



Token mobilny – Asseco MAA

Przewodnik dla użytkownika

Bankowości elektronicznej Bank Spółdzielczego w Kórniku(Asseco EBP)

Spis treści

Zasady bezpiecznego korzystania z Usługi Bankowości Internetowej Banku Spółdzielczego w Kórniku	3
Podstawowe zasady bezpieczeństwa	3
Szyfrowa transmisja danych	3
Automatyczne wylogowanie.....	4
Blokada	4
Limity transakcji	4
Zastrzeżenie środków dostępu	4
Logowanie do Usługi Bankowości Internetowej BANKU SPÓŁDZIELCZEGO W KÓRNIKU	4
Korzystanie z Usługi Bankowości Internetowej BANKU SPÓŁDZIELCZEGO W KÓRNIKU	5
Identyfikator ID	6
Aplikacja Mobilna Token Mobilny- Asseco MAA	6
Autoryzacja	6
(autoryzującego) podczas pierwszego logowania do Bankowości Internetowej	7
Lista dyspozycji do autoryzacji w aplikacji mobilnej Token Mobilny- Asseco MAA.....	15

Zasady bezpiecznego korzystania z Usługi Bankowości Internetowej

Bank Spółdzielczego w Kórniku

Po pierwsze bezpieczeństwo!

Przy projektowaniu i budowie Usługi Bankowości Internetowej 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 Mobilny- Asseco MAA 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 Bank Spółdzielczego w Kórniku.pl. po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Bank Spółdzielczego w Kórniku.pl przez firmę DigiCert
- Uważnie czytaj treść w wiadomości SMS / aplikacji Token Mobilny- Asseco MAA Przed potwierdzeniem transakcji sprawdzaj treść operacji jej kwotę oraz poprawność numeru rachunku odbiorcy.
- Nie otwieraj załączników z niepewnych źródeł i nie klikaj w podejrzane linki.
- 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.bs.kornik.sgb.pl/Bezpieczenstwo-transakcji-elektronicznych.html>

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 kilku błędnych prób zalogowania się do Usługi Bankowości Internetowej BS W KÓRNIKU następuje automatyczna blokada konta danego Użytkownika, która chroni konto przed dostępem osób nieupoważnionych. W celu odblokowania konta należy skontaktować się z bankiem pod nr 48618170401 lub do wybranej placówki banku a po godzinach pracy pod numerem 48618170591(odsluchamy w następnym dniu roboczym od godziny 8:00)lub odwiedzić najbliższą placówkę Banku.

Limity transakcji

Przed aktywacją Usługi Bankowości Internetowej BANK SPÓŁDZIELCZEGO W KÓRNIKU 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 Bank Spółdzielczego w Kórniku

- 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 BANK SPÓŁDZIELCZEGO W KÓRNIKU
- 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 Bank Spółdzielczego w Kórniku.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 Bank Spółdzielczego w Kórniku.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 bankiem pod nr 48618170401 lub do wybranej placówki banku a po godzinach pracy pod numerem 48618170591 (odsłuchamy w następnym dniu roboczym od godziny 8:00)**
- Jeśli przy logowaniu pojawi się **nietypowy** komunikat lub prośba o podanie danych osobowych, haseł lub ich aktualizację, należy przerwać logowanie i skontaktować się **bankiem pod nr 48618170401 lub do wybranej placówki banku a po godzinach pracy pod numerem 48618170591 (odsłuchamy w następnym dniu roboczym od godziny 8:00)**
- 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 Korzystanie z Usługi Bankowości Internetowej BANK SPÓŁDZIELCZEGO W KÓRNIKU
- **bankiem pod nr 48618170401 lub do wybranej placówki banku a po godzinach pracy pod numerem 48618170591 (odsłuchamy w następnym dniu roboczym od godziny 8:00)**
 - Po zalogowaniu się do Usługi Bankowości Internetowej BANK SPÓŁDZIELCZEGO W KÓRNIKU należy zostawiać komputera bez opieki
 - Korzystając z Usługi Bankowości Internetowej BANK SPÓŁDZIELCZEGO W KÓRNIKU 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 BANK SPÓŁDZIELCZEGO W KÓRNIKU należy używać klawiszy nawigacyjnych przeglądarki internetowej (np. Wstecz, Dalej, Odśwież), system posiada własne klawisze, które umożliwiają sprawne poruszanie się w ramach Usług Bankowości Internetowej BANK SPÓŁDZIELCZEGO W KÓRNIKU
 - 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 – 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 BANK SPÓŁDZIELCZEGO W KÓRNIKU w miejscach ogólnie dostępnych, np. w kawiarenkach internetowych lub poprzez publiczne (niezabezpieczone) sieci bezprzewodowe

Usługa Bankowości Internetowej Bank Spółdzielczego w Kórniku

Bankowość Internetowa Bank Spółdzielczego w Kórniku 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 Bank Spółdzielczego w Kórniku 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 Mobilny- Asseco MAA

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.

