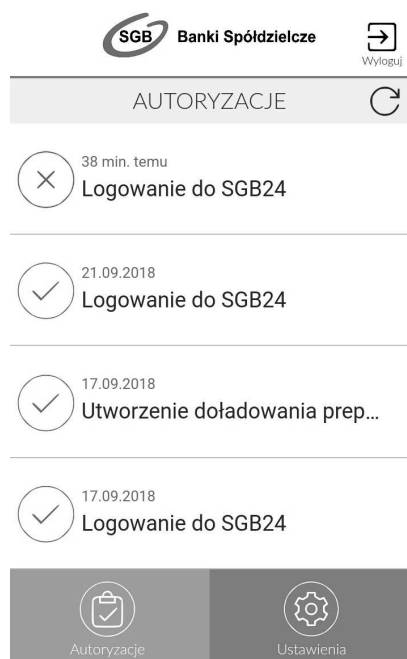


Oczekiwanie na uwierzytelnienie aplikacją mobilną

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

4. Aplikacja wyświetla na urządzeniu mobilnym powiadomienia z informacją o oczekującym powiadomieniu.

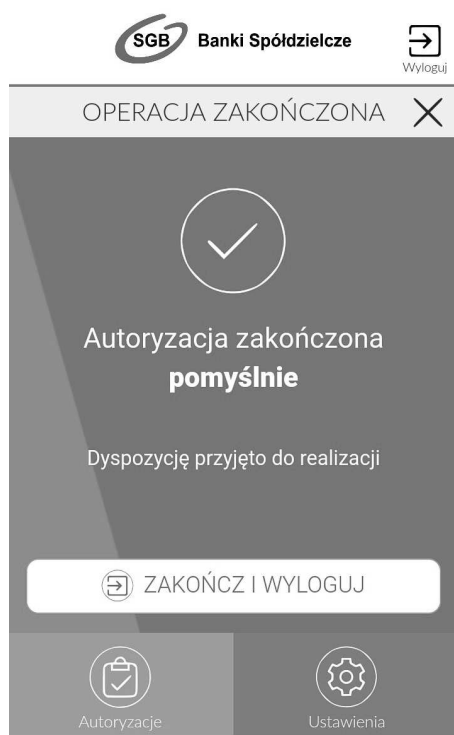
5. Użytkownik wybiera baner powiadomienia, które uruchamia aplikację Token SGB lub bezpośrednio uruchamia aplikację z systemu operacyjnego urządzenia mobilnego.
6. Użytkownik loguje się do aplikacji Token SGB poprzez wprowadzenie PIN-u.
7. Aplikacja Token SGB prezentuje dane dyspozycji logowania.



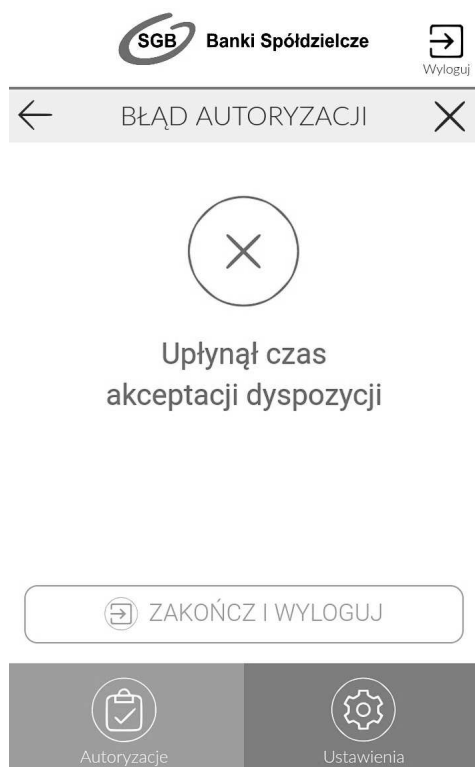
8. Użytkownik weryfikuje wyświetlone dane oraz potwierdza realizację dyspozycji logowania.



