

Rozdział 18. Urządzenia autoryzujące

W przypadku, gdy wartość usługi **AUTORYZACJA_MOBILNA** ustawiona jest na *T*, w systemie def3000/CEB w menu głównym aplikacji dostępna jest opcja *Urządzenia autoryzujące*.

Użytkownik po włączeniu usługi ma możliwość:

- autoryzacji dyspozycji metodą aplikacja mobilna Asseco MAA,
- sparowania aplikacji z systemem,
- podglądu listy aplikacji sparowanych z systemem,
- dezaktywacji aplikacji mobilnej.



Formatka *Urządzenia autoryzujące* prezentuje następujące informacje:

- **Nazwa urządzenia**,
- **Data powiązania** - data i godzina sparowania urządzenia,
- **Status** - dostępne wartości:
 - *Aktywny*,
 - *Nieaktywny*,
 - *Zablokowany*,
 - *Usunięty*,
 - *Zakończony*,
 - *Czeka na akceptację Administratora*,
 - *Zaakceptowany przez Administratora*,
 - *Odrzucony przez Administratora*.

Urządzenia autoryzujące			
☐ Dodaj urządzenie autoryzujące			
Nazwa urządzenia	Data powiązania	Status	
test	2017-10-27 12:46:08	Aktywny	
test2	2017-10-27 10:47:24	Usunięty	
test3	2017-10-27 09:34:51	Odrzucony przez Administratora	

Na liście urządzeń autoryzujących prezentowane są urządzenia o statusie: *Aktywny*, *Nieaktywny*, *Zablokowany*, *Usunięty*, *Zakończony*, *Czeka na akceptację Administratora*, *Zaakceptowany przez Administratora* oraz *Odrzucony przez Administratora*. Lista jest posortowana malejąco według daty powiązania.

Kliknięcie w nazwę urządzenia na liście spowoduje otwarcie formatki *Urządzenie autoryzujące - szczegóły*, która zawiera następujące informacje:

- **Nazwa urządzenia**,
- **Producent**,
- **Platforma**,
- **Wersja**,
- **Model**,
- **Data powiązania** - data i godzina sparowania z systemem,
- **Status** - dostępne wartości:

- Aktywny,
- Nieaktywny,
- Zablokowany,
- Usunięty,
- Zakończony,
- Czeka na akceptację Administratora,
- Zaakceptowany przez Administratora,
- Odrzucony przez Administratora.

Urządzenie autoryzujące - szczegóły

Nazwa urządzenia:	test
Producent:	HTC
Platforma:	ANDROID
Wersja:	4.4.3
Model:	HTC Desire 510
Data powiązania:	2017-07-17 14:45:08
Status:	Aktywny

Dezaktywuj
Zrezygnuj

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

- [Dezaktywuj] - przycisk umożliwia dezaktywację urządzenia mobilnego, przycisk jest widoczny dla urządzeń o statusie: *Aktywny* oraz *Zablokowany*,
- [Zrezygnuj] - powoduje zamknięcie okna *Urządzenie autoryzujące - szczegóły*.

Operacja dezaktywacji urządzenia autoryzującego wymaga potwierdzenia.

Urządzenie autoryzujące - dezaktywacja urządzenia

Nazwa urządzenia:	test
Producent:	samsung
Platforma:	ANDROID
Wersja:	7.0
Model:	SM-G920F
Data powiązania:	2017-11-02 08:12:18
Status:	Aktywny

Dezaktywuj urządzenie autoryzujące
Zamknij

Formatka potwierdzenia dezaktywacji urządzenia zawiera przyciski:

- [Dezaktywuj urządzenie autoryzujące] - dezaktywacja urządzenia autoryzującego,
- [Zamknij] - rezygnacja z dezaktywacji urządzenia i powrót na formatkę *Urządzenia autoryzujące*.

Urządzenie autoryzujące - szczegóły

Nazwa urządzenia:	test
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2017-11-08 12:46:49
Status:	Odrzucony przez Administratora

Usuń
Zrezygnuj

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

- [Usuń] - przycisk umożliwia usunięcie urządzenia mobilnego, przycisk jest widoczny dla urządzeń o statusie: *Czeka na akceptację przez Administratora*, *Zaakceptowany przez Administratora* oraz *Odrzucony przez Administratora*,
- [Zrezygnuj] - powoduje zamknięcie okna *Urządzenie autoryzujące - szczegóły*,
- [Dokończ dodawanie urządzenia] - przycisk dostępny tylko w statusie *Zaakceptowany przez Administratora*, który umożliwia dokończenie procesu [parowania urządzenia](#).

Operacja usunięcia urządzenia autoryzującego wymaga potwierdzenia.

Urządzenie autoryzujące - usuwanie urządzenia

Nazwa urządzenia:	test
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2017-11-08 12:46:49
Status:	Odrzucony przez Administratora

Usuń urządzenie autoryzujące

Zamknij

Formatka potwierdzenia usunięcia urządzenia zawiera przyciski:

- [Usuń urządzenie autoryzujące] - usunięcie urządzenia autoryzującego,
- [Zamknij] - rezygnacja z usunięcia urządzenia i powrót na formatkę *Urządzenia autoryzujące*.

