



Oprogramowanie dla bankowości.

Dokumentacja użytkownika systemu def3000/CBP



1. Informacje o dokumencie

Niniejszy dokument jest dokumentacją użytkownika systemu def3000/CBP w wersji 2.10.000C.

Metryka dokumentu:

Wersja systemu: 2.10.000C

Wersja dokumentu: 1

Przeznaczenie dokumentu: poufny, zewnętrzny

Identyfikator dokumentu: DOC.UZT_def3000_CBP_2.10.000CE

2. Konwencje typograficzne

W dokumentacji stosowane są następujące konwencje typograficzne

Konwencja typograficzna lub znak wizualny	Opis
Standardowy	Podstawowy tekst dokumentacji
Tabela	Tekst w tabeli
Nowe pojęcie	Nowe pojęcia. Wyróżnienie ważnych fragmentów tekstu.
Kursywa	Pozycje na listach wartości. Komunikaty systemowe. Parametry lub zmienne, których rzeczywiste nazwy lub wartości mają być dostarczane przez użytkownika. Nazwy opcji systemu. Ścieżki, np. <i>Dane archiwalne</i> → <i>Przeglądanie</i> .
Uwaga	Tekst uwagi, komentarza, zastrzeżenia - informacje, na które należy zwrócić uwagę podczas czytania dokumentacji lub pracy z systemem np.  Podany powyżej adres internetowy jest przykładowy. Informację o adresie strony usług internetowych udostępnia Bank.

Ostrzeżenie	Tekst ostrzeżenia - ostrzeżenia zawierają bardzo ważne informacje, na które należy zwrócić szczególną uwagę podczas czytania dokumentacji lub pracy z systemem, np.  Zmiany przeksięgowowań nie są kontrolowane przez system i wykonywane są wyłącznie na własną odpowiedzialność operatora!
Link	Odwołania do innych rozdziałów lub fragmentów tekstu. Adresy URL
Konwencja typograficzna lub znak wizualny	Opis
Kod źródłowy	Fragmenty kodu źródłowego. Przykłady wydruków <pre>{ "a": "b" }</pre>
CAPS LOCK	Wyróżnienie nagłówków akapitów. Nazwy klawiszy na klawiaturze kombinacje klawiszy, które należy nacisnąć jednocześnie zawierają znak "+" pomiędzy, np. CTRL+F.
[]	Nazwy przycisków, np. [Czynności]

3. Wprowadzenie

def3000/CBP (Customer Banking Platform) jest unikalnym rozwiązaniem bankowości internetowej i mobilnej opartym na najnowszej generacji Platformie internetowego dostępu klienta do produktów i usług biznesowych.

Dzięki zastosowaniu innowacyjnej koncepcji ekosystemu miniaplikacji, rozwiązanie to pozwala na osiągnięcie przewagi konkurencyjnej poprzez swobodne kształtowanie usług oferowanych klientowi na Platformie zdalnego dostępu.

Rozwiązanie def3000/CBP wyróżnia innowacyjna koncepcja udostępniania funkcjonalności systemu dla klientów instytucji poprzez komponenty zwane miniaplikacjami.

System def3000/CBP automatycznie dostosowuje swój wygląd i funkcjonalność do urządzenia, z którego użytkownik korzysta w danym momencie (jedno spójne rozwiązanie dla bankowości internetowej i mobilnej).

Rozwiązanie def3000/CBP pozwala na swobodne dopasowanie funkcjonalności do indywidualnych potrzeb i oczekiwań użytkownika.

Dokumentacja przedstawia ogólny opis systemu def3000/CBP. Szczegółowy opis funkcjonalności poszczególnych miniaplikacji dostępny jest w dedykowanych dokumentacjach.

Wyjaśnienie pojęć:

Platforma to uniwersalna platforma dostępu internetowego do usług biznesowych. Stanowi środowisko działania miniaplikacji, a tym samym bazę do stworzenia systemu udostępnionego użytkownikom, poprzez dodawane miniaplikacje, usługi biznesowe świadczone przez instytucję.

Miniaplikacja jest programowym modułem funkcjonalnym, osadzonym na Platformie, udostępniającym odbiorcom usług świadczonych przez instytucję, funkcjonalność biznesową np. Płatności.

Miniaplikacja integruje funkcjonalność tego samego obszaru funkcjonalnego np. Płatności i korzysta ze specyfikacji usług dostępnych na Platformie.

4. Tryby dostępu do systemu

Logowanie do systemu

Po uruchomieniu systemu def3000/CBP wyświetlane jest okno autoryzacji:

W zależności od rodzaju wydanych użytkownikowi środków dostępu logowanie może przebiegać w następujący sposób z wykorzystaniem:

1. identyfikatora alfanumerycznego i hasła maskowanego,
2. identyfikatora alfanumerycznego oraz hasła do tokena RSA i aktualnego wskazania tokena,
3. identyfikatora alfanumerycznego, hasła maskowanego i aplikacji Asseco MAA

W przypadku, gdy użytkownik posiada aktywną sesję bankowości internetowej, a następnie będzie próbował powielić ją w innej zakładce zostanie zaprezentowany komunikat informujący o nieprawidłowości takiego działania. Próba równoległej pracy w dwóch oknach skutkuje wylogowaniem użytkownika z systemu def3000/CBP.

Zdublowana zakładka



Platforma bankowości otwarta w innym oknie

Jesteś zalogowany do bankowości na innej zakładce przeglądarki.
Platforma bankowości może być jednocześnie otwarta tylko w jednym oknie.

Zamknij to okno i powrót do pracy w pierwotnej zakładce lub wyloguj się z bankowości (wylogowanie nastąpi na wszystkich zakładkach).

OPUŚĆ STRONĘ

WYLOGUJ Z BANKOWOŚCI

4.1. Logowanie do systemu def3000/CBP za pomocą hasła maskowanego lub tokena RSA

W przypadku logowania za pomocą hasła maskowanego, tokena RSA logowanie odbywa się w trybie dwukrokovym. W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny, następnie w drugim kroku dane uwierzytelniające.

Aby zalogować się do systemu należy w polu **Numer Identyfikacyjny** wprowadzić identyfikator alfanumeryczny użytkownika i użyć przycisku [DALEJ].

Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.

LOGOWANIE

PL

Numer Identyfikacyjny

Wpisz numer

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 Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia kodu dostępu. Logowanie może przebiegać z wykorzystaniem hasła maskowanego, tokena RSA.

Jako kod uwierzytelniający mogą zatem zostać użyte odpowiednio:

- wybrane znaki z hasła (hasło maskowane) - w polu **Kod dostępu** należy wprowadzić losowo wybrane wymagane pozycje z hasła, pozostałe znaki z hasła są ukryte i zastąpione znakiem •. Przy wpisywaniu hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:

←

LOGOWANIE

Kod dostępu

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

• •

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 Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

- hasło do tokena łącznie ze wskazaniem tokena RSA:

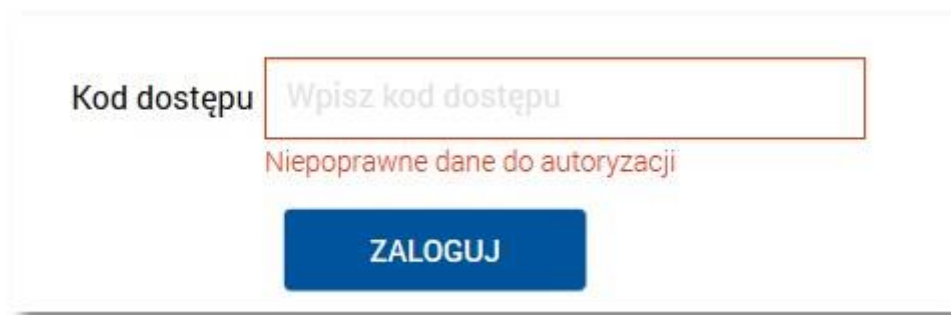
Za pomocą przycisku  możliwy jest powrót do poprzedniej strony logowania.

Po wprowadzeniu (w polu **Kod dostępu**) poprawnego kodu uwierzytelniającego należy użyć przycisku [ZALOGUJ]. System weryfikuje wprowadzone dane i jeżeli stwierdzi ich poprawność użytkownik zostanie zalogowany.

Jeżeli klient loguje się pierwszy raz, po wprowadzeniu identyfikatora a następnie hasła oraz wyborze przycisku [ZALOGUJ] zostanie zaprezentowana formatka *Nowy kod dostępu* wymuszająca zmianę hasła do logowania. Należy wpisać dwukrotnie nowe hasło oraz nacisnąć przycisk [ZAPISZ I ZALOGUJ].

W przypadku, gdy użytkownik korzysta z tokena mobilnego wówczas do użytkownika zostanie wysłany komunikat Push informujący o pozytywnym zalogowaniu do aplikacji def3000/CBP.

W przypadku błędnie wprowadzonych danych autoryzacyjnych system wyświetla komunikat: *"Niepoprawne dane do autoryzacji"* i nie pozwala zalogować się do systemu.



4.2. Aktywacja urządzenia mobilnego w procesie logowania do systemu def3000/CBP

W niniejszym rozdziale przedstawiono opis procesu logowania do systemu def3000/CBP za pomocą aplikacji mobilnej mToken Asseco MAA z uwzględnieniem przypadków, gdy użytkownik posiada bądź nie posiada aktywne urządzenie mobilne. Opis obejmuje następujące przypadki:

- Logowanie do systemu def3000/CBP, użytkownik posiada sparowane aktywne urządzenie mobilne.
- Logowanie do systemu def3000/CBP, użytkownik nie posiada sparowanego aktywnego urządzenia mobilnego.
- Użytkownik loguje się za pomocą hasła zresetowanego (tymczasowego) i posiada sparowane urządzenie mobilne.
- Użytkownik loguje się po raz pierwszy do systemu def3000/CBP i nie posiada sparowanego urządzenia lub loguje się za pomocą hasła zresetowanego (tymczasowego) i nie posiada sparowanego urządzenia mobilnego.
- Przypadek, gdy w systemie wyłączono możliwość parowania urządzenia w procesie logowania i użytkownik nie posiada sparowanego urządzenia oraz jest nowym użytkownikiem.
- Przypadek, gdy w systemie wyłączono możliwość parowania urządzenia podczas logowania i użytkownik nie posiada sparowanego urządzenia mobilnego.

Przypadek 1 – Proces logowania do systemu def3000/CBP, użytkownik posiada sparowane aktywne urządzenie.

Użytkownik podaje login, a następnie wybiera przycisk [DALEJ].

LOGOWANIE

PL

Numer Identyfikacyjny

K70003

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 (oznacza 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 Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Użytkownik podaje poszczególne znaki hasła maskowanego aplikacji Asseco MAA oraz wybiera przycisk [ZALOGUJ].

← LOGOWANIE

Kod dostępu

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

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 (oznacza 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 Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Następuje oczekiwanie na potwierdzenie logowania w aplikacji mobilnej Asseco MAA.

← Uwierzytelnianie

Oczekiwanie na uwierzytelnienie aplikacją mobilną

Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu logowania

W wyniku akceptacji akcji logowania w aplikacji mobilnej Asseco MAA prezentowane jest potwierdzenie.

DOC.UZT_def3000_CBP_2.10.000CE

Strona 8



W wyniku odrzucenia logowania w aplikacji mobilnej Asseco MAA lub upłynięcia czasu na podjęcie decyzji prezentowany jest komunikat jak na poniższym ekranie.



Przypadek 2 – Poprawne logowanie do systemu def3000/CBP, użytkownik nie posiada sparowanego aktywnego urządzenia.

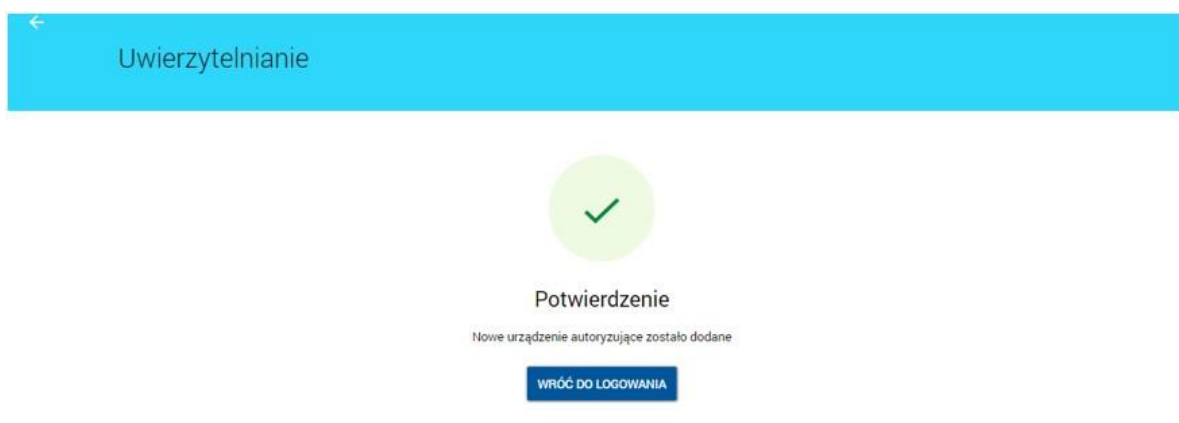
W przypadku, gdy użytkownik nie posiada sparowanego urządzenia po podaniu loginu i hasła Asseso MAA maskowanego prezentowany jest pierwszy krok parowania urządzenia.