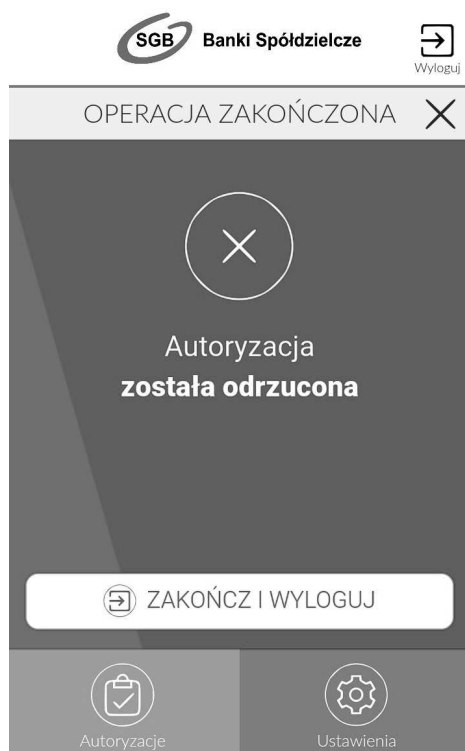
9. Użytkownik wybiera opcję [AKCEPTUJ] i potwierdza logowanie poprzez wprowadzenie PIN-u
10. Aplikacja Token KDBS24 wysyła podpisaną dyspozycją do systemu.
11. Użytkownik zostaje zalogowany do systemu Bankowości Internetowej.
12. Aplikacja mobilna Token KDBS24 prezentuje potwierdzenie autoryzacji dyspozycji.



W przypadku, gdy użytkownik nie podpisał dyspozycji w określonym czasie po wskazaniu dyspozycji w aplikacji Token SGB zostanie zaprezentowany komunikat informujący o błędnej akceptacji.



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



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

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

w systemie Bankowości Elektronicznej jest wyświetlony komunikat:



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.

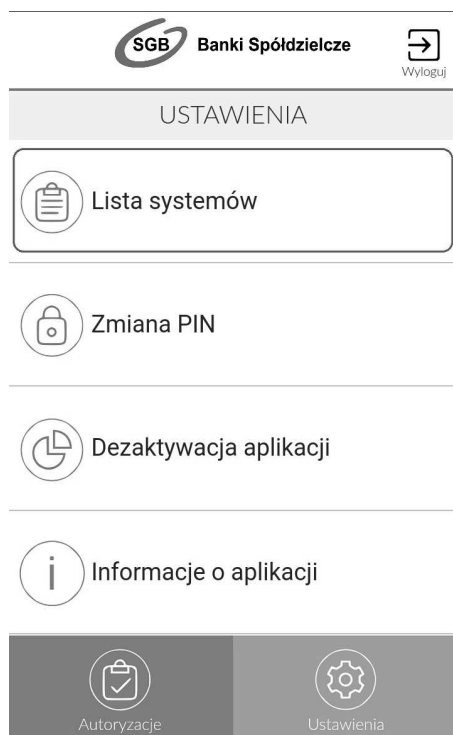


Użytkownik po wyborze interesującego go systemu Bankowości Internetowej, a następnie przycisku [ZALOGUJ] będzie pracował w wybranym systemie. Użytkownik będzie widział wyłącznie powiadomienia oraz **dyspozycje do autoryzacji** we wskazanym systemie bankowości internetowej.



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.

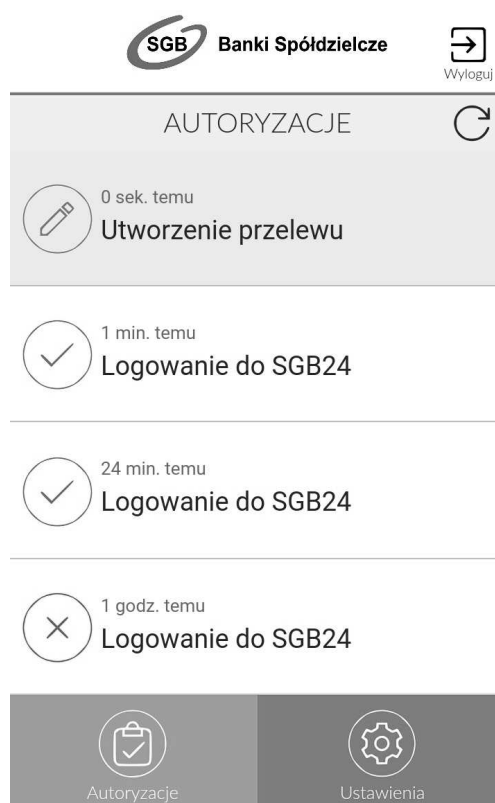



Lista dyspozycji do autoryzacji w aplikacji mobilnej Token SGB

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 (oznaczone ikonką )
- *Anulowana* – dyspozycja nie zaakceptowana w określonym czasie (oznaczone ikonką )
- *Odrzucona* – dyspozycja odrzucona (oznaczone ikonką )
- *Oczekująca* – dyspozycja oczekuje na zaakceptowanie (oznaczone ikonką )

W ramach obsługi jednego systemu bankowości internetowej, pojawienie się kolejnej dyspozycji do autoryzacji anuluje obecnie aktywne dyspozycje 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 widocznie **Autoryzacje** przenosi użytkownika do podglądu szczegółów autoryzacji.