Dezaktywacja urządzenia powoduje odwiązanie urządzenia autoryzującego od systemu def3000/CEB. Po poprawnej dezaktywacji, urządzenie zostanie zaprezentowane na liście urządzeń autoryzujących ze statusem *Nieaktywny*.

Urządzenia autoryzujące			
Dodaj urządzenie autoryzujące			
Nazwa urządzenia	Data powiązania	Status	
test	2017-11-02 08:12:18	Nieaktywny	

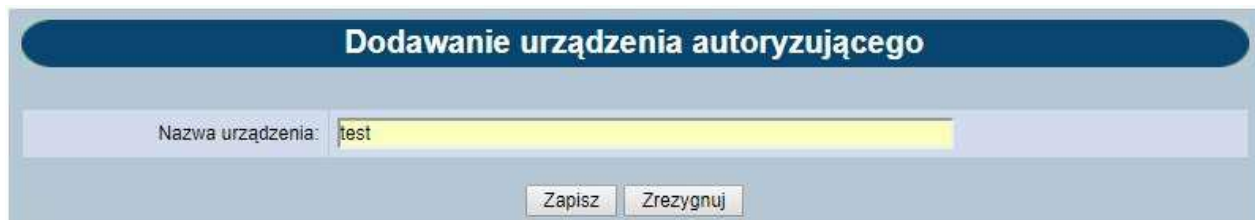
Ponowne użycie urządzenia wymaga ponownego sparowania urządzenia.

18.1. Parowanie urządzenia autoryzującego

W celu sparowania urządzenia autoryzującego należy wybrać opcję *Dodaj urządzenie autoryzujące* dostępną nad listą urządzeń na formatce *Urządzenia autoryzujące*.

Urządzenia autoryzujące			
Dodaj urządzenie autoryzujące			
Nazwa urządzenia	Data powiązania	Status	

Kliknięcie w opcję *Dodaj urządzenie autoryzujące* spowoduje otwarcie formularza do wprowadzenia nazwy urządzenia autoryzującego w polu **Nazwa urządzenia**.



Po nadaniu nazwy urządzenia i kliknięciu na przycisk [Zapisz] konieczne jest wykonanie autoryzacji dyspozycji sparowania aplikacji z systemem obecnie posiadaną przez Użytkownika metodą autoryzacji (np. karta mikroprocesorowa lub token VASCO).



W kolejnym kroku po wyborze przycisku [Podpisz] system def3000/CEB za pośrednictwem systemu GUARDIAN generuje oraz prezentuje użytkownikowi kod parowania urządzenia autoryzującego oraz komunikat jakie dane będą wymagane do wprowadzenia przez użytkownika w aplikacji mobilnej Asseco MAA w celu potwierdzenia parowania. Dodatkową daną wymaganą w procesie parowania jest kod weryfikacyjny wysyłany za pomocą SMS. Kod parowania posiada termin ważności. Po przekroczeniu terminu ważności kodu parowania jego użycie nie jest możliwe. W przypadku, gdy użytkownik ma w systemie BankAdmin ustawioną inną metodę autoryzacji niż aplikacja mobilna (np. dodał aplikacja mobilna a obecnie posiada token RSA) to system zaprezentuje komunikat o konieczności kontaktu z bankiem w celu zmiany metody autoryzacji.

Dodawanie urządzenia autoryzującego

Kod aktywacyjny: **407624**

W celu dokończenia procesu aktywacji, wygenerowany kod wprowadź w urządzeniu autoryzującym: **test**.

W trakcie aktywowania usługi w urządzeniu mobilnym zostaniesz poproszona/poproszony o podanie kodu weryfikacyjnego, który zostanie wysłany za pomocą SMS na numer: **048500256999**.

Kod jest ważny przez 5 minut.

W celu aktywowania mobilnej autoryzacji skontaktuj się z nami.

Pozostań na stronie i dokończ proces aktywacji na urządzeniu autoryzującym.



Oczekiwanie na zakończenie procesu aktywacji.

Zamknij

Po poprawnym sparowaniu urządzenie prezentowane jest na liście ze statusem *Aktywny*.

Urządzenia autoryzujące		
☐ Dodaj urządzenie autoryzujące		
Nazwa urządzenia	Data powiązania	Status
test	2017-07-17 14.45.08	Aktywny

Sparowanie nowego urządzenia autoryzującego możliwe jest w przypadku, kiedy na liście nie znajduje się urządzenie w statusie:

- *Aktywny*,
- *Czeka na akceptację Administratora*,
- *Zaakceptowany przez Administratora*.

Sparowanie systemu z innym urządzeniem wymaga [dezaktywacji/usunięcia urządzenia](#) poprzedniego.

Na formatce parowania następuje weryfikacja, czy użytkownik ma już dodane urządzenie, jeśli tak to dla użytkownika wyświetlany jest komunikat:

Na liście jest już dodane urządzenie autoryzujące w statusie: Aktywny, Czekając na akceptację Administratora lub Zaakceptowany przez Administratora.
Aby dodać nowe urządzenie należy usunąć poprzednie z listy.

OK

W przypadku, gdy użytkownik nie posiada przypisanej metody autoryzacji (np. karta mikroprocesorowa lub token VASCO) a ma przypisaną metodę autoryzacji aplikacja mobilna to sparowanie aplikacji będzie wymagało potwierdzenia przez Administratora Klienta korporacyjnego.