Po wyborze przycisku [POSIADAM APLIKACJĘ] zostanie wyświetlona formatka z drugim krokiem procesu, na której prezentowany jest kod aktywacyjny, który należy wprowadzić w aplikacji mobilnej Asseco MAA podczas rejestracji urządzenia. Pasek postępu odlicza czas pozostały na parowanie.



Po sparowaniu urządzenia w aplikacji mobilnej AssecO MAA w aplikacji def3000/CBP prezentowane jest potwierdzenie.



W przypadku, gdy urządzenie nie zostało sparowane - przykładowo upłynął czas na parowanie w systemie def3000/CBP prezentowany jest komunikat jak na poniższym ekranie.



Przypadek 3 – użytkownik loguje się za pomocą hasła zresetowanego (tymczasowego) i posiada sparowane urządzenie.

Logowanie za pomocą hasła tymczasowego, które użytkownik otrzymał za pomocą SMS. Wymagana jest zmiana hasła.

Potwierdzenie w aplikacji mobilnej AssecO MAA. Zalogowanie do systemu def3000/CBP.

Przypadek 4 – użytkownik nie posiada sparowanego urządzenia - loguje się po raz pierwszy lub po resecie hasła (za pomocą hasła tymczasowego).

Logowanie do systemu def3000/CBP odbywa się za pomocą hasła tymczasowego, które użytkownik otrzymał za pomocą SMS. Użytkownik paruje urządzenie. Po pomyślnym sparowaniu urządzenia następuje powrót do okna logowania. Użytkownik ponownie loguje się do systemu def3000/CBP za pomocą hasła tymczasowego. Wymagana jest zmiana hasła tymczasowego. Potwierdzenie w aplikacji mobilnej AssecO MAA logowania do systemu def3000/CBP.

Przypadek 5 – w przypadku, gdy wyłączono możliwość parowania urządzenia w procesie logowania oraz użytkownik nie posiada sparowanego urządzenia i jest użytkownikiem nowym.

Logowanie za pomocą loginu i hasła tymczasowego. Wymagana jest zmiana hasła tymczasowego. Powrót do logowania. Logowanie za pomocą loginu i hasła.

Po podaniu loginu i hasła – prezentowany jest komunikat *"Brak aktywnego urządzenia"*.

The screenshot shows a login interface with a blue header containing a back arrow and the word 'LOGOWANIE'. Below the header is a grid of 24 input fields for a 'Kod dostępu' (Access code), numbered 1 to 24. A red error message 'Brak aktywnego urządzenia' is displayed below the grid. A blue 'ZALOGUJ' button is positioned below the error message. Below the button, there is a section titled 'Pamiętaj o podstawowych zasadach bezpieczeństwa:' (Remember the basic security rules:) with a list of instructions:

- 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 Centrum Usług Internetowych przez firmę DigiCert Inc

 The text continues: 'Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.' and 'Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)'.

Przypadek 6 – w przypadku, gdy wyłączono możliwość parowania urządzenia w procesie logowania i użytkownik nie posiada sparowanego urządzenia po podaniu loginu i hasła prezentowany jest komunikat *"Brak aktywnego urządzenia"*.

4.2.1. Logowanie do systemu def3000/CBP za pomocą aplikacji Assecoco MAA po zmianie z logowania hasłem maskowanym na logowanie mobilne



Jeżeli użytkownik dotychczas logował się do def3000/CBP za pomocą **hasła maskowanego**, wówczas dotychczasowe hasło służy do logowania za pomocą aplikacji Assecoco MAA.

W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny w polu **Numer Identyfikacyjny**. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tą wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.

LOGOWANIE

PL

Numer Identyfikacyjny

Wpisz numer

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 (oznacza 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 Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia hasła maskowanego. Wymagane jest podanie losowo wybranych pozycji z hasła, pozostałe znaki z hasła są ukryte i zastąpione znakiem •. Przy wpisywaniu hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:

←

LOGOWANIE

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Kod dostępu

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

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 (oznacza 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 Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Po wybraniu [ZALOGUJ] zostaje wyświetlony komunikat informujący o konieczności potwierdzenia logowania za pomocą aplikacji Asseco MAA zainstalowanej na sparowanym urządzeniu.

←

Uwierzytelnianie

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

Oczekiwanie na uwierzytelnienie aplikacją mobilną.

Na sparowane urządzenie zostaje wysłane powiadomienie z informacją o autoryzacji logowania do systemu.

DOC.UZT_def3000_CBP_2.10.000CE

Strona 13

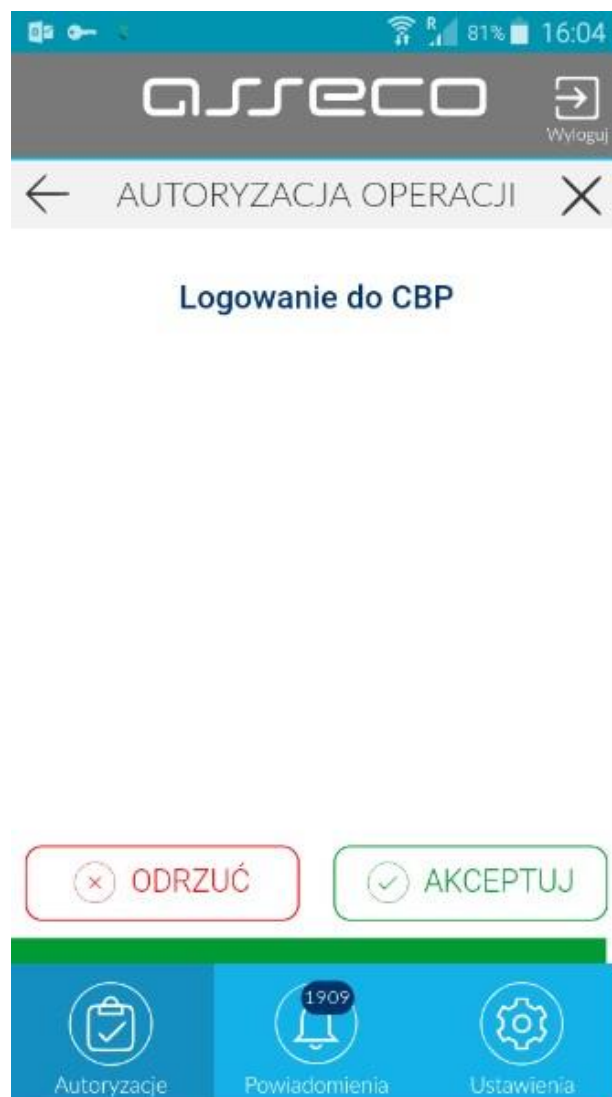


Stuknięcie w powiadomienie przenosi do aplikacji Asseco MAA. Wymagane jest zalogowanie do aplikacji Asseco MAA PINem ustawionym podczas rejestracji urządzenia.

Po zalogowaniu do aplikacji Asseco MAA na liście autoryzacji znajduje się nowa aktywna autoryzacja.



Po wybraniu autoryzacji zostają wyświetlone jej szczegóły:



Akceptacja autoryzacji powoduje zalogowanie Klienta do systemu def3000/CBP.

W przypadku:

- odrzucenia autoryzacji w aplikacji Assecoco MAA przez Klienta lub
- upływu czasu na autoryzację prezentowany jest komunikat:



4.2.2. Pierwsze logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA po zmianie z logowania tokenem RSA na logowanie mobilne



Jeżeli użytkownik dotychczas logował się do def3000/CBP za pomocą **tokena RSA**, wówczas Pracownik banku generuje **tymczasowe hasło mobilne**, które zostaje wysłane do

Klienta za pomocą wiadomości SMS lub przekazane w oddziale Banku.

Hasło tymczasowe mobilne wymaga zmiany podczas pierwszego logowania przy pomocy aplikacji Asseco MAA.



Jeżeli hasło mobilne użytkownika jest **zablokowane lub nieaktywne** (minął czas ważności hasła)
- hasło mobilne użytkownika może zostać zresetowane

Nowe hasło tymczasowe mobilne zostaje wysłane na numer SMS Klienta. Podczas pierwszego logowania aplikacją mobilną po podaniu hasła tymczasowego mobilnego wymagane jest podanie nowego hasła mobilnego.

W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny w polu **Numer Identyfikacyjny**. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.

Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia **tymczasowego hasła mobilnego**. Przy wpisywaniu hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:

←

LOGOWANIE

Kod dostępu

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

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 (oznacza 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 Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Po wybraniu [ZALOGUJ] zostaje wyświetlona formatka zmiany hasła:

←

Nowe hasło dostępu

🔒

Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator użytkownika

K60001

Nowe hasło dostępu

••••••••

✓

Powtórz nowe hasło

••••••••

✓

ZAPISZ I ZALOGUJ

Definiując swoje nowe hasło dostępu pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

○ musi składać się z 10-24 znaków

○ dozwolone znaki: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#\$%^&*()-+=[]\|;':<,>/?

W oknie należy wprowadzić nowe hasło spełniające wymogi polityki bezpieczeństwa znajdujące się w dolnej części formatki. Po powtórzeniu hasła i wybraniu [ZAPISZ I ZALOGUJ] zostaje wyświetlony komunikat informujący o konieczności potwierdzenia logowania za pomocą aplikacji Asseco MAA zainstalowanej na sparowanym urządzeniu:

←

Uwierzytelnianie

📱

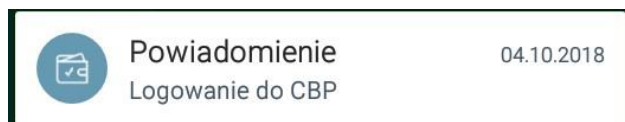
Powiadomienie uwierzytelniające zostało wysłane do urządzenia mobilnego.

Pozostań na tej stronie i potwierdź operację w aplikacji mobilnej.

🔄

Oczekiwanie na uwierzytelnienie aplikacją mobilną.

Na sparowane urządzenie zostaje wysłany push z informacją o autoryzacji logowania do systemu.



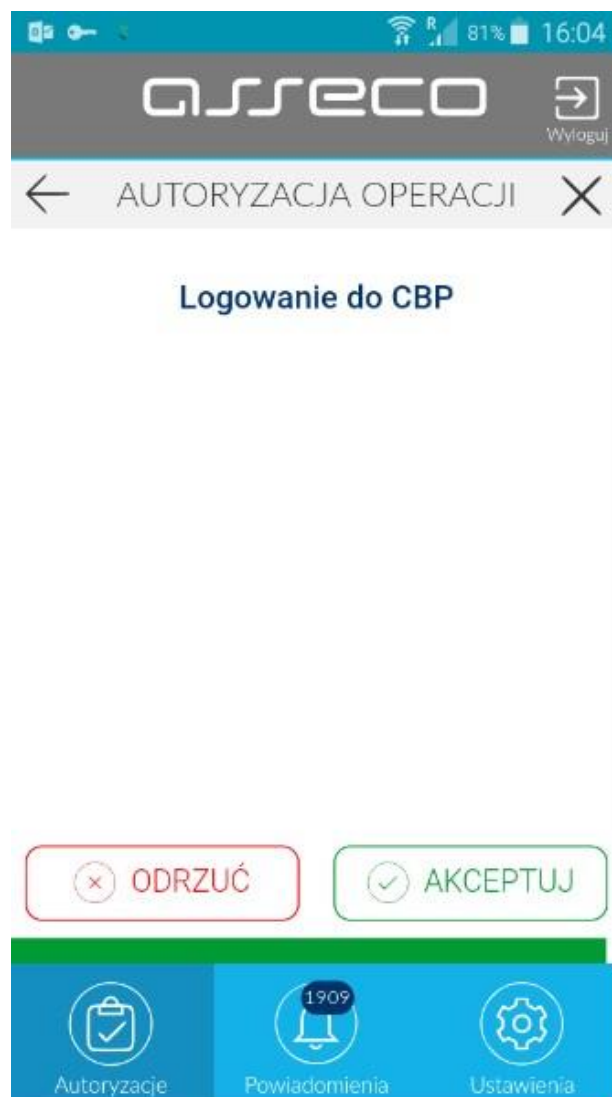
Stuknięcie w push przerosi do aplikacji AssecO MAA. Wymagane jest zalogowanie do aplikacji AssecO MAA PINem ustawionym podczas rejestracji urządzenia.

The screenshot shows the login interface of the AssecO MAA application. At the top, the status bar shows icons for signal, Wi-Fi, battery (40%), and time (00:10). The app's header features a menu icon, the 'assecO' logo, and the title 'LOGOWANIE'. Below this, the user's branch 'BS Kamienna Góra' and a masked PIN '(AW***0)' are shown, along with the text 'Bank spoldzielczy - oddzial Kamienna Gora'. The main instruction 'Podaj PIN, aby się zalogować' is followed by a text input field labeled 'Wprowadź PIN'. Below the input field is a numeric keypad with digits 1-9, 0, and a backspace icon. At the bottom, a large blue button with a right arrow and the text 'ZALOGUJ' is visible.