Rejestracja urządzenia autoryzacyjnego podczas logowania do Usługi Bankowości Elektronicznej (korporacyjne)

W celu zmiany sposobu logowania na Token SGB na wniosek użytkownika, po zmianach dokonanych w banku, ustanawiane jest hasło tymczasowe. Wygenerowane hasło tymczasowe wysłane jest za pomocą sms na numer telefonu użytkownika. Hasło jest wymagane przy logowaniu do systemu Usługi Bankowości Elektronicznej (pierwszy krok uwierzytelniania). Hasło ważne jest przez określony okres czasu (24 h). Użytkownik powinien dokonać zmiany hasła przed upływem okresu ważności, podczas logowania.

Proces pierwszego logowania za pomocą aplikacji mobilnej Token SGB w przypadku, gdy użytkownik nie posiada aktywnego sparowanego urządzenia autoryzującego jest następujący:

1. Użytkownik wybiera sposób logowania: Logowanie aplikacją mobilną
2. Użytkownik wpisuje Identyfikator użytkownika oraz hasło tymczasowe i następnie wybiera przycisk [OK]

Wygenerowane hasło tymczasowe wysłane jest za pomocą sms na numer telefonu użytkownika. Hasło ważne jest przez określony okres czasu (24 h). Użytkownik powinien dokonać zmiany hasła przed upływem okresu ważności, podczas logowania.



3. Użytkownik wpisuje nazwę urządzenia i następnie wybiera przycisk [DODAJ].



4. W kolejnym kroku system generuje oraz prezentuje użytkownikowi kod aktywacyjny oraz komunikat jakie dane będą wymagane do wprowadzenia przez użytkownika w aplikacji mobilnej Token SGB w celu potwierdzenia parowania



5. Prezentowany kod aktywacyjny użytkownik wprowadza w aplikacji mobilnej Token SGB:

REJESTRACJA URZĄDZENIA

Przepisz kod aktywacyjny wyświetlony w bankowości internetowej

Wprowadź kod aktywacyjny

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| | 0 | ⊗ |

DALEJ

6. Po wprowadzeniu kodu aktywacyjnego Użytkownik otrzymuje dodatkowy kod SMS, który następnie wprowadza w aplikacji mobilnej Token SGB:

← REJESTRACJA URZĄDZENIA ×



W celu identyfikacji konieczne jest **podanie kodu weryfikacyjnego**, który zostanie przesłany za pomocą SMS

Wprowadź kod weryfikacyjny

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| | 0 | ⊗ |

DALEJ

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

← REJESTRACJA URZĄDZENIA ×



Wprowadź **PIN**, który będzie służył do logowania do aplikacji

Wprowadź PIN ?

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| | 0 | ⊗ |

DALEJ

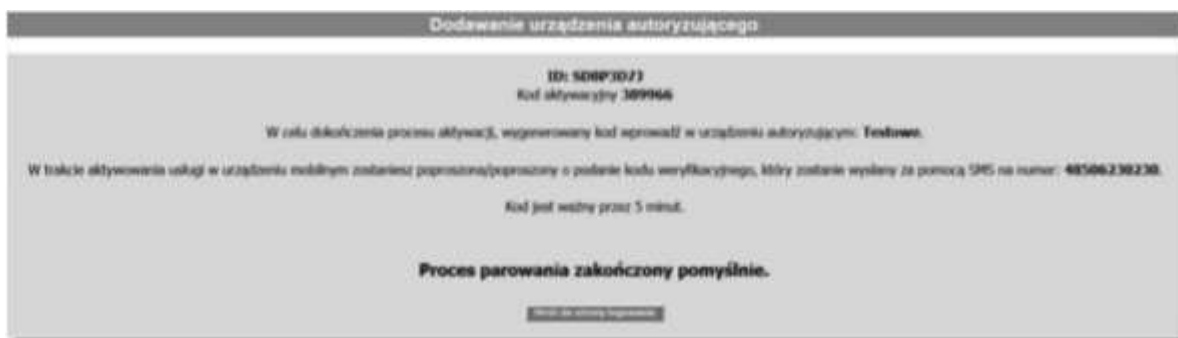
8. Po poprawnym sparowaniu urządzenia użytkownikowi wyświetlony jest komunikat potwierdzający dodanie urządzenia w aplikacji mobilnej Token SGB oraz w systemie Usługi Bankowości Elektronicznej.