Dodawanie urządzenia autoryzującego

Nazwa urządzenia:

test

Zapisz

Zrezygnuj

Po nadaniu nazwy urządzenia i kliknięciu na przycisk [Zapisz] zaprezentowany zostanie komunikat.

Dodawanie urządzenia autoryzującego

Dodanie urządzenia autoryzującego wymaga potwierdzenia przez Administratora Klienta korporacyjnego (brak aktywnego środka autoryzującego).

Zamknij

Po poprawnym dodaniu urządzenie na liście zostanie zaprezentowane ze statusem *Czekając na akceptację Administratora*, gdzie Administrator musi [zaakceptować/odrzuć urządzenie autoryzujące](#).

Urządzenia autoryzujące

☐ Dodaj urządzenie autoryzujące

Nazwa urządzenia	Data powiązania	Status
test	2017-08-10 11:45:06	Czekając na akceptację Administratora

Po odrzuceniu urządzenia przez Administratora, urządzenie zostanie zaprezentowane na liście ze statusem *Odrzucony przez Administratora*.

Urządzenia autoryzujące

☐ Dodaj urządzenie autoryzujące

Nazwa urządzenia	Data powiązania	Status
test	2017-08-10 14:38:59	Odrzucony przez Administratora

Po poprawnym zaakceptowaniu urządzenia przez Administratora urządzenie otrzyma status *Zaakceptowany przez Administratora*.

Urządzenia autoryzujące		
Dodaj urządzenie autoryzujące		
Nazwa urządzenia	Data powiązania	Status
test	2017-08-10 14:16:35	Zaakceptowany przez Administratora

Po wejściu w szczegóły urządzenia na formatce *Urządzenie autoryzujące - szczegóły* dostępne są przyciski funkcyjne:

- [Usuń] - przycisk umożliwiający usunięcie (dezaktywację) urządzenia mobilnego,
- [Zrezygnuj] - powoduje zamknięcie okna *Urządzenie autoryzujące - szczegóły*,
- [Dokończ dodawanie urządzenia] - przycisk dostępny jest tylko w statusie *Zaakceptowany przez Administratora*, przycisk umożliwia dokończenie procesu parowania urządzenia.

Urządzenie autoryzujące - szczegóły	
Nazwa urządzenia:	test
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2017-08-10 14:16:35
Status:	Zaakceptowany przez Administratora
Dokończ dodawanie urządzenia Usuń Zrezygnuj	

Po kliknięciu na przycisk [Dokończ dodawanie urządzenia] nastąpi zaprezentowanie użytkownikowi kodu parowania aplikacji mobilnej Asseco MAA (wygenerowany przez system GUARDIAN) oraz komunikat jakie dane będą wymagane do wprowadzenia przez użytkownika w aplikacji mobilnej Asseco MAA w celu potwierdzenia parowania aplikacji. Dodatkową daną wymaganą w procesie parowania jest kod weryfikacyjny wysyłany za pomocą SMS. Jeżeli użytkownik nie przepisze kodu parowania do aplikacji mobilnej Asseco MAA, to urządzenie otrzymuje status *Zakończony* i jest widoczne z takim statusem na liście urządzeń. Wprowadzenie kodu w aplikacji mobilnej Asseco MAA spowoduje, że urządzenie stanie się aktywne i otrzyma status *Aktywny*.



Do obsługi funkcjonalności dyspozycji za pomocą aplikacji mobilnej konieczne jest pobranie ze sklepu aplikacji mobilnej (Google Play (Android), App Store (iOS)) oraz zainstalowanie na urządzeniu mobilnym. Szczegółowy opis funkcjonalności aplikacji mobilnej Asseco MAA znajduje się w dokumentacji użytkownika dedykowanej dla tego systemu.

18.2. Proces autoryzacji dyspozycji złożonej w systemie def3000/CEB za pomocą aplikacji mobilnej Asseco MAA

Aplikacja mobilna Asseco MAA umożliwia autoryzację dyspozycji (podpisem niekwalifikowanym) złożonej w systemie def3000/CEB. Użytkownik ma możliwość podpisania zlecenia za pomocą obecnie dostępnych metod akceptacji (karta mikroprocesorowa, token VASCO) oraz za pomocą aplikacji mobilnej - podpis niekwalifikowany (nowy sposób autoryzacji). Definiowanie domyślnej metody autoryzacji dyspozycji jest realizowane w systemie BankAdmin. Typ podpisu *aplikacja mobilna* definiujemy w systemie BankAdmin.

Użytkownik po wybraniu dyspozycji oczekującej na autoryzację, przeniesiony zostanie na formularz, na którym zaprezentowane zostaną szczegóły autoryzowanej dyspozycji wraz z możliwością potwierdzenia lub odrzucenia autoryzacji. Dane dyspozycji oczekującej na autoryzację pobierane są z systemu GUARDIAN. Autoryzacja dyspozycji polega na podpisaniu kluczem prywatnym (zapisanym w aplikacji mobilnej Asseco MAA) danych dyspozycji oraz przekazaniu ich do systemu GUARDIAN w celu weryfikacji. Po poprawnym zweryfikowaniu autoryzacji aplikacja mobilna Asseco MAA prezentuje potwierdzenie autoryzacji. W przypadku odrzucenia autoryzacji aplikacja prezentuje komunikat o anulowaniu autoryzacji. Wynik autoryzacji również prezentowany jest w systemie

def3000/CEB. W przypadku przekroczenia dopuszczalnego czasu na autoryzację aplikacja prezentuje [komunikat](#) o przekroczeniu czasu autoryzacji (autoryzacja zlecenia w takim przypadku jest niemożliwa).