Po zalogowaniu do aplikacji AssecO MAA na liście autoryzacji znajduje się nowa aktywna autoryzacja.



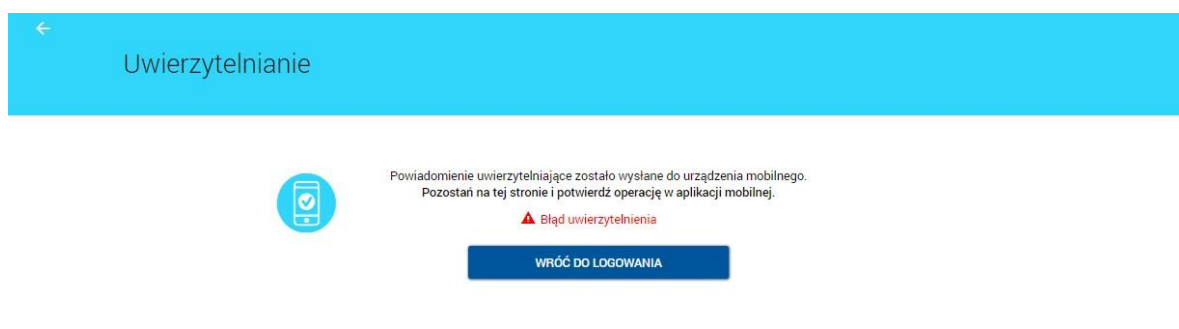
Po wybraniu autoryzacji zostają wyświetlone jej szczegóły:



Akceptacja autoryzacji powoduje zalogowanie Klienta do systemu def3000/CBP.

W przypadku:

- odrzucenia autoryzacji w aplikacji AssecO MAA przez Klienta lub
- upływu czasu na autoryzację prezentowany jest komunikat:



4.2.3. Kolejne logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA

Klient może logować się do systemu def3000/CBP za pomocą aplikacji mobilnej Asseco MAA, jeżeli posiada sparowane aktywne urządzenie oraz hasło mobilne.

W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny w polu **Numer Identyfikacyjny**. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.

LOGOWANIE PL

Numer Identyfikacyjny

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 Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia hasła maskowanego. Wymagane jest podanie losowo wybranych pozycji z hasła, pozostałe znaki z hasła są ukryte i zastąpione znakiem •. Przy wpisywaniu hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:

LOGOWANIE PL

Kod dostępu

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			•			•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

ZALOGUJ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

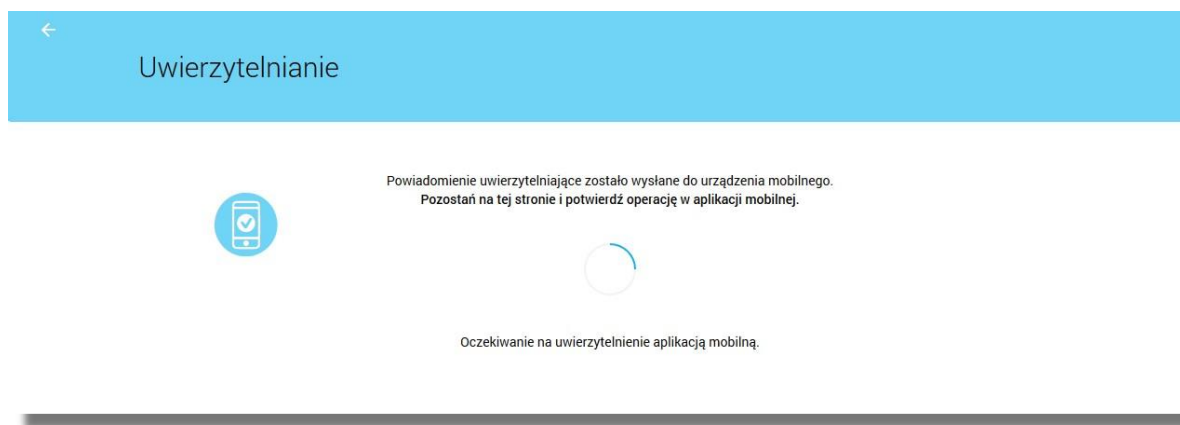
Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- 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 Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Po wybraniu [ZALOGUJ] zostaje wyświetlony komunikat informujący o konieczności potwierdzenia logowania za pomocą aplikacji Asseco MAA zainstalowanej na sparowanym urządzeniu.



Na sparowane urządzenie zostaje wysłany push z informacją o autoryzacji logowania do systemu.



Stuknięcie w push przenosi do aplikacji Assecoco MAA. Wymagane jest zalogowanie do aplikacji Assecoco MAA PINem ustawionym podczas rejestracji urządzenia.

assecO

LOGOWANIE

BS Kamienna Góra (AW***0)
Bank spółdzielczy - oddział Kamienna Góra

Podaj PIN, aby się zalogować

Wprowadź PIN

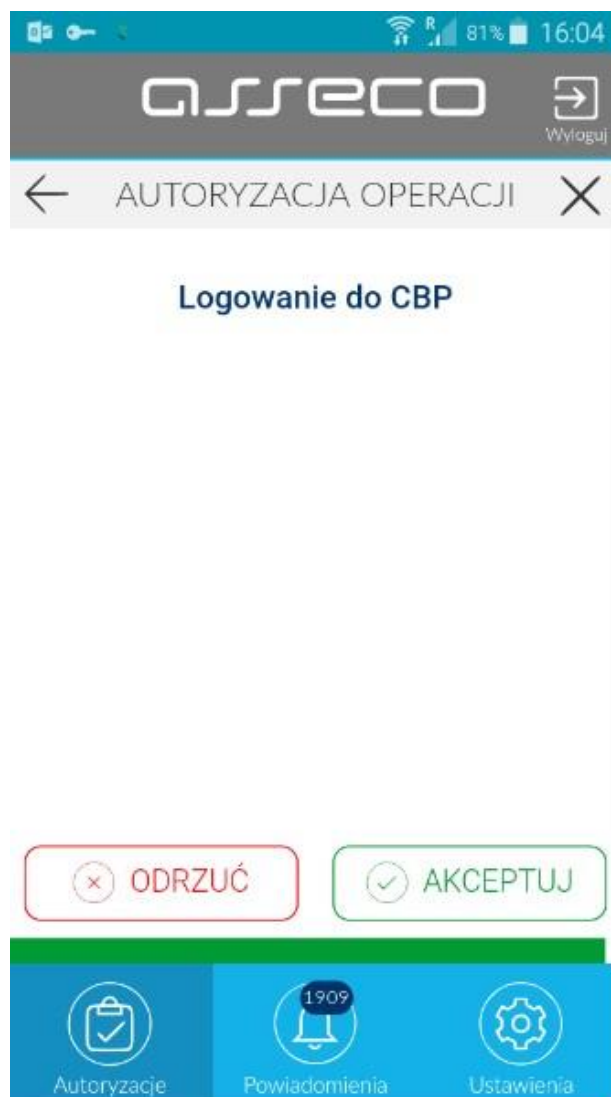
1	2	3
4	5	6
7	8	9
	0	⌫

> ZALOGUJ

Po zalogowaniu do aplikacji AssecO MAA na liście autoryzacji znajduje się nowa aktywna autoryzacja.



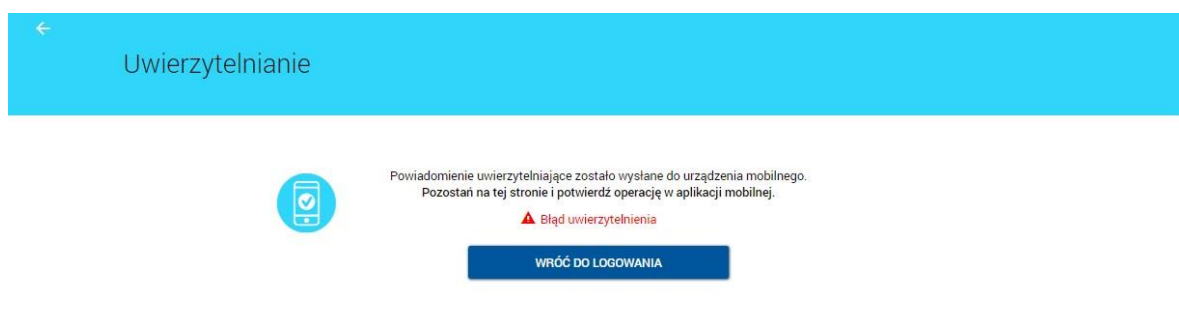
Po wybraniu autoryzacji zostają wyświetlone jej szczegóły:



Akceptacja autoryzacji powoduje zalogowanie Klienta do systemu def3000/CBP.

W przypadku:

- odrzucenia autoryzacji w aplikacji Assecoco MAA przez Klienta lub
- upływu czasu na autoryzację prezentowany jest komunikat:



5. Wybór języka

Na pierwszej stronie logowania użytkownik ma możliwość zmiany języka systemu po wybraniu przycisku znajdującego się w prawym górnym rogu formatki.

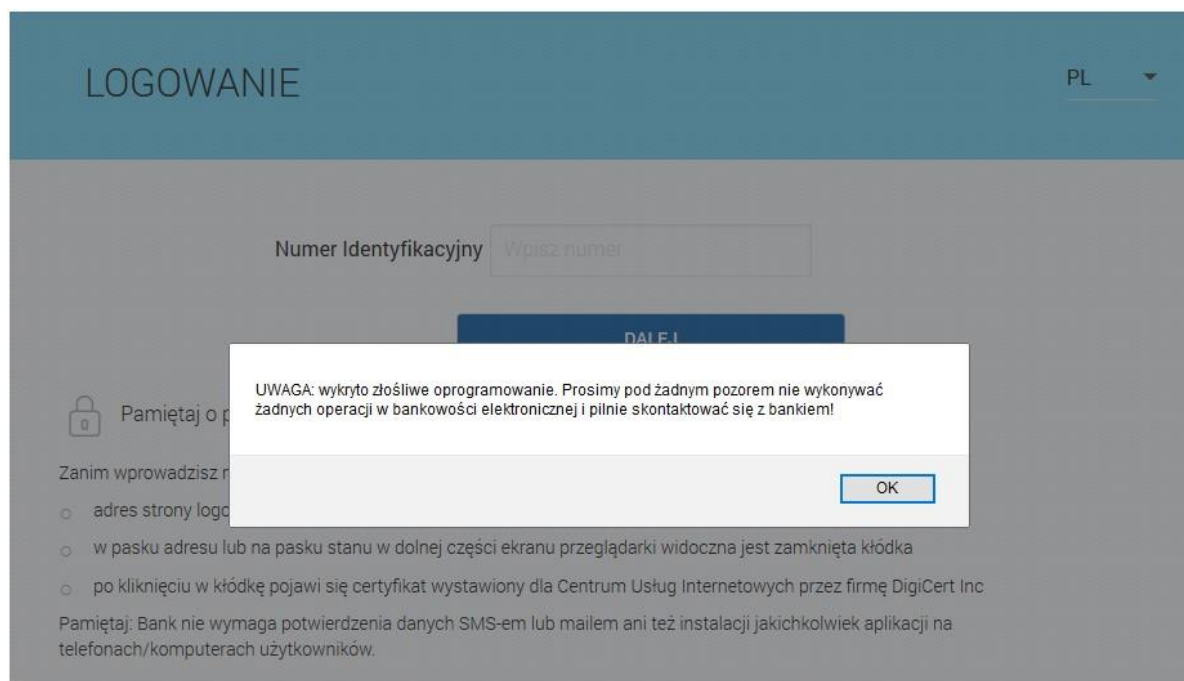


6. Strona logowania i personalizacja

Strona logowania wyświetlana jest:

- w wyniku przejścia na adres serwisu (domyślny język strony - przekazany w parametrze wywołania lub polski, jeśli nie przekazano podczas wywołania),
- wskutek niepowodzenia procesu logowania do systemu,
- wskutek wylogowania z powodu wygaśnięcia sesji użytkownika w systemie (językiem strony logowania jest wówczas język użytkownika używany w systemie),
- w wyniku ponownego przejścia na stronę logowania (przyciskiem [ZALOGUJ PONOWNIE]) ze strony wylogowania (językiem strony jest język ze strony wylogowania).