Aktywacja zakończona pomyślnie

Twoje urządzenie zostało zarejestrowane. Od teraz możesz używać aplikacji mobilnej do autoryzacji transakcji

➔ LOGOWANIE



Zmiana hasła tymczasowego podczas logowania do Usługi Bankowości Elektronicznej (korporacyjne)

Po sparowaniu urządzenia autoryzującego podczas pierwszego logowania do Bankowości Elektronicznej za pomocą aplikacji mobilnej Token SGB wymagana jest zmiana hasła tymczasowego na hasło stałe spełniające wymogi bezpieczeństwa.

1. Użytkownik wprowadza Identyfikator użytkownika oraz to samo hasło tymczasowe, które otrzymał w wiadomości sms do pierwszego logowania.
2. Po autentykacji użytkownika wymagana jest zmiana hasła tymczasowego na własne poprzez podanie nowego hasła i powtórzenie nowego hasła.

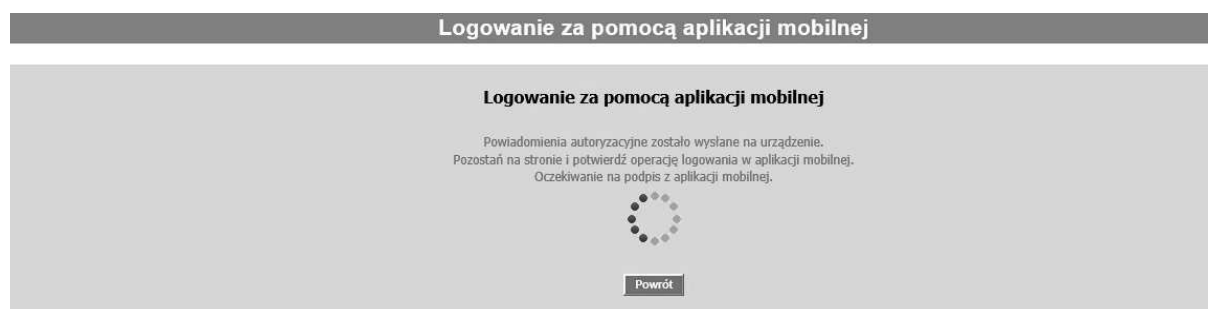


Logowanie do Usługi Bankowości Elektronicznej SGB (korporacyjne) za pomocą aplikacji mobilnej Token SGB

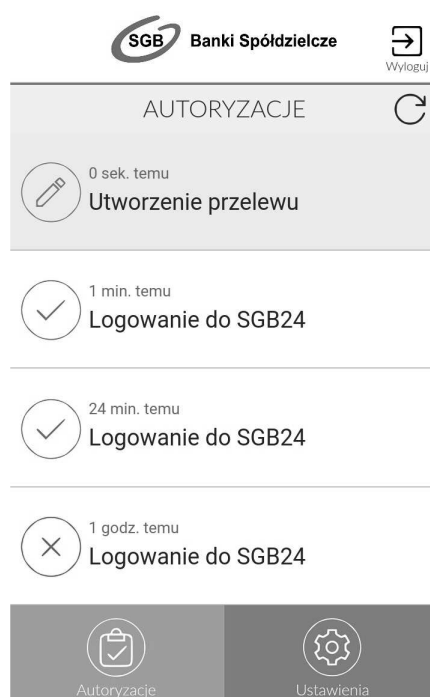
Użytkownik ma możliwość zalogowania się do systemu Usług Bankowości Elektronicznej SGB (korporacyjne) za pomocą aplikacji mobilnej Token SGB, jeżeli posiada sparowane aktywne urządzenie oraz ustanowione przez siebie hasło.