Logowanie

- Identyfikator ID + aplikacja Token Mobilny- Asseco MAA (wraz z PINem do aplikacji Token Asseco MAA)

Autoryzacja

- Aplikacja mToken Asseco MAA
- **Uwaga!** W przypadku utraty urządzenia mobilnego należy niezwłocznie zastrzec dostęp do usługi zgłaszając ten fakt w bankiem pod nr 48618170401 lub do wybranej placówki banku a po godzinach pracy pod numerem 48618170591 (odsluchamy w następnym dniu roboczym od godziny 8:00)

. Należy pamiętać również, by w przypadku zmiany numeru telefonu zgłosić ten fakt do Banku.

Środki dostępu służą zarówno do logowania do Usługi Bankowości Internetowej BANK SPÓŁDZIELCZEGO W KÓRNIKU, jak i do autoryzacji zleceń w systemie dyspozycji.

Wymagania Sprzętowe dla aplikacji mobilnej

➤ Aplikacja mToken Asseco MAA
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 Bank Spółdzielczego w Kórniku

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 mToken Asseco MAA
 - . 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 mToken Asseco MAA 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,

SGB Spółdzielcza Grupa Bankowa

Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator użytkownika

Nowe hasło
Wpisz hasło

Powtórz nowe hasło
Wpisz ponownie nowe hasło

DALEJ

Zadbaj o zachowanie poufności swojego hasła. Nie udostępniaj hasła innym osobom, na żadnych stronach internetowych, pocztą elektroniczną, wiadomością SMS lub w odpowiedzi na żądania otrzymane od pracowników banku.

Definiując swoje hasło pamiętaj o zachowaniu zasad bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

Zasady budowy haseł są następujące:

- o musi składać się z 8-20 znaków
- o musi zawierać przynajmniej jedną wielką literę
- o musi zawierać przynajmniej jedną małą literę
- o musi zawierać przynajmniej jedną cyfrę

Po wprowadzeniu hasła Użytkownik wybiera przycisk **[DALEJ]**.

3. Użytkownik wpisuje dowolną nazwę urządzenia i wybiera przycisk **[DALEJ]**

- Użytkownik uruchamia aplikację mToken Asseco MAA
- i prezentowany kod aktywacyjny wprowadza w mToken Asseco MAA

4.

SGB Spółdzielcza Grupa Bankowa

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:

- Użytkownik nadaje PIN do logowania w aplikacji mToken Asseco MAA
6. :

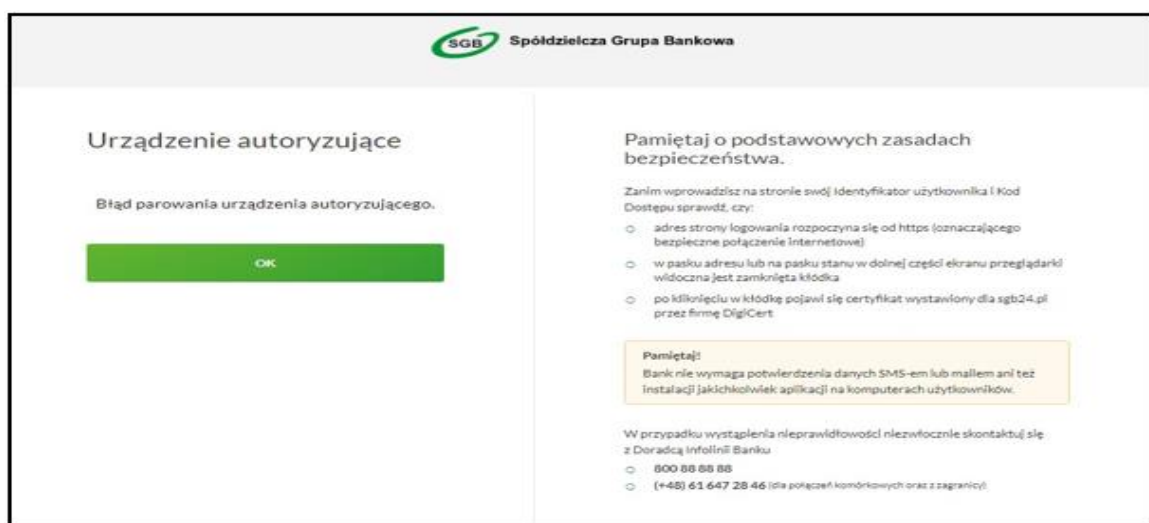
7. Po poprawnym sparowaniu urządzenia Użytkownikowi wyświetlony jest komunikat potwierdzający dodanie urządzenia:

- w aplikacji mToken Asseco MAA
- :



- 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:

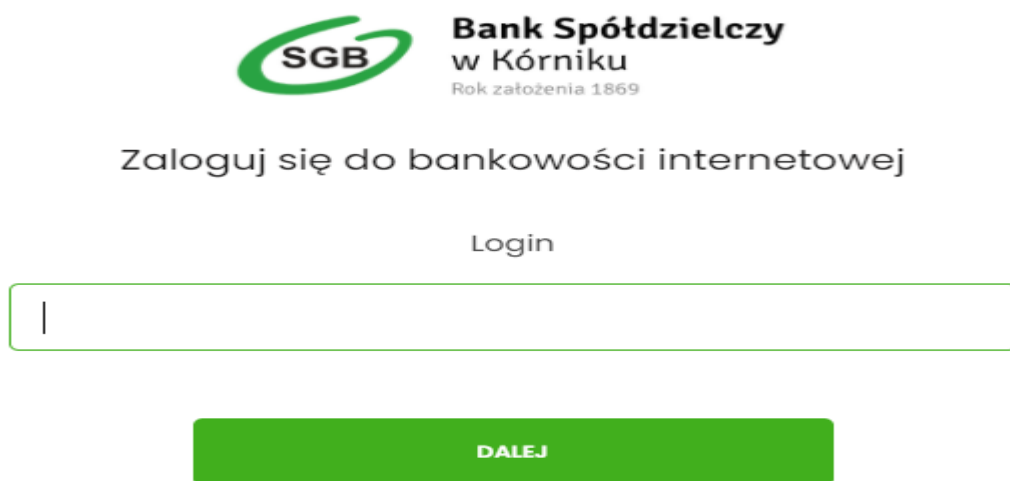


Logowanie do systemu Bankowości Internetowej za pomocą aplikacji mobilnej mToken Asseco MAA

Użytkownik ma możliwość zalogowania do systemu bankowości elektronicznej za pomocą aplikacji mobilnej mToken Asseco MAA jeżeli posiada aktywne urządzenie oraz ustanowione przez siebie hasła. Proces logowania za pomocą aplikacji mobilnej mToken Asseco MAA jest następujący :

W polu Identyfikator Użytkownik wprowadza identyfikator ID nadany przez Bank i wybiera opcję **DALEJ** , a następnie w polu **HASŁO** (w postaci maskowanej) wprowadza hasło do logowania i wybiera przycisk **ZALOGUJ**

1.



SGB Bank Spółdzielczy
w Kórniku
Rok założenia 1869

Zaloguj się do bankowości internetowej

Login

DALEJ

2.



SGB Bank Spółdzielczy
w Kórniku
Rok założenia 1869

Zaloguj się do bankowości internetowej

Wpisz wskazane znaki hasła dla KO3E5CCNO

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

ZALOGUJ

ANULUJ

3.

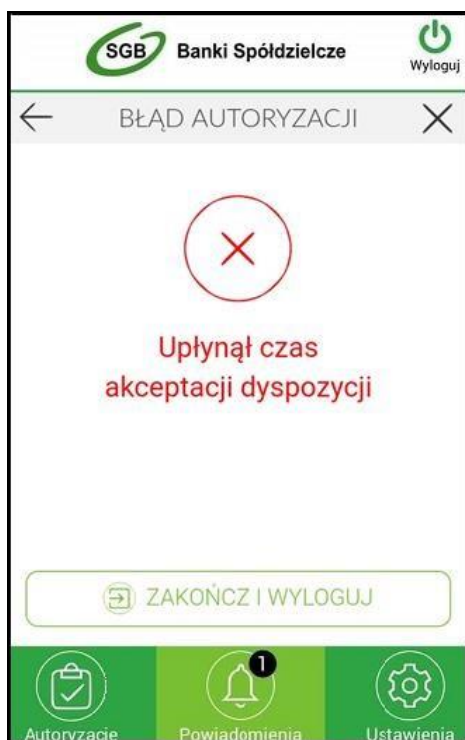
Użytkownik weryfikuje wyświetlone dane oraz potwierdza realizację dyspozycji logowania wybierając opcję [AKCEPTUJ].



4. Aplikacja mToken Asseco MAA wysyła podpisaną dyspozycję do systemu.
5. Użytkownik zostaje zalogowany do systemu Bankowości Internetowej.
6. Aplikacja mToken Asseco MAA prezentuje potwierdzenie autoryzacji logowania.



7. W przypadku, gdy Użytkownik nie autoryzował dyspozycji w określonym czasie po wskazaniu dyspozycji w aplikacji mToken Asseco MAA zostanie zaprezentowany komunikat informujący o braku akceptacji.



8. W przypadku odrzucenia autoryzacji w aplikacji mToken Asseco MAA , prezentowany jest komunikat:







9. W przypadku, gdy logowanie do Bankowości Internetowej nie powiodło się z powodu:
- braku autoryzacji dyspozycji w określonym czasie,
 - odrzucenia autoryzacji w aplikacji mobilnej mToken Asseco MAA, 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




Lista dyspozycji do autoryzacji w aplikacji mobilnej Token Mobilny-Asseco MAA

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 Mobilny- Asseco MAA 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.