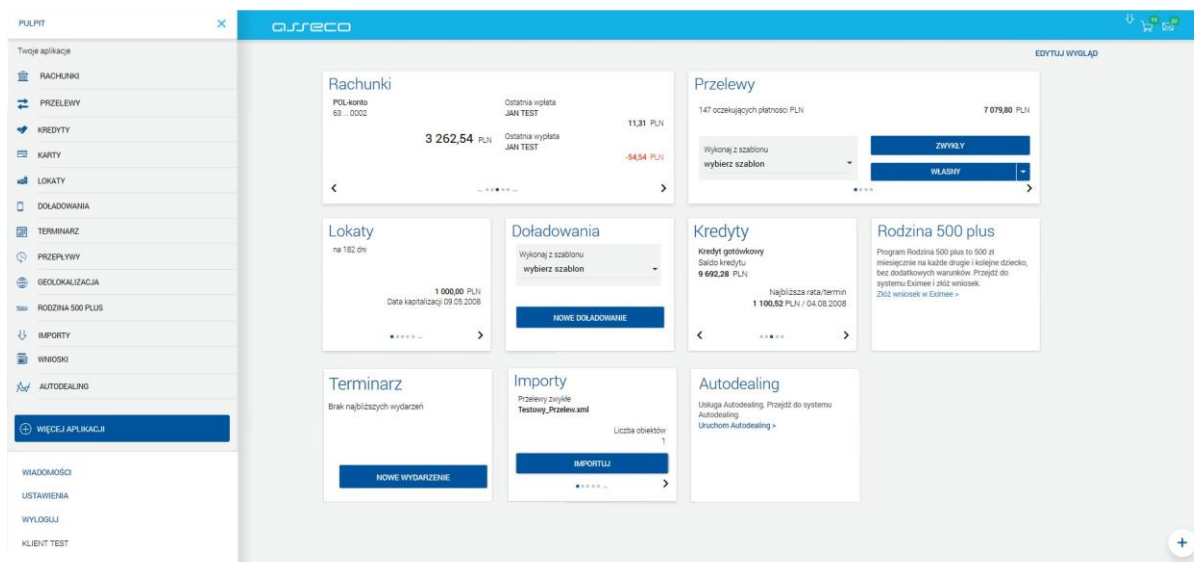
W systemie def3000/CBP zastosowany jest mechanizm weryfikujący działanie wirusa podmieniającego stronę logowania oraz dodającego elementy do strony logowania. W przypadku wykrycia złośliwego oprogramowania po uruchomieniu systemu def3000/CBP zostanie zaprezentowany komunikat jak na poniższym ekranie.



W procesie logowania do systemu hasło maskowane wprowadzone przez użytkownika jest automatycznie szyfrowane przez system.

Zachowanie strony logowania jest zgodne z paradygmatem Responsive Web Design, tj. w zależności od urządzenia, na którym otwarta została strona do logowania, wyświetlane są odpowiednie rozmiarowo pliki graficzne.

Użytkownikowi po zalogowaniu do systemu def3000/CBP wyświetlany jest pulpit z miniaplikacjami:



System automatycznie kończy sesję pracy użytkownika w systemie po upływie 10 minut bezczynności użytkownika. Po upływie czasu trwania sesji, wybranie dowolnej akcji w systemie powoduje zaprezentowanie [strony wylogowania](#).

W sytuacji, gdy do zakończenia sesji w systemie została 1 minuta w nagłówku systemu wyświetlany jest licznik prezentujący czas pozostały do zakończenia sesji wraz z komunikatem: *"Do wylogowania pozostało"*:

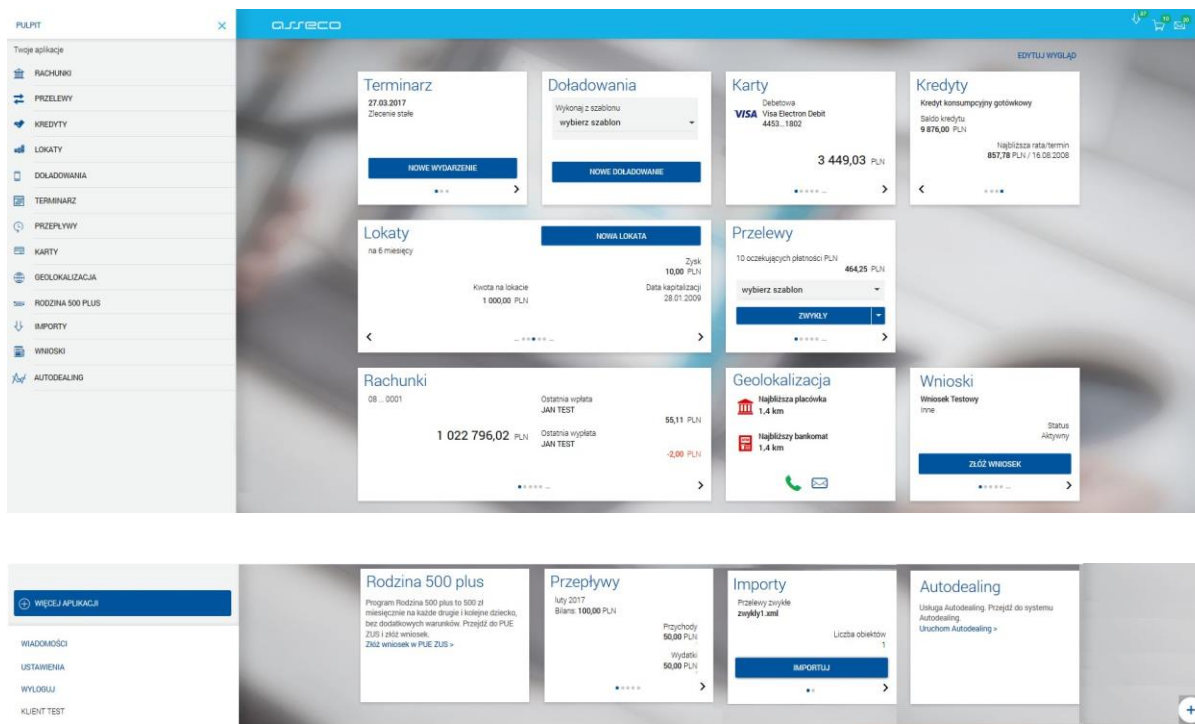


Licznik końca sesji znika po podjęciu aktywności w systemie.

7. Ustawienia własne systemu

Użytkownik systemu def3000/CBP ma możliwość własnej konfiguracji wyglądu systemu. Użytkownik może pobierać udostępnione (przez daną instytucję) miniaplikacje z [butik](#) - może wybrać te z nich, które najlepiej trafiają w jego gust i potrzeby. Lista pobranych miniaplikacji z butik prezentowana jest w panelu sterowania na liście *Twoje aplikacje*. Użytkownik może także sam zdecydować, które z dostępnych dla niego miniaplikacji mają być prezentowane na pulpicie, w jakiej kolejności oraz w jakiej formie mają być prezentowane (standardowej czy rozszerzonej) za pomocą dostępnej na pulpicie opcji [EDYTUJ WYGLĄD](#).

Przykładowe ustawienie wyglądu systemu:

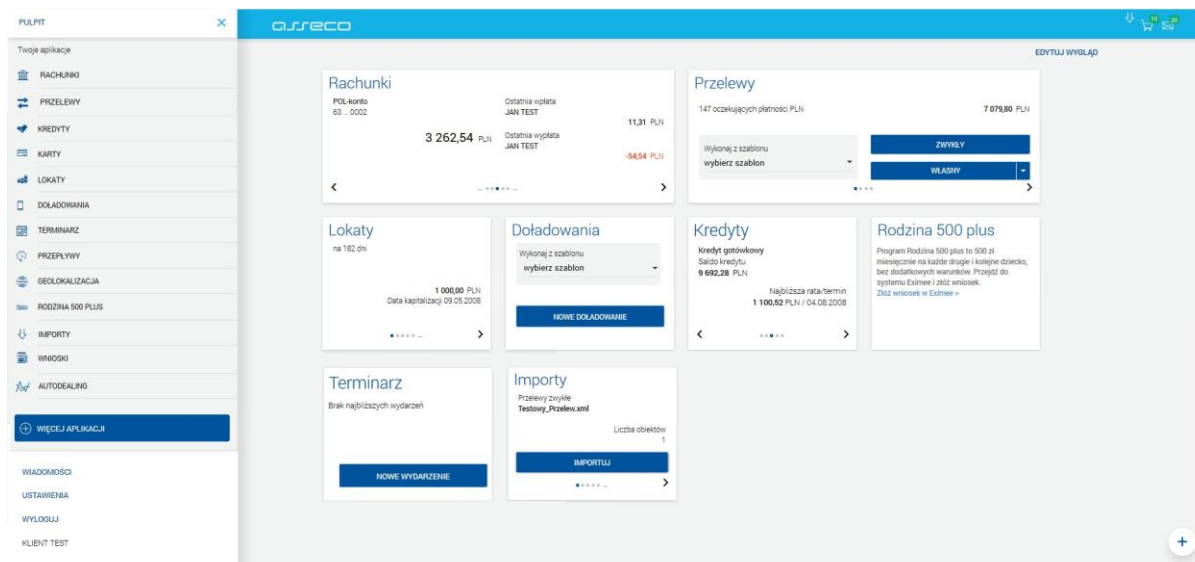


8. Pulpit użytkownika

Użytkownikowi systemu def3000/CBP po zalogowaniu do systemu wyświetlany jest pulpit z miniaplikacjami.

Pulpit systemu zawiera prezentowany w formie widżetów zestaw miniaplikacji używanych przez użytkownika.

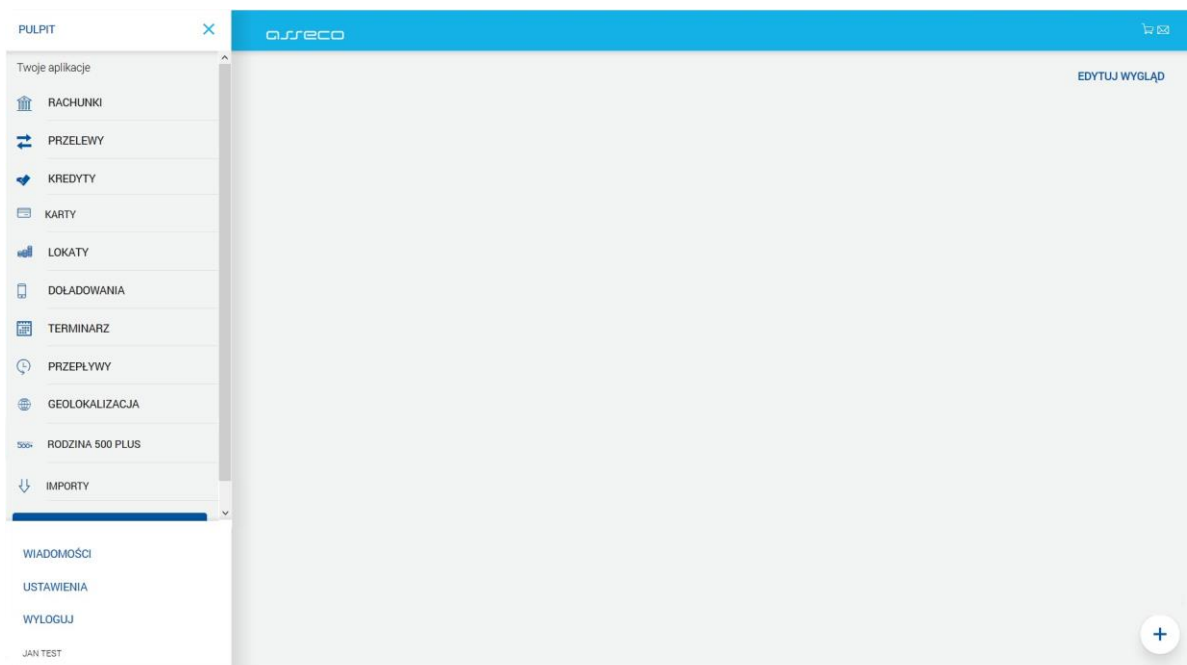
Pulpit stanowi także obszar roboczy użytkownika, w którym prezentowana jest otwarta miniaplikacja.



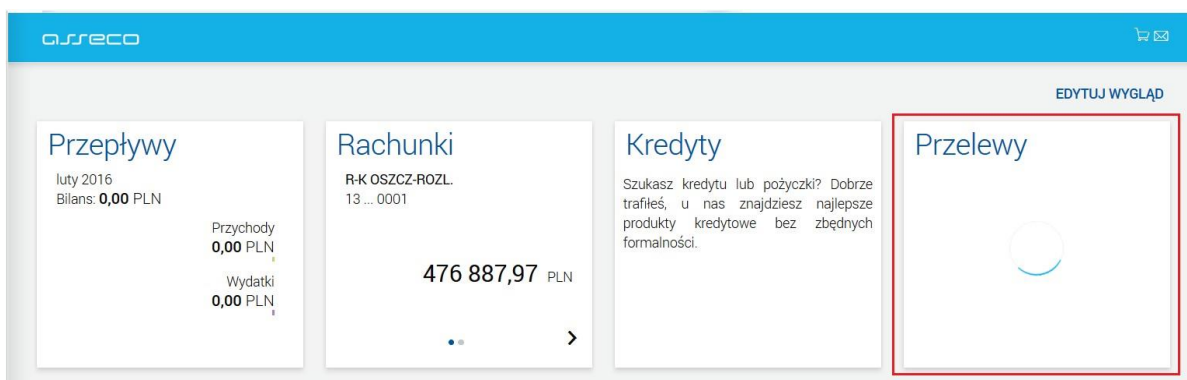
Układ miniaplikacji na pulpicie jest indywidualnie pamiętany dla użytkownika. Domyślny układ miniaplikacji na pulpicie przewiduje widoczność wszystkich miniaplikacji z zachowaniem ustalonej kolejności dla widoku "Twoje aplikacje".

Widoczność poszczególnych miniaplikacji na pulpicie uzależniona jest od udostępnienia danej miniaplikacji w [butiku](#).