Proces logowania za pomocą aplikacji mobilnej Token SGB jest następujący:

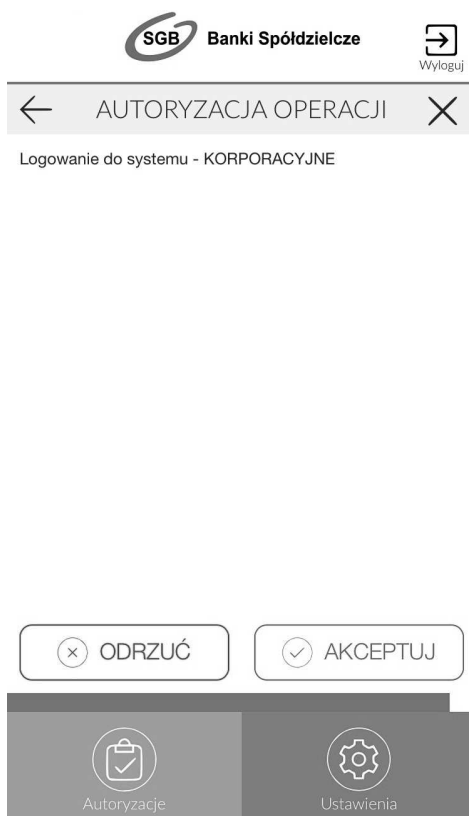
1. Użytkownik wybiera opcję logowania – Logowanie aplikacją mobilną.
2. Wpisuje Identyfikator użytkownika i hasło ustawione w momencie pierwszego logowania po sparowaniu urządzenia lub zmienione w aplikacji i wybiera przycisk [OK].
3. W systemie prezentowany jest ekran informujący o wystaniu dyspozycji logowania do aplikacji mobilnej Token SGB



4. System wysyła do aplikacji mobilnej Token SGB powiadomienie na urządzenie mobilne z informacją o oczekującym powiadomieniu
5. Użytkownik wybiera powiadomienie, które uruchamia aplikację mobilną Token SGB lub bezpośrednio uruchamia aplikację z systemu operacyjnego urządzenia mobilnego.
6. Użytkownik loguje się do aplikacji mobilnej Token SGB.
7. Aplikacja mobilna Token SGB prezentuje dane dyspozycji logowania.



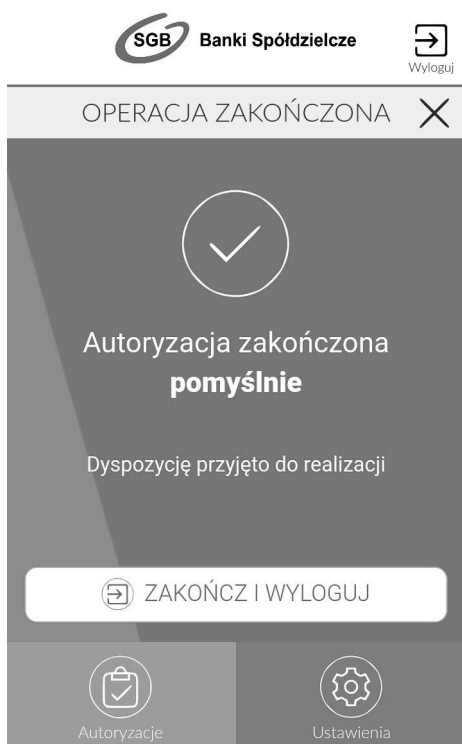
8. Użytkownik weryfikuje wyświetlone dane oraz potwierdza realizację dyspozycji logowania.



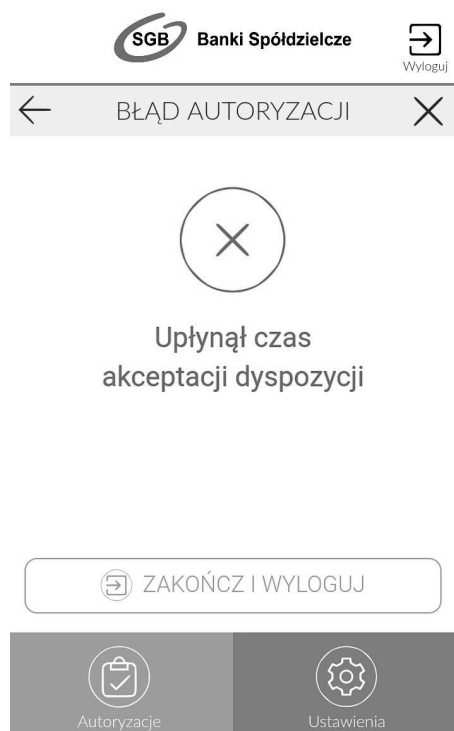
9. System po wprowadzeniu PIN-u przez Użytkownika weryfikuje pozytywnie wejście do aplikacji mobilnej Token SGB.