Proces autoryzacji dyspozycji za pomocą aplikacji mobilnej Asseco MAA jest następujący:

1. Użytkownik wybiera opcję autoryzacji dyspozycji w systemie def3000/CEB (podpis niekwalifikowany).
2. System def3000/CEB prezentuje ekran informujący o wystaniu dyspozycji do autoryzacji na aplikację mobilną Asseco MAA.

Przelew - akceptowanie

Referencje:	
Rachunek do obciążenia:	22 8707 0006 0001 2830 3000 0007
Nazwa kontrahenta:	Test Rzeszów
Nr rachunku kontrahenta:	36 2030 0045 1110 0000 0255 7250
Kwota:	1,00 PLN
Tytułem:	Faktura VAT nr 0123456789/2018
Droga płatności:	Elxbr
Data:	2017-07-28
Zleceniodawca:	Jan Test

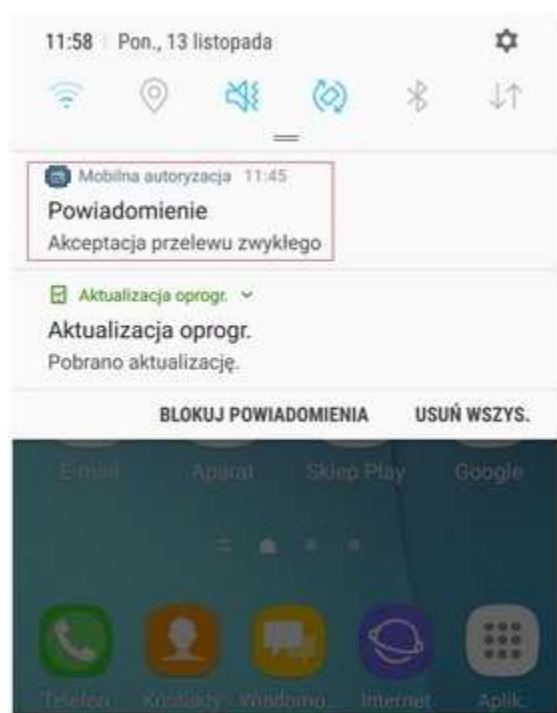
Powiadomienie autoryzacyjne zostało wysłane na urządzenie.
Pozostań na stronie i potwierdź operację w aplikacji mobilnej.



Oczekiwanie na podpis aplikacją mobilną

Zamknij

3. System def3000/CEB za pośrednictwem systemu GUARDIAN wysyła do aplikacji mobilnej Asseco MAA powiadomienie PUSH o nowej dyspozycji do autoryzacji.
4. Aplikacja mobilna Asseco MAA wyświetla na urządzeniu mobilnym baner o powiadomieniu PUSH z informacją o oczekującym powiadomieniu autoryzacyjnym.



5. Użytkownik wybiera baner powiadomienia PUSH, który uruchamia aplikację mobilną Asseco MAA lub bezpośrednio uruchamia aplikację z systemu operacyjnego urządzenia mobilnego.
6. Użytkownik loguje się do aplikacji mobilnej Asseco MAA za pomocą kodu PIN zdefiniowanego przez użytkownika w procesie rejestracji urządzenia autoryzującego.

7. Aplikacja mobilna Asseco MAA pobiera z systemu GUARDIAN dane do autoryzacji.

8. Aplikacja mobilna Asseco MAA prezentuje dane dyspozycji do autoryzacji, w celu przejścia na ekran potwierdzenia operacji należy wybrać przycisk [AKCEPTUJ]. Aplikacja mobilna Asseco MAA prezentuje czas jaki pozostał do potwierdzenia autoryzacji, po upływie którego dyspozycja jest anulowana.

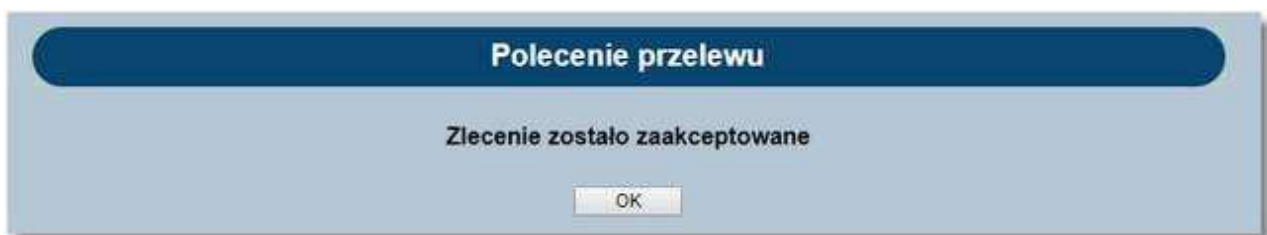


9. W przypadku podjęcia przez użytkownika decyzji o akceptacji transakcji, użytkownik weryfikuje wprowadzone dane oraz potwierdza realizację dyspozycji poprzez wprowadzenie poprawnego kodu PIN (zdefiniowanego przez użytkownika w procesie rejestracji urządzenia autoryzującego) oraz wybór przycisku [ZATWIERDŹ].