Po wyświetleniu pulpitu nie są prezentowane żadne widżety. Pojawiają się one dopiero w momencie, gdy zostaną na niego załadowane dane:



Jeżeli ładowanie danych na widżet trwa dłużej niż ustalona maksymalna długość oczekiwania, wówczas widżet prezentowany jest w trybie ładowania danych:



Położenie widżetów nie zmienia się - w miejsce niezaladowanych widżetów prezentowane jest puste miejsce. Wartość maksymalnego czasu opóźnienia jest ustawiona na stałe w systemie i wynosi 0,5 s.

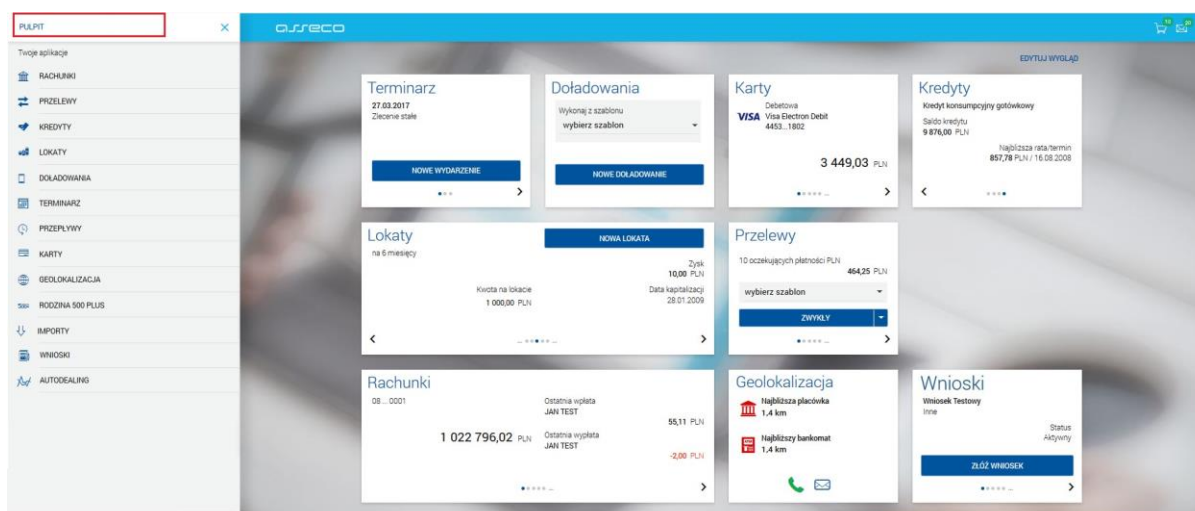
Kliknięcie w obszar wybranej miniaplikacji powoduje jej otwarcie na pulpicie:

Rachunki		
WSZYSTKIE RACHUNKI	RACHUNKI BIEŻĄCE	RACHUNKI WALUTOWE
Wszystkie rachunki		
		HISTORIA WYCiąGI ZBIORCZE
		FILTRUJ
POBIERZ LISTĘ RACHUNKÓW		
Rach.oszcz.rozl. Numer rachunku 75 9496 0008 0007 1417 3000 0001	Saldo księgowe 25 166,98 PLN	Saldo dostępne 23 583,43 PLN
Rach.oszcz.rozl.edit Numer rachunku 52 9496 0008 0005 4986 3000 0001	Saldo księgowe 60,18 PLN	Saldo dostępne 0,00 PLN
Rach.oszcz.rozl. Numer rachunku 90 9496 0008 0007 1417 2000 0001	Saldo księgowe 285,05 EUR	Saldo dostępne 285,05 EUR
Podsumowanie	Saldo księgowe 25 227,16 PLN 285,05 EUR	Saldo dostępne 23 583,43 PLN 285,05 EUR

W przypadku, gdy klient nie posiada dedykowanego produktu zachowanie systemu po wyborze kafła miniaplikacji jest następujące:

- w sytuacji, gdy nie przypisano linku do obrazu personalizowanego pustego kafła nastąpi przejście do wnętrza aplikacji,
- w sytuacji, gdy przypisano link do obrazu personalizowanego pustego kafła wówczas nastąpi otwarcie w nowym oknie/zakładce strony podlinkowanej.

Użytkownik systemu def3000/CBP może w dowolnym momencie korzystania z systemu oraz z poziomu dowolnej opcji wyświetlić pulpit, wybierając dostępny w panelu sterowania przycisk [PULPIT]:



Pulpit można wyświetlić także zamykając otwartą miniaplikację przyciskiem  umieszczonym w prawym, górnym rogu miniaplikacji:

Terminarz

Wydarzenia z miesiąca

Grudzień 2018

poniedziałek	wtorek	środa	czwartek	piątek	sobota	niedziela
26	27	28	29 tytuł testowy Numer umowy 12/LB/161209	30 Koniec okresu lokaty	Gru 1	2
3	4	5 Przelew testowy	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23

Za pomocą linku [EDYTUJ WYGLĄD](#) znajdującego się na pulpicie nad widżetami miniaplikacji, możliwe jest dodawanie, usuwanie widżetu miniaplikacji na pulpicie, zmiana lokalizacji widżetu, a także zmiana rozmiaru widżetu.

W przypadku, gdy w opcji *Ustawienia* → *Domyślny rachunek* zdefiniowano domyślne rachunki dla produktów, w poszczególnych kafelkach dostępnych na pulpicie - Rachunek/Produkt wskazany jako domyślny zaprezentowany będzie na początku wyświetlania aktualnie dostępnych pozycji. Domyślny rachunek bieżący prezentowany będzie w pierwszej kolejności jako rachunek, z którego będą realizowane przelewy/doładowania.

8.1. Widok "Twoje aplikacje"

Widok "Twoje aplikacje" obejmuje wszystkie miniaplikacje dostępne dla użytkownika i występujące w wersji produkcyjnej. Na widoczność opcji prezentowanych w widoku "Twoje aplikacje" mają także wpływ ustawienia w [butik](#).

PULPIT

Twoje aplikacje

RACHUNKI

PRZELEWY

KREDYTY

KARTY

LOKATY

DOŁADOWANIA

TERMINARZ

PRZEPIWY

GEOLOKALIZACJA

RODZINA 500 PLUS

IMPORTY

WNIOSKI

AUTODEALING

WIĘCEJ APLIKACJI

WIADOMOŚCI

USTAWIENIA

WYŁOGU

JAVI TEST

asreco

EDYTUJ WYGLĄD

Karty

Karty

599 762,45 PLN

Rachunki

44...0001

599 762,45 PLN

Przelewy

5 oczekujących płatności PLN

1 144,75 PLN

Kredyty

Kredyt gotówkowy

9 692,28 PLN

Lokaty

na 1 miesiąc

14 081,00 PLN

Przeprawy

lipiec 2018

0,00 PLN

Kolejność miniaplikacji ustalona dla widoku uwzględnia znaczenie biznesowe miniaplikacji (**RACHUNKI**,

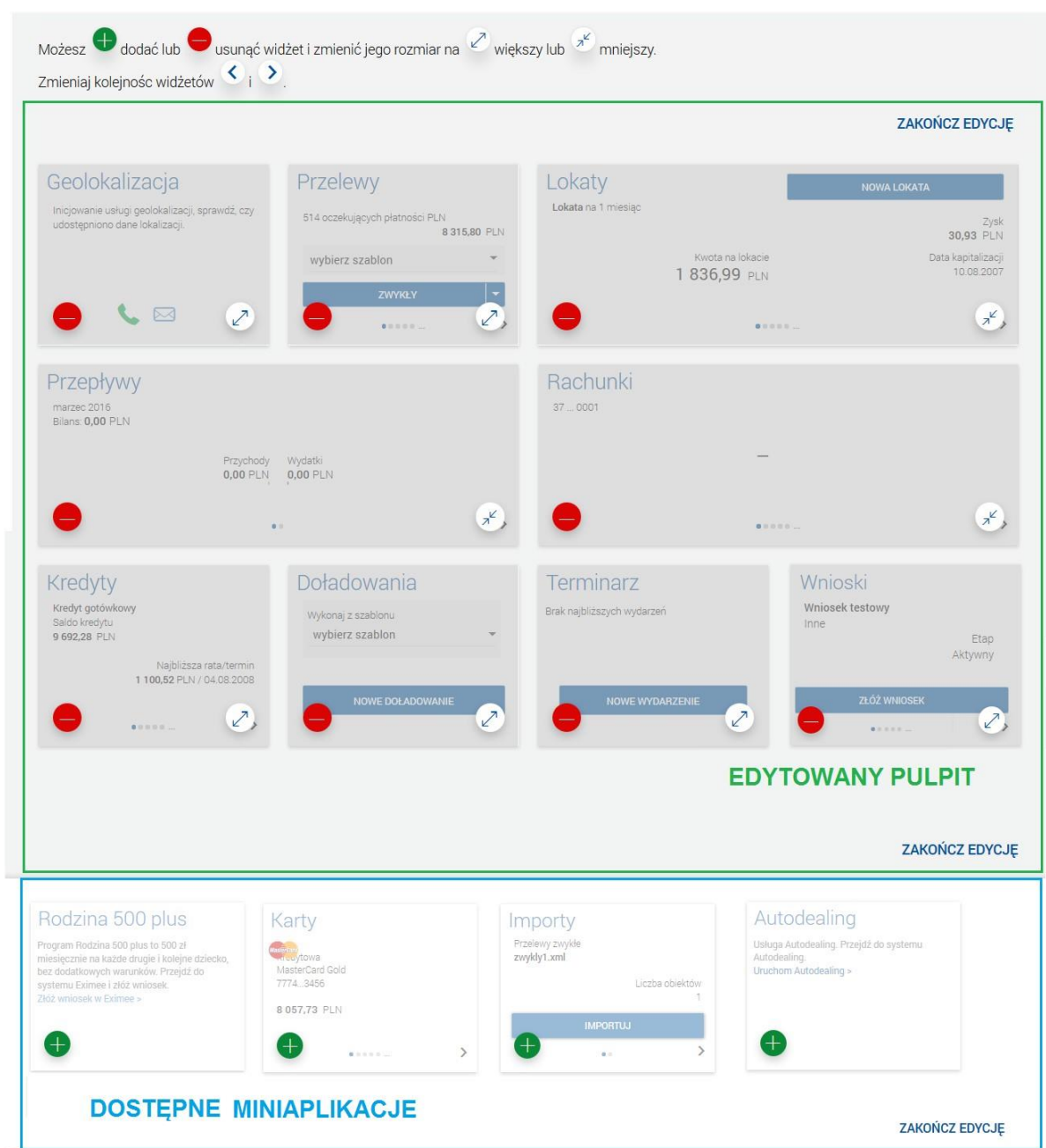
PRZELEWY, KREDYTY, KARTY, LOKATY, DOŁADOWANIA, TERMINARZ, PRZEPŁYWY, GEOLOKALIZACJA).

Wybranie konkretnej miniaplikacji na liście powoduje przejście do widoku głównego tej miniaplikacji.

8.2. Edycja wyglądu pulpitu

Edycja wyglądu pulpitu użytkownika możliwa jest po wybraniu linku *EDYTUJ WYGLĄD* dostępnego na pulpicie nad widżetami miniaplikacji.

Po wybraniu opcji *EDYTUJ WYGLĄD* wyświetlany jest pulpit użytkownika w trybie edycji. Ekran edycji pulpitu podzielony jest na dwie sekcje: edytowany pulpit oraz dostępne miniaplikacje:



Edycja pulpitu odbywa się za pomocą przycisków znajdujących się na poszczególnych elementach.

Dodawanie/usuwanie miniaplikacji w trybie edycji pulpitu odbywa się za pomocą przycisków  i  znajdujących się na poszczególnych elementach.

W trybie edycji pulpitu użytkownik może:

- dodać nową miniaplikację na pulpit - za pomocą przycisku  znajdującego się w sekcji dostępnych miniaplikacji na widżecie miniaplikacji, która nie została jeszcze dodana do pulpitu.

W sekcji dostępnych miniaplikacji prezentowane są tylko te miniaplikacje (dostępne dla użytkownika), które nie znajdują się na jego pulpicie. Po wybraniu interesujących użytkownika miniaplikacji, będą one wyświetlane na pulpicie w formie widżetów.

W sytuacji, gdy wszystkie dostępne dla użytkownika miniaplikacje są już dodane do pulpitu, sekcja dostępnych miniaplikacji jest pusta.

- usunąć wybraną miniaplikację z pulpitu za pomocą przycisku  dostępnego na widżecie miniaplikacji w sekcji edytowanego pulpitu,
- zmienić kolejność ułożenia miniaplikacji na pulpicie, za pomocą przycisków dostępnych na widżecie miniaplikacji w sekcji edytowanego pulpitu:



- przesuwa miniaplikację w lewo,

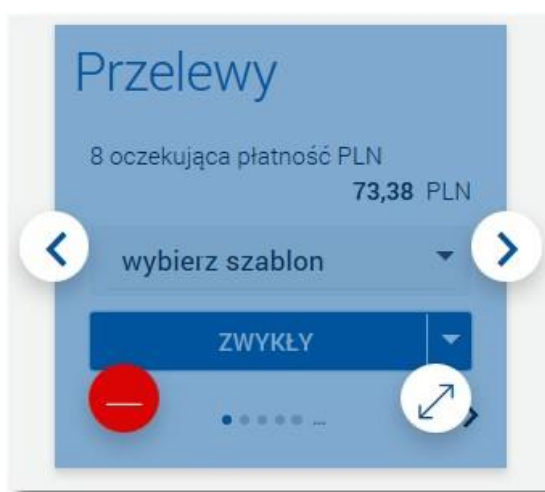


- przesuwa miniaplikację w prawo.