10. Użytkownik zostaje zalogowany do systemu.

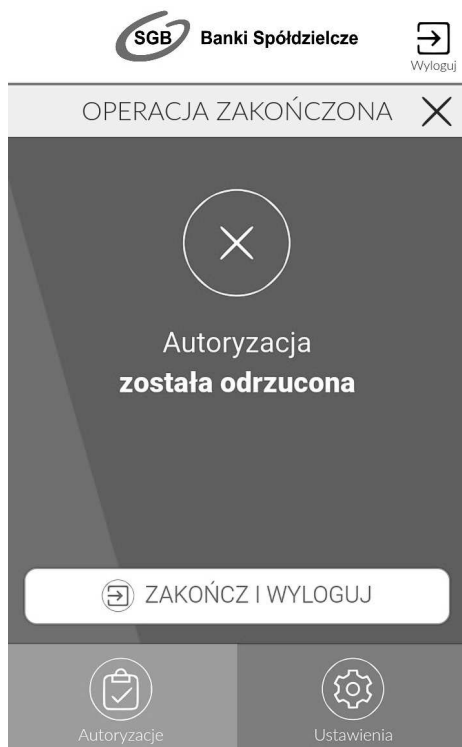
11. Aplikacja mobilna Token SGB prezentuje potwierdzenie autoryzacji dyspozycji.



W przypadku, gdy użytkownik nie podpisał dyspozycji w określonym czasie po wskazaniu dyspozycji w aplikacji mobilnej Token SGB zostanie zaprezentowany komunikat informujący o błędnej akceptacji.



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



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

- braku podpisania dyspozycji w określonym czasie,
- odrzucenia autoryzacji w aplikacji mobilnej Token SGB w systemie jest wyświetlony komunikat:

Logowanie za pomocą aplikacji mobilnej

Logowanie za pomocą aplikacji mobilnej

Powiadomienia autoryzacyjne zostało wysłane na urządzenie.
Pozostań na stronie i potwierdź operację logowania w aplikacji mobilnej.
Oczekiwanie na podpis z aplikacji mobilnej.

Błąd logowania za pomocą aplikacji mobilnej

Powrót

Urządzenia autoryzujące

Wybranie opcji Urządzenia autoryzujące umożliwia użytkownikowi: sparowanie aplikacji mobilnej Token SGB z systemem, podgląd listy urządzeń sparowanych z systemem (włącznie z historycznymi urządzeniami), dezaktywację aplikacji mobilnej Token SGB.

Tabele Konfiguracja Hasła Komunikaty **Urządzenia autoryzujące** Wylogowanie

Wybór nazwy urządzenia z listy umożliwia wyświetlenie szczegółów dot. wskazanego urządzenia autoryzacyjnego.

Urządzenia autoryzujące - szczegóły

| | |
|-----------------------------|------------------|
| Nazwa urządzenia: | test |
| Producent: | samsung |
| Platforma: | ANDROID |
| Wersja: | 7.0 |
| Model: | SM-G920F |
| Data powiązania: | 2018-06-29 09:30 |
| Status: | Aktywne |
| <p>Dezaktywuj Zrezygnuj</p> | |

Dodatkowo na formatce Urządzenie autoryzujące - szczegóły dostępne są przyciski funkcyjne:

[Dezaktywuj] - przycisk umożliwia dezaktywację urządzenia mobilnego, przycisk jest widoczny dla urządzeń o statusie: Aktywne

[Zrezygnuj] - powoduje zamknięcie okna Urządzenie autoryzujące – szczegóły.

Dezaktywacja urządzenia powoduje usunięcie tego urządzenia w systemie. Po poprawnej dezaktywacji, urządzenie zostanie zaprezentowane na liście urządzeń autoryzujących ze statusem Nieaktywne.

Ponowne użycie urządzenia wymaga ponownego sparowania urządzenia.

Opcja Zmień hasło aplikacji mobilnej Token SGB umożliwia zmianę hasła do aplikacji mobilnej Token SGB, za pomocą którego użytkownik loguje się w systemie.

W celu zmiany hasła do aplikacji mobilnej Token SGB, należy wpisać aktualnie obowiązujące hasło a następnie dwukrotnie nowe hasło i zatwierdzić poprzez przycisk [Zmień].

Zmień hasło aplikacji mobilnej

| | |
|---|----------------------|
| Stare hasło | <input type="text"/> |
| Nowe hasło | <input type="text"/> |
| Powtórz nowe hasło | <input type="text"/> |
| <input type="button" value="Zmień"/> <input type="button" value="Zrezygnuj"/> | |