The screenshot shows the ASSECO mobile application interface. At the top, there is a header bar with the ASSECO logo on the left and a 'Wyloguj' (Logout) button on the right. Below the header, there is a title bar with a back arrow, the text 'AUTORYZACJA OPERACJI', and a close 'X' button. The main content area is titled 'Podaj PIN' (Enter PIN) and features a text input field with the placeholder 'Wprowadź PIN'. Below the input field is a numeric keypad with digits 1 through 9, 0, and a delete button (represented by a square with an 'X'). At the bottom of the main content area is a button with a checkmark icon and the text 'ZATWIERDŹ' (Confirm). The bottom of the screen features a blue navigation bar with three icons: a clipboard for 'Autoryzacje' (Authorizations), a bell for 'Powiadomienia' (Notifications), and a gear for 'Ustawienia' (Settings).



10. Aplikacja mobilna Asseco MAA podpisuje dyspozycję za pomocą klucza prywatnego.
11. Aplikacja mobilna Asseco MAA wysyła podpisaną dyspozycję do systemu GUARDIAN.
12. System GUARDIAN weryfikuje podpis dyspozycji złożony w aplikacji mobilnej Asseco MAA oraz przekazuje wynik do aplikacji mobilnej Asseco MAA oraz do systemu def3000/CEB (weryfikacja pozytywna).
13. System def3000/CEB prezentuje potwierdzenie autoryzacji dyspozycji.



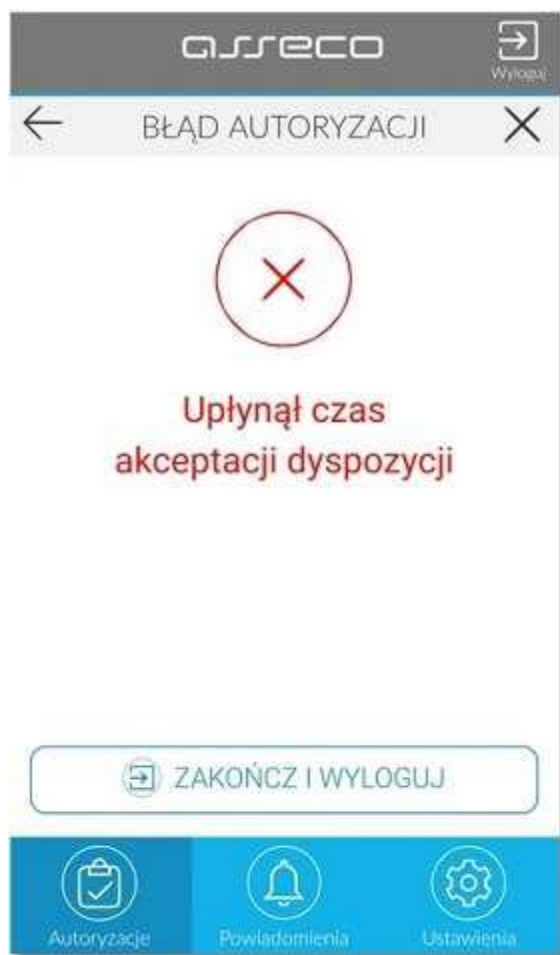
Wybór przycisku [ODRZUĆ] powoduje odrzucenie potwierdzenia autoryzacji i ustawienie statusu dyspozycji na *odrzucona*.



W systemie def3000/CEB zostanie zaprezentowany komunikat o anulowaniu autoryzacji dyspozycji.

Przelew - akceptowanie	
Referencja:	
Rachunek do obciążenia:	22 8707 0006 0001 2830 3000 0007
Nazwa kontrahenta:	Test Rzeszów
Nr rachunku kontrahenta:	36 2030 0045 1110 0000 0255 7250
Kwota:	1,00 PLN
Tytułem:	Faktura VAT nr 0123456789/2018
Droga płatności:	Elbix
Data:	2017-07-28
Zlecająca:	Jan Test
Dyspozycja autoryzacji została odrzucona w aplikacji mobilnej	
Zamknij	

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



W systemie def3000/CEB na ekranie dyspozycji prezentowany jest komunikat informujący o anulowaniu autoryzacji.

Przelew - akceptowanie

Referencja:	
Rachunek do obciążenia:	22 8707 0006 0001 2830 3000 0007
Nazwa kontrahenta:	Test Rzeszów
Nr rachunku kontrahenta:	36 2030 0045 1110 0000 0255 7250
Kwota:	1,00 PLN
Tytułem:	Faktura VAT nr 0123456789/2018
Droga płatności:	Elbix
Data:	2017-07-28
Zleciłodawca:	Jan Test

Upłynął czas oczekiwania na podpis aplikacją mobilną

Zamknij

W przypadku braku aktywnej aplikacji mobilnej Asseco MAA zostanie zaprezentowany komunikat.