- przełączyć wygląd widżetu miniaplikacji pomiędzy dwoma wariantami rozmiaru: standardowym i dużym (rozszerzonym) za pomocą przycisków dostępnych na widżecie miniaplikacji w sekcji edytowanego pulpitu:

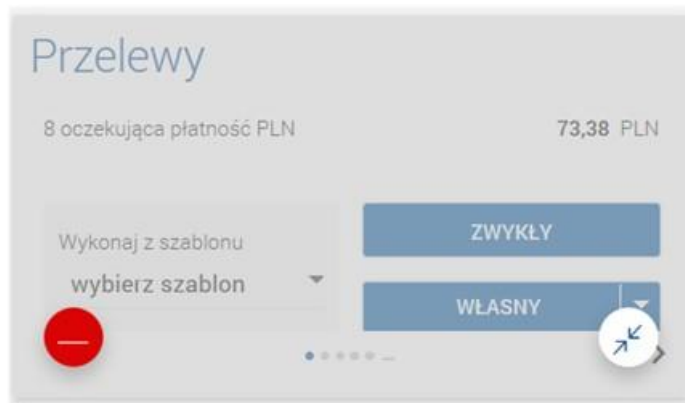


- wyświetla widżet miniaplikacji w rozmiarze standardowym:





- wyświetla widżet miniaplikacji w rozmiarze dużym (rozszerzonym):



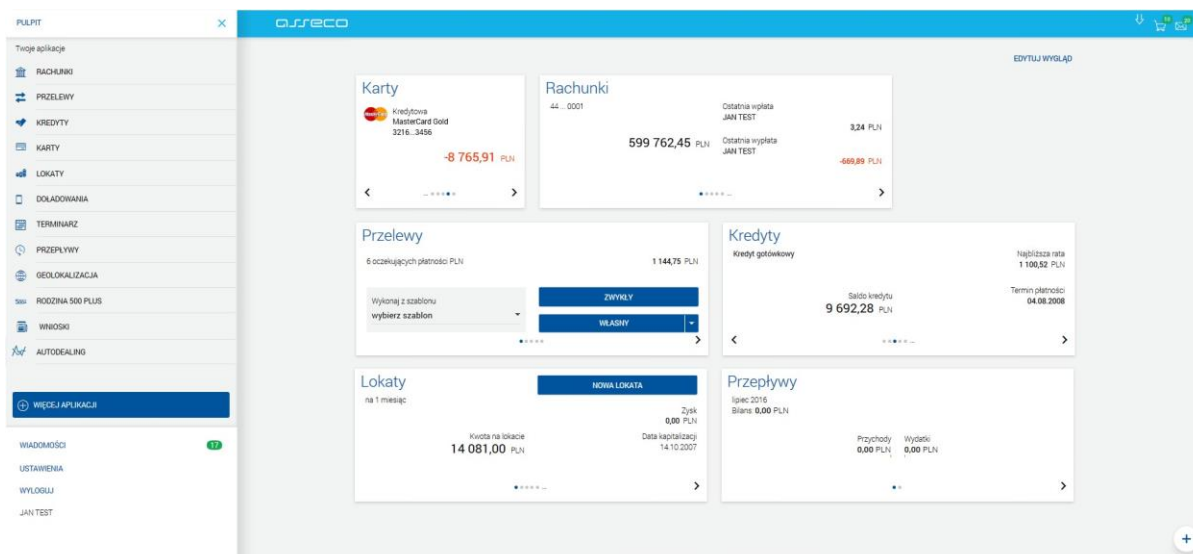
Domyślnie widżety mają rozmiar standardowy, dopiero po przeciągnięciu na edytowany pulpit istnieje możliwość rozszerzenia jego rozmiaru. Rozszerzony rozmiar widżetu nie jest dostępny na urządzeniach z układem 2-kolumnowym (smartfon). Widżety w wersji rozszerzonej prezentują szerszy zakres danych niż widżety w postaci standardowej.

Zatwierdzenie edycji pulpitu odbywa się poprzez link **ZAKOŃCZ EDYCJĘ** znajdujący się w trzech sekcjach ekranu (prawy górny róg edytowanego pulpitu, pod edytowanym pulpitem po prawej stronie oraz pod sekcją dostępnych do wyboru miniaplikacji).

9. Panel sterowania

Panel sterowania umożliwia dostęp do ogólnej konfiguracji użytkownika, opcji wylogowania z systemu, szybkiego przejścia do pulpitu czy też przejścia do poszczególnych miniaplikacji dostępnych dla użytkownika.

W ramach układu 10-kolumnowego (desktop) po wejściu do systemu def3000/CBP panel sterowania jest domyślnie rozwinięty. Przejście do dowolnej opcji lub kliknięcie w dowolny obszar ekranu nie zamyka menu.



Menu udostępnia następujące opcje:

- **PULPIT** - umożliwia wyświetlenie pulpitu z miniaplikacjami,

Twoje aplikacje - zawiera listę dostępnych i pobranych przez użytkownika miniaplikacji z [butik](#). Wybranie konkretnej miniaplikacji na liście powoduje przejście do widoku głównego tej miniaplikacji,

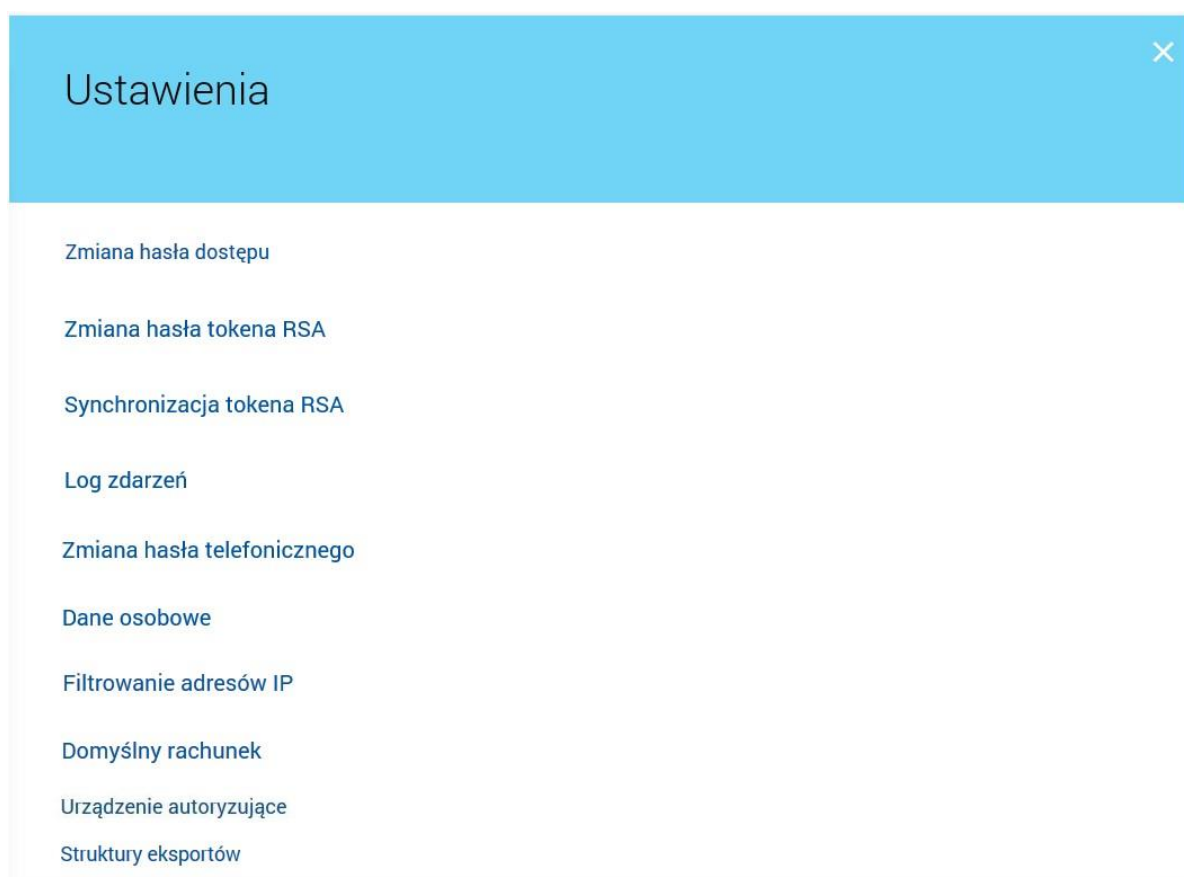
-  - umożliwia przejście do [butik](#) z miniaplikacjami,
- **1 WIADOMOŚCI** - umożliwia przejście do miniaplikacji Wiadomości,
- **USTAWIENIA** - zapewnia dostęp do opcji [ustawień systemu](#),
- **WYLOGUJ** - umożliwia [wylogowanie użytkownika z systemu](#).

Dodatkowo w dolnej części panelu wyświetlane jest imię i nazwisko zalogowanego użytkownika (użytkownika, do którego przypisany jest login).

Użytkownik może zamknąć (ukryć) panel sterowania poprzez użycie dedykowanej opcji .

10. Zarządzanie ustawieniami

Do zarządzania ustawieniami systemu służy dostępna w panelu sterowania opcja *USTAWIENIA*. Wybranie tej opcji powoduje wyświetlenie opcji konfiguracji ustawień:

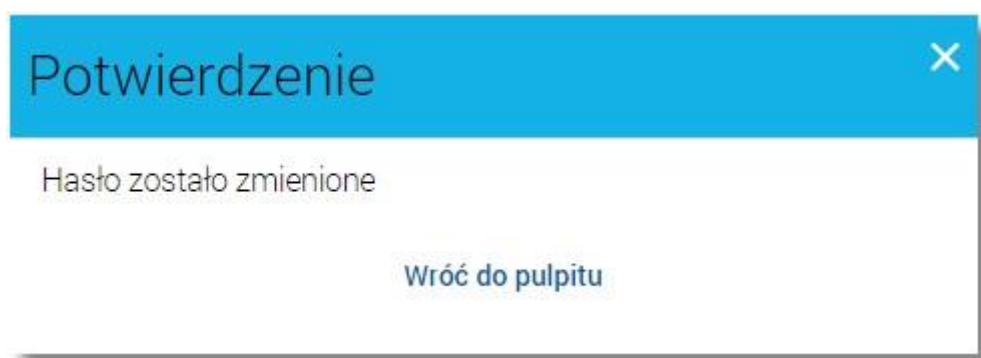


- [Zmiana hasła dostępu](#) - umożliwia zmianę kodu dostępu do logowania,
- [Zmiana hasła tokena RSA](#) - umożliwia zmianę hasła tokena RSA, opcja jest dostępna tylko jeśli użytkownik do logowania nie używa tokena RSA, natomiast do autoryzacji używa tokena RSA,

Operacja zmiany hasła dostępu nie wymaga autoryzacji. System waliduje hasło według takich samych reguł jak w systemie def2500/REB.

Wprowadzone hasła w polach **Nowe hasło dostępu** oraz **Powtórz nowe hasło** muszą być jednakowe. W przypadku, gdy w polach wprowadzono dwa różne hasła, system wyświetla komunikat "*Hasła nie są takie same*", uniemożliwiając tym samym zakończenie procesu zmiany hasła.

Po poprawnym wypełnieniu formularza zmiany hasła dostępu do systemu należy zaakceptować wprowadzone dane przyciskiem [ZATWIERDŹ], system przekazuje wówczas do serwera autoryzacji żądanie zmiany hasła dostępu użytkownika i w przypadku, gdy nowe hasło spełnia reguły bezpieczeństwa zdefiniowane w instytucji system prezentuje komunikat potwierdzający poprawne wykonanie operacji.



Zmiana hasła może być także wywołana automatycznie w procesie uwierzytelniania w przypadku pierwszego logowania do systemu hasłem początkowym lub w przypadku, gdy termin ważności hasła upłynął.

10.1. Zmiana hasła tokena RSA

Opcja *Zmiana hasła tokena RSA* dostępna jest w systemie w przypadku, gdy autoryzacja dokonywana jest za pomocą tokena RSA a logowanie do aplikacji nie odbywa się przy pomocy tokena RSA (tylko hasła stałego lub maskowanego).

Opcja *Zmiana hasła tokena RSA* umożliwia zmianę hasła tokena RSA, ustawienie hasła tokena RSA po jego zresetowaniu lub ustawienie hasła startowego dla tokena RSA (dodatkowe potwierdzenie kolejnym odczytem tokena) poprzez podanie na formularzu *Zmiana hasła tokena RSA* następujących danych:

- **Obecny kod dostępu,** • **Nowe hasło dostępu,**
- **Powtórz nowe hasło.**

←

Zmiana hasła tokena RSA

×

Prosimy pamiętać, że hasło dostępu jest numerem poufnym. W związku z tym nie powinien być ujawniany osobom trzecim. Definiując swoje hasło dostępu pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

Hasło Dostępu:

- ☐ musi składać się z 4-8 znaków

Obecny kod dostępu

••••

Nowe hasło dostępu

Wpisz nowe hasło dostępu

Powtórz nowe hasło

Powtórz nowe hasło dostępu

ZATWIERDŹ

Nowe hasło dostępu musi składać się z 4-8 cyfr, nie powinno zaczynać się od cyfry zero. W przypadku, gdy nastąpi próba wpisanie więcej niż 8 cyfr pod polem **Nowe hasło dostępu** zostanie zaprezentowany komunikat informujący, iż tylko 8 znaków zostało uwzględnionych. Komunikat nie blokuje zatwierdzenia poprawnych kodów dostępu (ograniczonych do 8). Komunikat znika, gdy skasuje się dowolny z znaków w polu **Nowe hasło dostępu**.

←

Zmiana hasła tokena RSA

×

Prosimy pamiętać, że hasło dostępu jest numerem poufnym. W związku z tym nie powinien być ujawniany osobom trzecim. Definiując swoje hasło dostępu pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

Hasło Dostępu:

- ☐ musi składać się z 4-8 znaków

Obecny kod dostępu

••••

Nowe hasło dostępu

••••••••

Uwaga! Uwzględniono tylko 8 znaków

Powtórz nowe hasło

Powtórz nowe hasło dostępu

ZATWIERDŹ

Po wprowadzeniu poprawnych danych na formularzu i potwierdzeniu zmiany przyciskiem [ZATWIERDŹ] nowe hasło będzie obowiązywać przy autoryzacji zleceń.

10.2. Synchronizacja tokena RSA

Opcja *Synchronizacja tokena RSA* dostępna po wybraniu w panelu sterowania opcji *USTAWIENIA* służy do synchronizacji tokena RSA. Opcja dostępna jest w systemie w przypadku kiedy autoryzacja dokonywana jest za pomocą tokena RSA a logowanie do aplikacji nie odbywa się przy pomocy tokena RSA.

Użytkownik ma możliwość synchronizacji tokena (urządzenia tokena RSA) w przypadku np. przekroczenia ilości błędnie wprowadzonych wskazań tokena.

W celu zsynchronizowania tokena RSA należy wprowadzić następujące dane:

- **Numer seryjny tokena RSA,**
- **Aktualne wskazanie tokena RSA,**
- **Następne wskazanie tokena RSA,** oraz wybrać przycisk [ZATWIERDŹ].

10.3. Log zdarzeń

W opcji *Log zdarzeń* prezentowane jest 10 ostatnich zdarzeń logowania/wylogowania użytkownika na serwerze autoryzacyjnym (GUARDIAN) posortowanych malejąco po dacie zdarzenia. Dla każdego zdarzenia prezentowana jest data i godzina zdarzenia, adres IP oraz opis zdarzenia. W przypadku aktywnej usługi **bezpieczeństwo.filtrowanie_ip** w def2500/REB zdarzeniom informującym o poprawnej autoryzacji na serwerze autoryzacyjnym towarzyszą zdarzenia z aplikacji def2500/REB informujące o pozytywnej/negatywnej weryfikacji adresu IP użytkownika. Ewentualna obecność tych zdarzeń sprawia, że lista może zawierać więcej niż 10 pozycji.

Dostępne są następujące typy zdarzeń:

- *"Poprawna autoryzacja na serwerze autoryzacji",*
- *"Poprawne logowanie - wymagana zmiana hasła",*
- *"Niepoprawna autoryzacja na serwerze autoryzacji",*
- *"Poprawne logowanie do bankowości elektronicznej (pozytywna weryfikacja adresu IP)",* • *"Niepoprawne logowanie do bankowości elektronicznej (negatywna weryfikacja adresu IP)",*
- *"Wylogowanie z aplikacji".*

Zdarzenia *"Niepoprawna autoryzacja na serwerze autoryzacji"* oraz *"Niepoprawne logowanie do bankowości elektronicznej (negatywna weryfikacja adresu IP)"* wyróżnione są kolorem na liście (szare tło).

Log zdarzeń		
Data zdarzenia	Adres IP	Opis zdarzenia
27.11.2015 14:00:19	172.20.23.155	Poprawne logowanie do bankowości elektronicznej (pozytywna weryfikacja adresu IP)
27.11.2015 14:00:12	172.20.23.155	Poprawne logowanie do bankowości elektronicznej (pozytywna weryfikacja adresu IP)
27.11.2015 13:50:18	172.20.23.155	Niepoprawne logowanie do bankowości elektronicznej (negatywna weryfikacja adresu IP)
27.11.2015 13:37:42	172.20.23.155	Poprawne logowanie do bankowości elektronicznej (pozytywna weryfikacja adresu IP)
27.11.2015 13:33:03	172.20.23.155	Niepoprawne logowanie do bankowości elektronicznej (negatywna weryfikacja adresu IP)
27.11.2015 13:33:02	172.20.23.155	Poprawne logowanie do bankowości elektronicznej (pozytywna weryfikacja adresu IP)

10.4. Dane osobowe

Użycie opcji *Dane osobowe* dostępnej po wybraniu opcji *USTAWIENIA* w panelu sterowania powoduje wyświetlenie (w trybie podglądu) danych osobowych zalogowanego użytkownika (osoby fizycznej, do której przypisany jest login):

Dane osobowe	
Imię i nazwisko	Jan Test
PESEL	90090909019
Adres	Testowa 1/1 85-000 Bydgoszcz
Typ dokumentu tożsamości	Paszport
Numer dokumentu tożsamości	ZZ5*****5
Numer telefonu do kontaktu	48515*****5
Aktualny adres IP	10.104.8.202

- Imię i nazwisko,

- **PESEL** - pole prezentowane jest w przypadku, gdy włączona jest usługa,
- **Adres** - w układzie 3 linii (w jednej linii kod pocztowy oraz miejscowość)
- **Typ dokumentu tożsamości**,
- **Numer dokumentu tożsamości** - numer prezentowany w postaci zamaskowanej według następującej zasady:
 - pierwsze 3 znaki (nie więcej niż połowa długości numeru),
 - ostatni 1 znak,
 - pozostałe znaki maskowane gwiazdkami *,
- **Numer telefonu do kontaktu** - numer prezentowany w postaci zamaskowanej według następującej zasady:
 - pierwsze 5 znaków (nie więcej niż połowa długości numeru),
 - ostatni 1 znak,
 - pozostałe znaki maskowane gwiazdkami *,
- **Aktualny adres IP** - aktualny adres IP urządzenia, z którego loguje się użytkownik.

10.5. Domyślny rachunek

Wybór opcji *Domyślny rachunek* umożliwia użytkownikowi wskazanie domyślnego rachunku/produktu dla:

- *Rachunków Bieżących (RB)*,
- *Lokat*,
- *Kredytów*,
- *Kart płatniczych*.

←

Domyślny rachunek

×

Domyślny rachunek	Rachunek Testowy 44 8707 0006 0000 4864 3000 0001	▼
Domyślny kredyt	Kredyt gotówkowy 74 8707 0006 0000 4864 1000 0001	▼
Domyślna lokata	Lokata Testowa 48 8707 0006 0000 7171 4000 0002	▼
Domyślna karta	Visa Electron Debit - Główna 85 1020 5385 8716 1341 6785 8367	▼

ZAPISZ

Wskazane domyślnych rachunków/produktów możliwe jest przy pomocy rozwijanej listy wartości dla każdej w/w pozycji z osobna z aktualnie dostępnymi rachunkami/produktami. Każda zmiana w konfiguracji skutkuje wskazaniem domyślnych rachunków/produktów. W przypadku braku wskazania wartości domyślnych system prezentuje i sortuje rachunki/produkty wg [domyślnego sortowania](#). Domyślnie po wyborze opcji dla produktów prezentowana jest wartość *Brak* (w przypadku, gdy użytkownik nie określił jeszcze własnych ustawień).

W procesie logowania system ustawi domyślne rachunki/produkty zgodnie z konfiguracją określoną przez użytkownika w opcji *Domyślny rachunek*.

Konfiguracja domyślnych rachunków/produktów ma wpływ na:

- Kolejność wyświetlania rachunków bieżących, lokat, kredytów i kart płatniczych w poszczególnych kaflach dostępnych na pulpicie - Rachunek/Produkt wskazany jako domyślny będzie zaprezentowany na początku wyświetlania aktualnie dostępnych pozycji,
- Kolejność wyboru rachunku bieżącego dla wypłat/spłat dla miniaplikacji:
 - *Przelewy,*
 - *Doładowania,*
 - *Spłata Kredytu,*
 - *Nowa lokata.*

Domyślny Rachunek Bieżący prezentowany jest w pierwszej kolejności jako rachunek, z którego będą realizowane przelewy/doładowania. Użytkownik będzie mógł wskazać inny dostępny rachunek za pomocą istniejącej listy wartości. W przypadku zmiany przez Użytkownika w/w rachunku, system zapamięta ten rachunek jako domyślny w ramach danej miniaplikacji w bieżącej sesji Użytkownika (w przypadku wyjścia z danej miniaplikacji i przy ponownym powrocie do niej rachunkiem domyślnym będzie rachunek ostatnio wskazany do obciążenia).

W przypadku, gdy jako domyślny Rachunek Bieżący ustawiony zostanie rachunek w walucie obcej (np. EUR) wówczas przy płatności w PLN rachunki będą wyświetlane w kolejności domyślnej dla widoku.

W przypadku listy kart płatniczych, gdzie zbiór pogrupowany jest z uwzględnieniem typu karty, karta domyślna prezentowana będzie w osobnej kategorii opisanej zgodnie ze schematem "Domyślna karta ({typ karty})" (np. "Domyślna karta (Kredytowa)").

Wyżej wymieniona konfiguracja ma wpływ na kolejność wyświetlania rachunków/produktów:

- na głównym kafelku - pulpit,
- na liście wyborów rachunków bieżących, lokat, kredytów i kart płatniczych.

Bez wprowadzenia w/w zmian rachunki/lista rachunków jest prezentowana wg domyślnego sortowania.

Ustawienia domyślnych produktów dla:

- *Lokat,*

- *Kredytów,*
- *Kart płatniczych,*

prezentowane są tylko wtedy kiedy moduł odpowiedniego produktu zostanie zarejestrowany na koncie użytkownika.

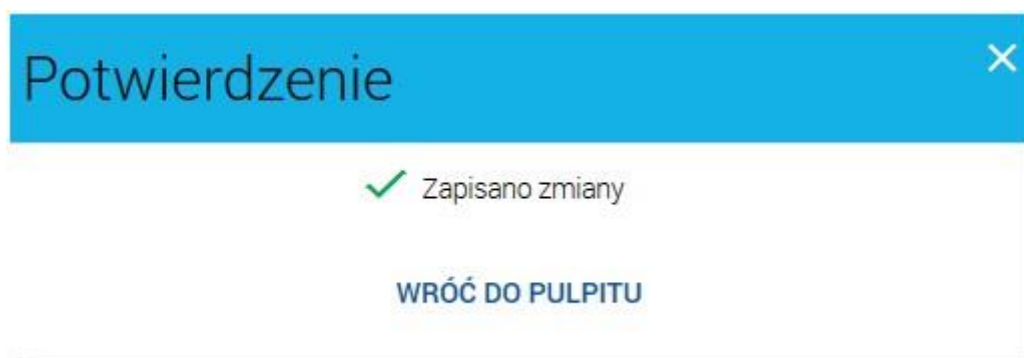
Ustawienie domyślne dla Rachunku Bieżącego dostępne jest zawsze niezależnie czy moduł Rachunków Bieżących jest zarejestrowany na koncie użytkownika czy też nie.

Domyślne sortowania dla rachunków/produktów są następujące:

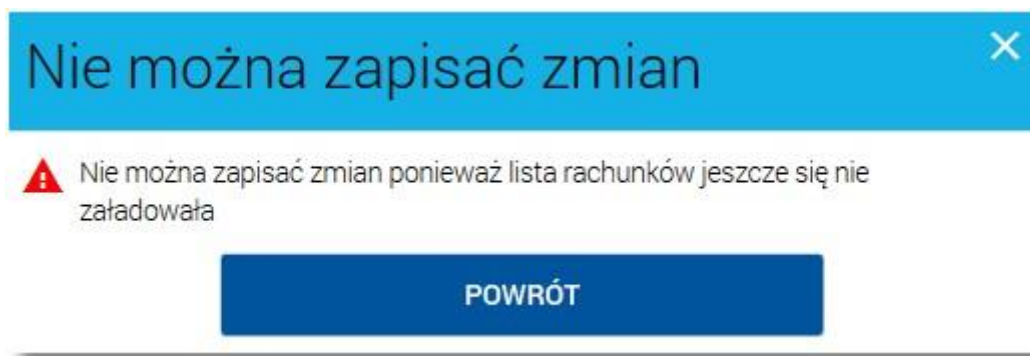
- **Rachunki** - sortowanie rosnące po dacie otwarcia,
- **Lokaty** - sortowanie rosnące po dacie zapadalności,
- **Kredyty** - sortowanie rosnące po dacie otwarcia.