Przelew - akceptowanie

Referencja:	
Rachunek do obciążenia:	22 8707 0006 0001 2830 3000 0007
Nazwa kontrahenta:	Test Rzeszów
Nr rachunku kontrahenta:	36 2030 0045 1110 0000 0255 7250
Kwota:	1,00 PLN
Tytułem:	Faktura VAT nr 0123456789/2018
Droga płatności:	Elbix
Data:	2017-07-28
Zleciłodawca:	Jan Test

Brak aktywnego urządzenia mobilnego

Zamknij

Wybranie opcji autoryzacji dyspozycji, np. przejście do formularza autoryzacji dyspozycji aplikacją mobilną Asseco MAA (podpis niekwalifikowany), powoduje, że dyspozycja przekazywana jest do autoryzacji do aplikacji mobilnej Asseco MAA. Zamknięcie formularza autoryzacji dyspozycji nie spowoduje przerwania realizacji tej dyspozycji (np. dla przelewu dyspozycja zostanie zrealizowana). Wyjątek stanowią dyspozycje, np. import kontrahentów, gdzie import jest realizowany po akceptacji. Dla takiego typu dyspozycji zlecenie autoryzacji zostanie przekazane do aplikacji mobilnej Asseco MAA, ale zamknięcie formularza autoryzacji spowoduje przerwanie akcji związanych z jej realizacją - import kontrahentów nie zostanie wykonany.

Dyspozycje, dla których zamknięcie formularza na etapie autoryzacji spowoduje przerwanie jej realizacji:

- Import kontrahentów,
- Dodanie kontrahenta- szablon,

- Przelewy zbiorcze - akceptacja pojedynczo,
- Przelewy zbiorcze - akceptacja razem,
- Przelewy zbiorcze - usuwanie,
- Wysyłanie plików do banku,
- Usuwanie przelewów,
- Akceptacja szablonu przelewów,
- Akceptacja przelewów/paczek - razem,
- Akceptacja przelewów/paczek - pojedynczo,
- Usuwanie paczki przelewów,
- Przelew zagraniczny - szablon,
- Zlecenia otwarte.

18.3. Lista urzędzeń autoryzujących

Użytkownik posiadający uprawnienia administratora po wejściu w opcję *Urządzenia autoryzujące* dostępne ma do wyboru 2 linki:

- [Lista urzędzeń autoryzujących](#) - [lista urzędzeń](#) (kliknięcie w link spowoduje dodanie linku [Dodaj urządzenie autoryzujące](#)),



- [Lista urzędzeń autoryzujących - administracja](#) - lista urzędzeń do akceptacji/odrzućenia przez Administratora.



Lista urzędzeń autoryzujących prezentuje urządzenia przypisane do użytkownika. Na liście wyświetlane są urządzenia o statusie:

- Aktywny,
- Nieaktywny,
- Zablokowany,
- Usunięty,
- Zakończony,
- Czeka na akceptację Administratora,
- Zaakceptowany przez Administratora,
- Odrzucony przez Administratora.

Lista jest posortowana malejąco według daty powiązania.

Lista zawiera następujące informacje:

- **Nazwa urządzenia**,
- **Data powiązania** - data i godzina sparowania urządzenia,
- **Status** - dostępne wartości:
 - Aktywny,
 - Nieaktywny,
 - Zablokowany,
 - Usunięty,

- Zakończony,
- Czekając na akceptację Administratora,
- Zaakceptowany przez Administratora,
- Odrzucony przez Administratora.

Przykładowy wygląd Listy urządzeń autoryzujących - administracja.

Urządzenia autoryzujące - administracja			
☐ Lista urządzeń autoryzujących	☐ Lista urządzeń autoryzujących - administracja		
Nazwa urządzenia	Data powiązania	Status	
test	2017-10-26 13:39:36	Odrzucony przez Administratora	
test2	2017-10-27 09:58:01	Zaakceptowany przez Administratora	

Przykładowy wygląd Listy urządzeń autoryzujących.

Urządzenia autoryzujące			
☐ Dodaj urządzenie autoryzujące			
Nazwa urządzenia	Data powiązania	Status	
test	2017-10-27 12:46:08	Aktywny	
test2	2017-10-27 10:47:24	Usunięty	
test3	2017-10-27 09:34:51	Odrzucony przez Administratora	

Kliknięcie w nazwę urządzenia na liście spowoduje otwarcie formatki *Urządzenie autoryzujące - szczegóły*, która zawiera następujące informacje:

- **Nazwa urządzenia**,
- **Producent**,
- **Platforma**,
- **Wersja**,
- **Model**,
- **Data powiązania** - data i godzina sparowania z systemem,
- **Status** - dostępne wartości:
 - Aktywny,
 - Nieaktywny,
 - Zablokowany,
 - Usunięty,
 - Zakończony,
 - Czekając na akceptację Administratora,
 - Zaakceptowany przez Administratora,
 - Odrzucony przez Administratora.

Przykładowy wygląd formatki *Urządzenie autoryzujące - szczegóły* dla urządzenia o statusie Aktywny.

Urządzenie autoryzujące - szczegóły

Nazwa urządzenia:	test
Producent:	HTC
Platforma:	ANDROID
Wersja:	4.4.3
Model:	HTC Desire 510
Data powiązania:	2017-07-17 14:45:08
Status:	Aktywny

Dezaktywuj
Zrezygnuj

Przykładowy wygląd formatki *Urządzenie autoryzujące - szczegóły* dla urządzenia o statusie *Zaakceptowany przez Administratora*.

Urządzenie autoryzujące - szczegóły

Nazwa urządzenia:	test
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2017-08-10 14:16:35
Status:	Zaakceptowany przez Administratora

Dokończ dodawanie urządzenia
Usuń
Zrezygnuj

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

- [Usuń] - przycisk umożliwiający usunięcie (dezaktywację) urządzenia mobilnego,
- [Zrezygnuj] - powoduje zamknięcie okna *Urządzenie autoryzujące - szczegóły*,
- [Dokończ dodawanie urządzenia] - przycisk dostępny tylko w statusie *Zaakceptowany przez Administratora*, przycisk umożliwia dokończenie procesu parowania urządzenia.

Lista urządzeń autoryzujących - administracja prezentuje urządzenia o statusie:

- *Czeka na akceptację Administratora*,
- *Zaakceptowany przez Administratora*,
- *Odrzucony przez Administratora*.

Lista jest posortowana rosnąco według daty powiązania.

Urządzenia będą widoczne dla wszystkich Administratorów Klienta korporacyjnego. W przypadku urządzenia do akceptacji wymagane jest potwierdzenie jednego Administratora. Akceptacja aplikacji mobilnej Asseco MAA przez Administratora wymagała będzie posiadania przez niego metody autoryzacji (np. karta mikroprocesorowa, token VASCO lub aplikacja mobilna). Administrator nie będzie miał możliwości zaakceptować/odrzuć w opcji administracji swojego urządzenia - będzie musiał zrobić to inny Administrator.

Lista zawiera następujące informacje:

- **Nazwa urządzenia**,
- **Data powiązania** - data i godzina sparowania urządzenia,
- **Status** - dostępne wartości to:
 - *Czeka na akceptację Administratora*,
 - *Zaakceptowany przez Administratora*,
 - *Odrzucony przez Administratora*.

Urządzenia autoryzujące - administracja			
Lista urządzeń autoryzujących		Lista urządzeń autoryzujących - administracja	
Nazwa urządzenia	Data powiązania	Status	
test	2017-10-26 13:39:36	Odrzucony przez Administratora	
test2	2017-10-27 09:58:01	Zaakceptowany przez Administratora	

18.3.1. Akceptacja dodania urządzenia autoryzującego

Użytkownik, który posiada uprawnienia administratora ma możliwość zaakceptować/odrzuć w opcji administracji urządzenie innego użytkownika.

Po naciśnięciu w link [Lista urządzeń autoryzujących - administracja](#) i kliknięciu w link z nazwą urządzenia na liście zostanie zaprezentowana formatka *Urządzenie autoryzujące - szczegóły*.

Urządzenia autoryzujące - administracja			
Lista urządzeń autoryzujących		Lista urządzeń autoryzujących - administracja	
Nazwa urządzenia	Data powiązania	Status	
test2	2017-08-10 08:39:38	Czeka na akceptację Administratora	

Na formatce *Urządzenie autoryzujące - szczegóły* dla urządzenia ze statusem *Czeka na akceptację Administratora* dostępne są następujące przyciski funkcyjne:

- [Akceptuj urządzenie] - akceptacja urządzenia potwierdzona przez administratora autoryzacją dostępnym środkiem autoryzującym, urządzenie otrzymuje status *Zaakceptowany przez Administratora*,
- [Odrzuć urządzenie] - odrzucenie urządzenia (nie wymaga autoryzacji), urządzenie otrzymuje status *Odrzucony przez Administratora*,
- [Zrezygnuj] - zamknięcie okna ze szczegółami urządzenia.

Urządzenie autoryzujące - szczegóły

Nazwa urządzenia:	test
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2017-08-09 14:45:06
Status:	Czeka na akceptację przez Administratora

Akceptuj urządzenie

Odrzuć urządzenie

Zrezygnuj

Wybór przycisku [Odrzuć urządzenie] przez Administratora spowoduje odrzucenie urządzenia autoryzującego. Po poprawnym odrzuceniu urządzenia zostanie zaprezentowany komunikat jak na poniższym ekranie.

Odrzucenie urządzenia autoryzującego przez Administratora

Urządzenie autoryzujące zostało odrzucone.

Zamknij

Po wykonaniu odrzucenia urządzenia na liście urządzenie jest widoczne ze statusem *Odrzucony przez Administratora*.

Urządzenia autoryzujące		
☐ Dodaj urządzenie autoryzujące		
Nazwa urządzenia	Data powiązania	Status
test	2017-08-10 14:38:59	Odrzucony przez Administratora

Wybór przycisku [Akceptuj urządzenie] przez Administratora zaprezentuje formatkę *Akceptacja urządzenia autoryzującego przez Administratora*, na której należy zaakceptować za pomocą dostępnej metody akceptacji (np. karta mikroprocesorowa, token VASCO). Administrator nie będzie miał możliwości zaakceptować/odrzuć w opcji administracji swojego urządzenia - będzie musiał zrobić to inny administrator.