Karty płatnicze sortowane są w poszczególnych kategoriach.

W celu zatwierdzenia wprowadzonych zmian na formatce *Domyślny rachunek* należy wbrać przycisk [ZAPISZ]. Zostanie zaprezentowany komunikat potwierdzający zapisanie zmian.



W przypadku próby zapisu zmian na formatce, w sytuacji gdy lista rachunków w poszczególnych sekcjach nie została załadowana zostanie zaprezentowany komunikat jak na poniższym ekranie.



Zmiana domyślnego rachunku bieżącego w wyniku aktywności w sesji

Podczas realizacji operacji związanej z wyborem rachunku bieżącego obciążanego (lub w przypadku zerwania lokaty również uznawanego) zapamiętywany jest ostatni wybór użytkownika.

Cechy rozwiązania:

- Dla każdej miniaplikacji wybór jest zapamiętywany niezależnie.
- Wybór rachunku jest zapamiętywany w chwili wydania dyspozycji (za takową akcję uznawane jest przejście użytkownika na drugi ekran formularza).
- Wybór jest pamiętany w czasie trwania sesji.
- Przy wejściu na formularz aktywny z wyborem rachunku domyślnie podstawiany jest rachunek ostatnio wybrany w danej miniaplikacji (nie ma wpływu na kolejność prezentowanych rachunków),
- Ostatnio użyty rachunek podstawiany jest tylko i wyłącznie wówczas, gdy na danej liście rachunków taki rachunek się znajduje,
- W przypadku, gdy dla danej miniaplikacji nie wykorzystano jeszcze żadnego rachunku automatycznie podstawiany jest pierwszy rachunek z listy wyboru,
- Wykonanie zmian w aplikacji za pośrednictwem [Butiku](#) powoduje rozpoczęcie nowej sesji użytkownika i utratę informacji o wykorzystanych ostatnio rachunkach.

11. Butik z miniaplikacjami

Po wybraniu opcji  **WIĘCEJ APLIKACJI** znajdującej się w [panelu sterowania](#) wyświetlany jest **Butik** z miniaplikacjami dostępnymi dla Klienta do samodzielnego wykorzystania.

Prezentowane są wyłącznie miniaplikacje zatwierdzone w systemie Asseco ABP do publikacji w danej jednostce organizacyjnej.

Użytkownik ma możliwość wyświetlania listy miniaplikacji w podziale na poniższe grupy:

- *Moje*: wszystkie wykorzystywane przez Klienta miniaplikacje, • *Nieaktywne*: miniaplikacje, z których Klient aktualnie nie korzysta.
- *Wszystkie*: wszystkie dostępne dla Klienta miniaplikacje.

Butik

MOJE NIEAKTYWNE WSZYSTKIE

Lista miniaplikacji

PRZYWRÓĆ DOMYŚLNE

Widoki miniaplikacji w Butiku zawierają dane przykładowe

300/500 plus

Złożenie wniosków o świadczenie wychowawcze „Program 300/500 plus”.

300/500 plus

Programy Dobry Start 300 plus oraz Rodzina 500 plus to możliwość uzyskania wsparcia finansowego dla rodzin wychowujących dzieci. Przejdź do systemu Eximie i złoż wniosek. [Złóż wniosek w Eximie >](#)

Autodealing

Miniaplikacja, która umożliwia integrację platformy Autodealing z systemem bankowości internetowej.

Autodealing

Usługa Autodealing. Przejdź do systemu Autodealing. [Uruchom Autodealing >](#)

Doładowania

Szybkie doładowanie telefonu oraz historia doładowań.

Doładowania

Wykonaj z szablonu **wybierz szablon**

NOWE DOŁADOWANIE

Geolokalizacja

Aplikacja prezentuje Twoją pozycję oraz najbliższe bankomaty i placówki banku na mapie.

Geolokalizacja

Najbliższa placówka 0,8 km

Najbliższy bankomat 1,1 km

Importy

Import plików z danymi przelewów oraz szablonów.

Importy

Przelewy zwykłe **elixir_1.txt**

Liczba przelewów 1

IMPORTUJ

Karty

Informacja o posiadanych kartach płatniczych wraz z możliwością ich zarządzania.

Karty

Kredytowa MasterCard Gold 9994...3456

8 057,73 PLN

Kredyty

Informacja o kredytach. Saldo, oprocentowanie, harmonogram spłat i inne.

Kredyty

Kredyt gotówkowy

Saldo kredytu 9 692,28 PLN

Najbliższa rata/termin 1 100,52 PLN / 04.08.2008

Lokaty

Oferta lokat i ich obsługa.

Lokaty

Lokata na 1 miesiąc

1 836,99 PLN

Data kapitalizacji 10.08.2007

Przelewy

Składanie przelewów jednorazowych i cyklicznych. Przeglądanie historii.

Przelewy

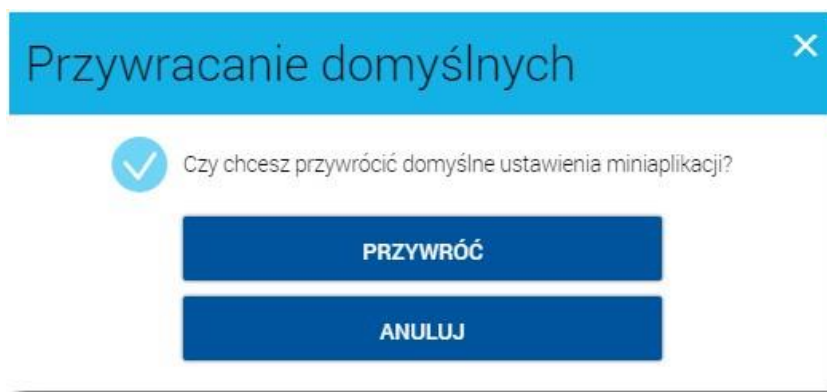
307 oczekująca płatność PLN 1 639,89 PLN

wybierz szablon

ZWYKŁY

Lista miniaplikacji posortowana jest alfabetycznie.

Użytkownik może przywrócić domyślny zestaw miniaplikacji wybierając opcję *PRZYWRÓĆ DOMYŚLNE*.



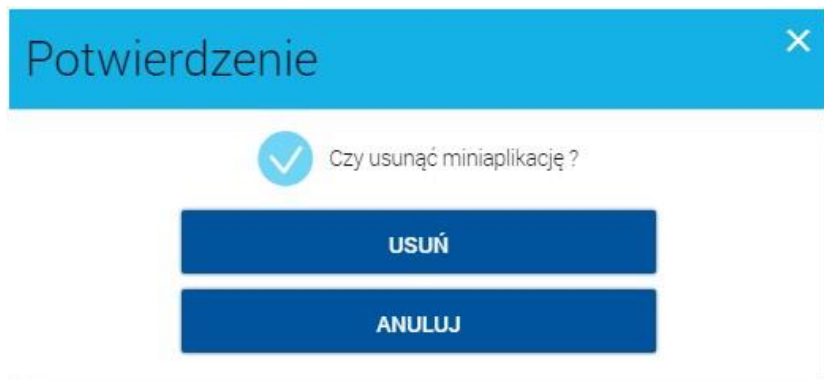
Wybranie opcji powoduje wyświetlenie przez system komunikatu z prośbą o potwierdzenie operacji poprzez przycisk [PRZYWRÓĆ] oraz powoduje przywrócenie domyślnego zestawu miniaplikacji, a mianowicie:

- z panelu sterowania (widok "Twoje aplikacje") i pulpitu znikną miniaplikacje, które nie są miniaplikacjami domyślnymi,
- w panelu sterowania (widok "Twoje aplikacje") dodane zostaną miniaplikacje domyślne, których użytkownik nie posiada,
- miniaplikacje domyślne, które użytkownik posiada pozostaną bez zmian (zachowane zostaną ich aktualne ustawienia i położenie).

Wybór przycisku  ([Dodaj]) dla wybranej miniaplikacji powoduje dodanie miniaplikacji na pulpicie z miniaplikacjami.

Dodanie miniaplikacji z butiku powoduje dodanie jej do listy miniaplikacji wyświetlanej w panelu sterowania na liście **Twoje aplikacje** oraz na pulpit. Użytkownik może sam zdecydować, które z dostępnych dla niego miniaplikacji mają znajdować się na pulpicie, w jakiej kolejności mają być prezentowane oraz w jakiej formie (standardowej, rozszerzonej) i umożliwia mu to link [EDYTUJ WYGLĄD](#) dostępny na pulpicie.

Wybór przycisku  ([Usuń]) dla wybranej miniaplikacji powoduje usunięcie miniaplikacji z listy. Operacja usunięcia miniaplikacji wymaga dodatkowo potwierdzenia poprzez przycisk [USUŃ].



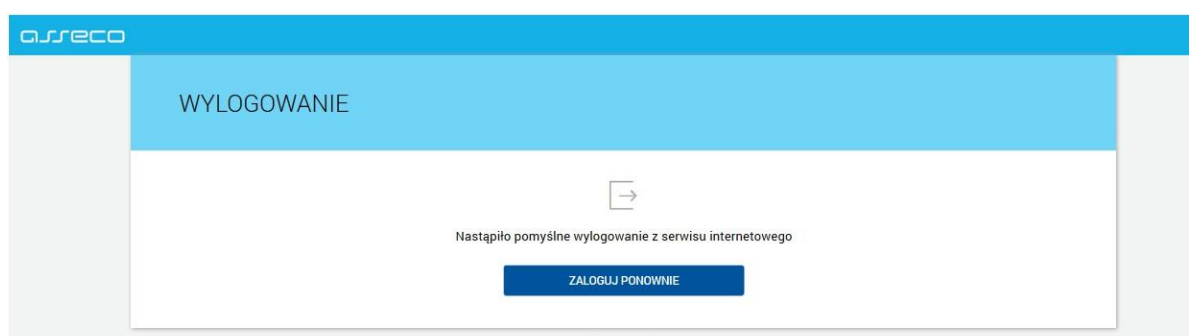
Po zmianie listy miniaplikacji (dodaniu, usunięciu lub przywróceniu domyślnych ustawień) system def3000/CBP dokona aktualizacji wyglądu pulpitu z miniaplikacjami i zawartości panelu sterowania dostosowując wygląd i zawartość do aktualnie posiadanej przez Użytkownika listy miniaplikacji.

Aktualizacja nastąpi po opuszczeniu butiku z miniaplikacjami.

12. Zakończenie pracy z systemem

Aby zakończyć pracę z systemem def3000/CBP należy użyć opcji *Wyloguj*, znajdującej się w [Panelu sterowania](#) systemu.

Po wybraniu tej opcji system wyświetla komunikat z informacją o poprawnym wylogowaniu z serwisu internetowego wraz z przyciskiem do ponownego zalogowania się do systemu - [ZALOGUJ PONOWNIE]:



Strona prezentowana jest w języku używanym przez użytkownika w systemie.

Wybranie przycisku [ZALOGUJ PONOWNIE] przenosi użytkownika na stronę [logowania do systemu](#).

Wylogowanie użytkownika z systemu może także nastąpić po upływie określonego czasu bezczynności użytkownika. Ma to na celu zwiększenie bezpieczeństwa. Jeżeli użytkownik nie wykonuje żadnych operacji przez 10 minut, system automatycznie kończy sesję pracy użytkownika w systemie i informuje użytkownika o tym fakcie komunikatem wylogowania (automatycznego):

AUTOMATYCZNE WYLOGOWANIE



Nastąpiło automatyczne wylogowanie

ZALOGUJ PONOWNIE



Automatyczne wylogowanie służy zwiększeniu bezpieczeństwa. Jeśli nie wykonujesz żadnych operacji, zostaniesz wylogowany automatycznie po 10 minutach bezczynności.

Automatyczne wylogowanie użytkownika z systemu może także nastąpić w wyniku zalogowania się do systemu def3000/CBP na innym urządzeniu przy pomocy tego samego loginu.

Copyright© Asseco Poland S.A. Materiały posiadają prawa do wykorzystania przez użytkownika systemu. Prawa autorskie należą do: Asseco Poland S.A. z siedzibą w Rzeszowie, ul. Olchowa 14, 35-322 Rzeszów tel.: +48 17 888 5555, fax: +48 17 888 5550 www.asseco.pl, e-mail: info@asseco.pl, NIP: 522-000-37-82, REGON: 010334578 Sąd Rejonowy w Rzeszowie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, KRS: 0000033391 Kapitał zakładowy w wysokości 83 000 303,00 PLN jest opłacony w całości; Nr Rej. GIOŚ: E0001990WZBW

Oprogramowanie dla bankowości.

Asseco Poland S.A.
ul. Olchowa 14
35-322 Rzeszów
tel.: +48 17 888 55 55
fax: +48 17 888 55 50

info@asseco.pl
asseco.pl

The logo for Asseco, featuring the word "ASSECO" in a stylized, bold, black font. The letters are composed of thick, blocky strokes, with the 'A' and 'S' having a distinctive geometric shape. The logo is centered on a solid blue background.