Akceptacja urządzenia autoryzującego przez Administratora

Nazwa urządzenia:	test
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2017-08-09 14:45:06
Status:	Czeka na akceptację przez Administratora

PIN

Po poprawnej akceptacji urządzenia autoryzującego wyświetlany jest komunikat.

Akceptacja urządzenia autoryzującego przez Administratora

Urządzenie autoryzujące zostało zaakceptowane.

Urządzenie autoryzujące jest widoczne na liście ze statusem *Zaakceptowany przez Administratora*.

Urządzenia autoryzujące		
☐ Lista urządzenia autoryzujące	☐ Lista urządzenia autoryzujące administracja	
☐ Dodaj urządzenie autoryzujące		
Nazwa urządzenia	Data powiązania	Status
test	2017-08-09 14:45:06	Zaakceptowany przez Administratora

Po kliknięciu w nazwę urządzenia na liście otwarta zostanie formatka *Urządzenie autoryzujące - szczegóły*, która pozwala dokończyć dodawanie urządzenia.

Urządzenie autoryzujące - szczegóły

Nazwa urządzenia:	test
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2017-08-10 14:16:35
Status:	Zaakceptowany przez Administratora

Dokończ dodawanie urządzenia
Usuń
Zrezygnuj

Formatka *Urządzenie autoryzujące - szczegóły* prezentuje następujące przyciski funkcyjne:

- [Usuń] - przycisk umożliwiający usunięcie (dezaktywację) urządzenia mobilnego,
- [Zrezygnuj] - powoduje zamknięcie okna *Urządzenie autoryzujące - szczegóły*,
- [Dokończ dodawanie urządzenia] - przycisk dostępny jest tylko w statusie *Zaakceptowany przez Administratora*, przycisk umożliwia dokończenie procesu [parowania urządzenia](#).

Rozdział 19. AutoDealing

W przypadku, gdy wartość usługi **USLUGA_AUTODEALING** ustawiona jest na *T* oraz użytkownik posiada przypisany identyfikator systemu Autodealing (userId) i status weryfikacji użytkownika w systemie Autodealing jest pozytywny, w systemie def3000/CEB w menu głównym aplikacji dostępna jest opcja *AutoDealing* umożliwiająca dostęp do systemu Autodealing uruchamianego przez wygenerowany link [AutoDealing](#). Domyślnie usługa ustawiona jest na wartość *N* - dostęp wyłączony.



Uruchomienie aplikacji Autodealing następuje w osobnym oknie przeglądarki bez potrzeby jawnego (dane nie są wprowadzane przez użytkownika) uwierzytelnienia użytkownika przez system Autodealing przy założeniu, że użytkownik jest zalogowany do aplikacji def3000/CEB. Integracja odbywa się na poziomie wywołań żądania POST protokołu HTTPS. Dane, które podlegają wymianie (dostępne w adresie URL) to:

- userId - unikalny identyfikator użytkownika w systemie Autodealing. Identyfikator (userId) jest przypisywany do Użytkownika - operatora,
- tokenSSO - token, na podstawie, którego następuje uwierzytelnienie,
- systemName - nazwa systemu "Autodealing".

Podczas logowania się użytkownika do systemu def3000/CEB generowany jest tokenSSO.

TokenSSO zapamiętywany jest na potrzeby bieżącej sesji. Użytkownik, klikając w link [AutoDealing](#) otworzy nowe okno przeglądarki internetowej, z żądaniem HTTPS/POST z parametrami: userId, tokenSSO, systemName. W wyniku wykonania żądania nastąpi uruchomienie usługi TokenLogin systemu Autodealing. Jej uruchomienie z kolei spowoduje walidację tokena SSO. System Autodealing wywoła metodę ValidateSSO, której rezultatem końcowym będzie:

- wyświetlenie okna przeglądarki z aplikacją Autodealing po poprawnym zwalidowaniu sesji użytkownika,
- albo informacji o błędzie.

Po autentykacji użytkownika w systemie Autodealing nie będzie bieżącej kontroli sesji w systemie def3000/CEB, czyli możliwe będzie korzystanie przez klienta z aplikacji Autodealing, niezależnie od zamknięcia aplikacji def3000/CEB lub wygaśnięcia sesji aplikacji def3000/CEB, aż do czasu wygaśnięcia ważności tokenaSSO.

Do poprawnego połączenia z aplikacją Autodealing wymagane jest ustawienie następujących parametrów na bazie systemu BankAdmin:

- **autodealing_url** - adres serwera Autodealing. Należy zwrócić uwagę, aby adres URL był poprawny: zawierał przedrostek "https://", adres IP, port i zakończony był ukośnikiem (/).
- **autodealing_nazwa_systemu** - nazwa systemu Autodealing. Domyślnie wartość ta ustawiona jest na "Autodealing".
- **autodeal_czas_wyg_tokSSO_sek** - czas wygaśnięcia w sekundach tokenSSO w systemie Autodealing. Domyślnie wartość ta ustawiona jest na 86400 (24h).
- **autodealing_tokenSSO_url** - adres URL do modułu proxy mapującego wywołania HTTP na wywołania usług z Guardian-service.